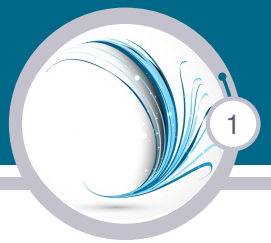
Université Grenoble Alpes - Saint Martin d'Hères
Inria - Grenoble - Rhônes alpes

La sécurité des outils de sécurité

Aurélien Monnet-Paquet
aurelien.monnet-paquet@e.ujf-grenoble.fr

16 Juin 2016

Plan



Introduction

Les **logiciels de sécurité** protègent particuliers et entreprises face aux **attaques**.

Nous avons testé la **sécurité des logiciels de sécurité** face aux de **bombe de compression**.

Qu'est ce qui **protége** les outils de sécurité ?

Outils de sécurité
Antivirus

Un **antivirus** analyse un fichier de différentes manières :

- **Analyse statique (signature)**
  - Méthode **populaire** chez les éditeurs.
  - Inefficace contre les malwares polymorphes.

Outils de sécurité
Antivirus

Un **antivirus** analyse un fichier de différentes manières :

- **Analyse statique (signature)**
  - Méthode **populaire** chez les éditeurs.
  - Inefficace contre les malwares polymorphes.
- **Analyse dynamique**
  - Exécution du code dans une *VM*.
  - Méthode la plus **puissante**.
  - Coût important en CPU et peut provoquer des fausses alertes.

Outils de sécurité
Antivirus

Un **antivirus** analyse un fichier de différentes manières :

- **Analyse statique (signature)**
  - Méthode **populaire** chez les éditeurs.
  - Inefficace contre les malwares polymorphes.
- **Analyse dynamique**
  - Exécution du code dans une *VM*.
  - Méthode la plus **puissante**.
  - Coût important en CPU et peut provoquer des fausses alertes.
- Extrait les fichiers compressés pour analyse.

Nous avons testé **ClamAV** et **Comodo** comme antivirus Linux.

Outils de sécurité
Agrégateurs d'antivirus - Sites web

Outils utilisés en **réponse à un incident** (pas de temps réel) d'où l'importance d'avoir plusieurs antivirus qui analysent le fichier suspect.

Site web	**VirusTotal**	**Jotti**	**Virscan**
Nombre d'antivirus	57	19	39
Localisation	Google, Espagne	Pays-bas	Chine
Type d'hébergement	Cloud	Cloud	Cloud

Avantage

Analyse plus complète des fichiers soumis.

Inconvénient

Aucun contrôle de nos fichiers.

Les frameworks fontionnent de la même manière que les sites web.

Les *frameworks* permettent :

- D'analyser en **local**.
- **D'identifier et classer** le type des fichiers grâce à **YARA**.
- **De confondre plusieurs fichiers** au contenu similaire (**ssdeep**).
- **Extraire et analyser récursivement** des fichiers compressés.

Les deux *frameworks* que nous avons testés sont :

- **Mastiff** : utilisable en ligne de commande
- **Viper** : utilisable via son interface web

Outils de sécurité
IDS

Les **systèmes de détection d'intrusion** analysent le trafic réseau et fonctionnent sur un système de règles et de "*pattern matching*".
Nous avons choisi d'étudier le comportement de **Suricata**.

Pour une règle 3 **actions** sont possibles :

- Laisser passer le paquet sans en finir l'analyse.
- Rejeter le paquet en générant une alerte et des paquets ICMP erreur.
- Générer une alerte dans le fichier de logs.

Génération de témoins :

- Génération d'un malware Windows connu.
- Génération d'un fichier inoffensif.

Génération de témoins :

- Génération d'un malware Windows connu.
- Génération d'un fichier inoffensif.

Compression du malware :

- Compression du malware dans différents formats.

Génération de témoins :

- Génération d'un malware Windows connu.
- Génération d'un fichier inoffensif.

Compression du malware :

- Compression du malware dans différents formats.

Bombes de compression :

- Little boy.
- Snake.
- Quines.

