Règles YARA : tests pratiques

Franck Jeannot

Montréal, Canada, Novembre 2017, P455, v1.0

Abstract

YARA rules direct practice by using the tool **YARA Gui**.

Keywords: YARA, yara rules, YARA Gui, NVISO, Inquest, entropie

1. Introduction

On met en pratique directement l'usage de règles YARA avec l'outil **YARA Gui**. On peut se référer notamment aux revues relatives à l'usage et détection de champ DDE dans des documents MS WORD [1] comme point de départ sur la justification et fort intérêt d'utiliser ce genre d'outil. Dans cet exemple, après avoir téléchargé YARA Gui [2] on met en pratique divers jeux de règles utiles.

2. Obtention et compilation de règles

Je suggère d'obtenir et tester des règles YARA existentes de sources reconnues [3]. De plus pour chaque règle, il convient de la documenter : source, usage... etc

Exemple de rajout de commentaire d'une règle Yara avec ici son url source :

```
//Source : https://github.com/tenable/yara-rules/tree/master/generic
```

Avec **YARA Gui** il suffit ensuite de sélectionner un fichier et de l'appliquer à une règle pour en générer la compilation (voir statut suivant ***compiled***).

1. https://www.franckjeannot.com/wp-content/uploads/yaradde.pdf
2. https://sigint9.github.io/yaragui/
3. https://github.com/InQuest/awesome-yara

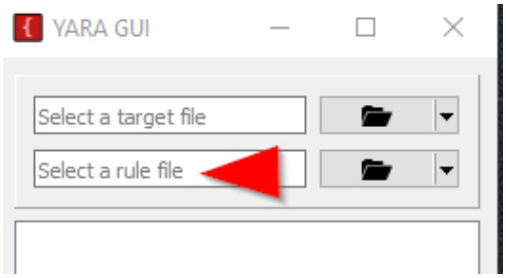

FIGURE *(1): Sélection d'une règle YARA*

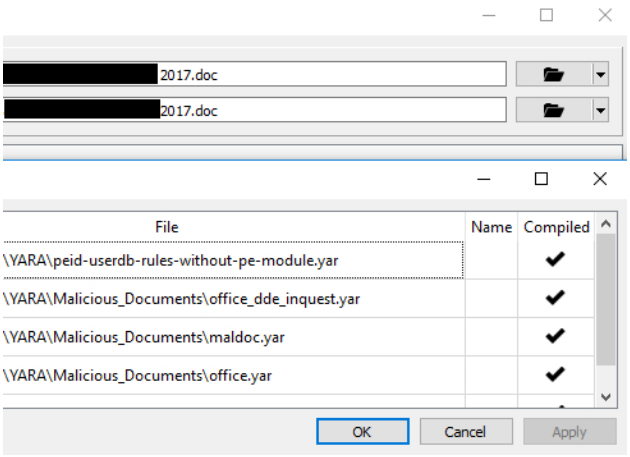

FIGURE *(2): Plusieurs règles ont été utilisées avec succès et compilées*

3. Yara Gui : exemple de règles sur les packers

Dans ce cas de figure on s'intéresse à détecter des signatures spécifiques de Packers, cela peut s'avérer utile dans une analyse ou bien avant execution d'un .exe Windows. Des références utiles sur ce sujet sont celles de **Didier Stevens** et **Securityflux** [4] [5].

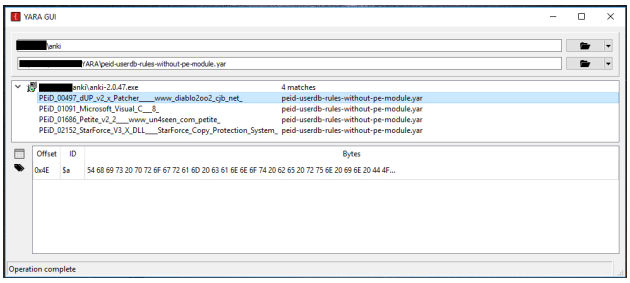

FIGURE *(3): Exemple d'interface et scan d'un fichier .exe*

4. http://www.securityflux.com/?p=121
5. https://blog.didierstevens.com/2015/03/18/update-peid-userdb-to-yara-rules-py

Dans l'exemple précédent il a été utilisé un ensemble de règles publiquement disponibles et mises à disposition sur le Github de Didier Stevens [6]. Pour une investigation plus fine et plus avancée il existe des outils et formats plus spécialisés comme PEidb.

4. Yara Gui : exemple des documents compressés

Une limitation de ce petit utilitaire très simple qu'est Yara Gui est de ne pas faire la décompression de fichiers compressés. Le format MS Word .docx en fait partie [7]. Dans l'exemple ci-dessous on considère une analyse multi-documents comme suit :

1 un document testa.docx avec avec un DDE embarqué...
2 testa.docx décompressé avec tous les paquets .xml dont **document.xml**
3 un exemple de graphe d'entropie 1D de testa.docx

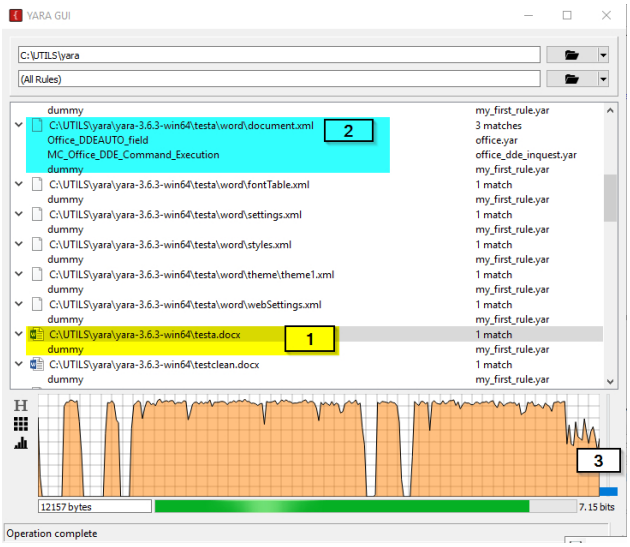

FIGURE *(4): Exemple d'analyse multi-documents et entropie*

Conclusion : on s'aperçoit que seule la règle par défaut "dummy" pour testa.**docx** est activée, cette règle est juste une vérification de bon déroulement. Finalement le DDE n'est découvert que dans le fichier décompressé **document.xml** (zone mise en valeur en bleu), au final, dans le cas de documents compressés, on utilisera **zipdump.py** comme contournement. [8]

6. https://raw.githubusercontent.com/DidierStevens/DidierStevensSuite/master/peid-userdb-rules-without-pe-module.yara
7. https://www.franckjeannot.com/wp-content/uploads/yaradde.pdf
8. https://github.com/DidierStevens/DidierStevensSuite/blob/master/zipdump.py