Je suis pleinement conscient(e) que le plagiat de documents ou d'une partie de document constitue une fraude caractérisée.
Nom, date et signature :

Étude des fichiers compressé sur les moyens de protection défensifs

Monnet-Paquet Aurélien
.
Supervised by : Lauradoux Cédric

Juin 2016

Abstract
Présentation de l'étude du comportement des outils défensif appliqué à un environnement de fichiers compressé par différents types d'algorithmes.
Cette étude permettra d'analyser le comportement des outils :

- Systèmes de détection d'intrusion (ou IDS) : Suricata
- Sites agrégateurs d'antivirus : VirusTotal, Jotti, Virscan
- Framework d'analyse de malware : Mastiff, Viper
- Antivirus Windows / Linux : ClamAV, Comodo

lorsqu'ils sont soumis à des fichiers compressés.

Keywords Bombe de compression · IDS · VirusTotal · Antivirus · Framework de détection de malware

1 Introduction

Selon l'étude de McAfee/CSIS de 2014, les pertes économique dues à la cybercriminalité représente 445 milliards de dollars par an, avec des attaques en forte hausse.
Le but de ce rapport est d'analyser le comportement des outils défensifs sur les fichiers compressés.
Est-ce que tous les formats de compression sont supportés ?
Le comportement des antivirus commun entre les sites sont-ils similaire ?
Est-ce que les bombes sont détectées ?

Monnet-Paquet Aurelien
Université Grenoble Alpes, 38400 Saint Martin d'Hères
E-mail: monnetpa@e.ujf-grenoble.fr

Lauradoux Cedric
Inria, 38334 Montbonnot
E-mail: cedric.lauradoux@inria.fr

2 Les IDS : Sonde de détection d'intrusion

2.1 Présentation

Les entreprises sont des cibles privilégiées par des pirates car elle renferment bien souvent les données (sensible) de leurs utilisateurs ainsi que des secret industriels. La mise en place d'un IDS à l'entrée (/ sortie) du réseau de l'entreprise permettrai de minimiser les fuites de ses données.
Un IDS analyse le trafic réseau de manière transparente et permet ainsi de remonter des alertes pour l'administrateur voire même de bloquer certaine connexions.
Est il possible de bloquer Suricata [2] sur l'analyse d'une bombe de compression afin de laisser passer un autre malware dans le réseau de l'entreprise ?

2.2 Fonctionnement

Un IDS fonctionne sur un système de règles. Un administrateur, définit un certain nombre de règles que l'IDS doit vérifier lors de l'analyse du réseau. Suivant l'action affectée à une règle qui "matcherai", l'IDS peut :

- laisser passer un paquet
- détruire la paquet (mode IPS uniquement)
- rejeter le paquet, en générant des paquets ICMP erreur ainsi qu'une alerte
- générer une alerte visible dans un fichier de logs

2.3 Analyse

2.4 Conclusion sur les IDS

3 Les sites web agrégateurs d'Antivirus

3.1 Présentation

Dans cette section, nous allons analyser le comportement des agrégateurs d'antivirus que l'on peut trouver sur internet.
Cette expérience portera sur 3 sites :

- VirusTotal [4]
- Jotti [5]
- Virscan [6]

Nous allons tester chacun de ses sites en 3 étapes :

- 1. Analyse témoin : un fichier connu pour être malveillant
- 2. Analyse du même fichier dans différents formats de compression
- 3. Analyse de l'impact des différentes bombes de compression

3.2 Fonctionnement

VirusTotal est actuellement le site le plus populaire dans ce domaine. Il permet, à ce jour, d'analyser un fichier avec 57 antivirus différents. Il existe 3 manières pour soumettre un fichier :

- L'interface web
- L'API
- Recherche par hash

Remarque : pour pouvoir utilisé l'API, il faut avoir un compte actif.

Jotti permet d'analyser un fichier avec 19 des antivirus les plus repandu.
La soumission d'un fichier se fait via l'interface web su site.
Il est également possible d'effectuer une recherche par hash.

Virscan dispose de 39 antivirus pour analyser les fichiers soumis via leur site web.

3.3 Analyse

3.4 Conclusion sur les agrégateurs

4 Les Frameworks d'analyse de malwares

4.1 Présentation

L'utilisation de site comme VirusTotal implique l'envoi de fichiers vers des serveurs que l'on ne contrôle pas. Une entreprise ne peut se permettre de mettre leurs données sensibles dans des mains inconnues. C'est pourquoi, les framework tels que Mastiff et Viper sont important. En effet, une entreprise peut analyser de manière pousser un fichier suspect via un analyseur interne à cette entreprise.
Le but de cette expérience est de vérifier que ses outils sont conforment face a des bombes de compression.

4.2 Fonctionnement

4.3 Analyse

4.4 Conclusion sur les frameworks

5 Les Antivirus Linux / Windows

5.1 Présentation

Contrairement aux agrégateurs d'AV et aux frameworks, les antivirus utilisent les ressources (CPU + RAM) des machines cibles pour analyser un fichier suspect. En effet, les AV sont des programmes installés sur des systèmes pour les protéger des attaques que leurs propriétaires peuvent rencontrer.
Nous allons vérifier que ce type d'outil est robuste face aux attaques par déni de service provoqué par des bombes de compression.

5.2 Fonctionnement

5.3 Analyse

5.4 Conclusion sur les frameworks

6 Conclusion

References

1. David J. Day et Benjamin M. Burns, "A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines"
2. oisf.net, The Open Information Security Foundation, organisation à but non lucrative qui développe et met à jour Suricata.
3. redmine.openinfosecfoundation.org/projects/suricata/wiki/, la documentation pour utilisateurs et développeurs de Suricata.
4. virustotal.com, site agrégateurs d'antivirus, filière de Google.
5. virusscan.jotti.org, site agrégateurs d'antivirus, basé aux Pays-Bas.
6. www.virscan.org, site agrégateurs d'antivirus, basé en chine.
7. www.korelogic.com
8. www.viper.li
9. irma.quarkslab.com
10. www.comodo.com
11. www.clamav.net