Expérimentations
Méthodologie

Outil	Catégorie	Version
VirusTotal	Site web	
Jotti	Site web	
Virscan	Site web	
ClamAV	Antivirus	0.98.7
Comodo	Antivirus	1.1.268025.1
Mastiff	Framework	0.7.1
Viper	Framework	0.12.9
Suricata	IDS	3.0

Résultats et observations
Dissimulation du payload

Nom fichier	Ratio de détection			Résultats	
	VirusTotal	Jotti	Virscan	ClamAV	Comodo
payload	42/56	17/19	20/39	✓	✓
payload.gz	38/56	18/20	17/39	✓	✓
payload.lz	2/56	1/19	1/39	X	X
payload.lzma	7/56	4/19	4/39	X	X
payload.lzo	4/56	3/19	5/39	✓	X
payload.tar.bz2	32/56	17/20	18/39	✓	✓
payload.tar.gz	33/56	17/20	16/39	✓	✓
payload.tar.xz	18/56	13/20	5/39	✓	X
payload.zip	40/56	18/20	12/39	✓	✓

Résultats et observations

Dissimulation du payload - Bilan

- Tout le monde de détecte pas le payload.
- Tous les formats ne sont pas détecté :
  - **gz**, **zip**, et **bz2** sont **bien** supportés.
  - **lz**, **lzma** et **lzo** sont **mal** reconnus.

Résultats et observations

Antivirus et little boy

Nom du fichier	ClamAV		Comodo	
	Résultats	Temps	Résultats	Temps
payload.exe	✓	9.2s	✓	4s
fichier_inoffensif	X	8.9s	X	4s
250Mo.gz	X	9.6s	X	8s
1Go.gz	X	10s	X	20s
2Go.gz	X	12.4s	X	44s
250Mo.zip	X	12s	X	8s
1Go.zip	X	25.7s	X	21s

Résultats et observations

Antivirus et autres bombes

Nom du fichier	ClamAV		Comodo	
	Résultats	Temps	Résultats	Temps
Quine	X	8.4s	X	4s
Fragmentée	X	10.9s		> 15 min

- ClamAV décompresse au maximum 27 Mo dans le format xz.
- ClamAV : Erreur de segmentation avec environ 400 récursions.
- Comodo a une limite de profondeur.

Résultats et observations

Agrégateurs et bombes

Nom du fichier	Ratio de détection		
	VirusTotal	Jotti	Virscan
250Mo.gz	0/56	1/19	2/39
1Go.lz	0/56	0/19	0/39
250Mo.lzma	0/57	0/19	0/39
1Go.lzo	0/56	0/19	0/39
250Mo.tar.bz2	0/56	4/18	1/39
1Go.tar.gz	1/57	3/16	2/39
250Mo.tar.xz	0/57	2/20	0/39
1Go.zip	2/55	3/20	0/39
Quine	0/55	1/18	0/39
Framentée	1/56	4/15	0/39

Résultats et observations
Agrégateurs et bombes

Antivirus sans réponse		Antivirus avec réponse positive		
VirusTotal	**Jotti**	**VirusTotal**	**Jotti**	**Virscan**
TotalDefense	ESET	VBA32	VBA32	VBA32
Zoner	F-Secure	Baidu	Arcabit	Fprot
	Trend Micro	Zillya	AVG	Panda
	GData		Avast	
	Sophos		Sophos	

Résultats et observations

Antivirus - Bilan

Les antivirus ont un **comportement similaire sur un même site**.
Par contre, entre les sites, ce n'est pas le cas.

Limite de détection :

- **Taille** du fichier décompressé : 315 Mo.
- **Profondeur minimum** de détection : 6.

Résultats et observations
Agrégateurs - Frameworks + IDS

Mastiff analyse récursivement r.zip sans condition d'arrêt.
Envoie de manière abondante des requêtes vers VirusTotal.

Résultats et observations
Agrégateurs - Frameworks + IDS

Mastiff analyse récursivement r.zip sans condition d'arrêt.
Envoie de manière abondante des requêtes vers VirusTotal.

Viper extrait entièrement les fichiers au moment de la soumission.
Utilisation à 100% du CPU alloué à la VM.
Le temps d'occupation est proportionnel avec la taille du fichier decompressé.

Résultats et observations
Agrégateurs - Frameworks + IDS

Mastiff analyse récursivement r.zip sans condition d'arrêt.
Envoie de manière abondante des requêtes vers VirusTotal.

Viper extrait entièrement les fichiers au moment de la soumission.
Utilisation à 100% du CPU alloué à la VM.
Le temps d'occupation est proportionnel avec la taille du fichier decompressé.

Suricata déclenche bien les règles lors de l'analyse des fichiers.
Cependant, il n'y a aucune forte varation de l'utilisation du CPU et de la mémoire RAM.

Conclusion

- Le simple fait de compresser un malware peut leurrer jusqu'à 95% des antivirus.
- Les protections contre les DoS sont incomplètes :
  - Plusieurs antivirus sont victimes des bombes de compression.
  - On a pu provoquer une erreur de segmentation sur ClamAV.
  - Mastiff extrait à l'infini les fichiers compressés.
  - Les antivirus comme ClamAV et Comodo ne détectent jamais les bombes de compression.

Merci de votre attention!