TP2 : Antivirus

Remarques préliminaires :

Les expérimentations décrites dans ce document ne doivent pas être réalisées en dehors de la salle dédiée aux TP

Ce document est confidentiel, il vous est interdit de le redistribuer, de le diffuser même partiellement sous quelque forme que ce soit.

Partie 1 : Infection et détection en temps réel

Pour cette partie, utiliser la machine virtuelle windows fournie au TP précédent, en prenant soin de commencer par faire une copie de l'état initial pour pouvoir restaurer cet état si nécessaire (avec Virtual Box).

A) Scénario classique d'infection, sans anti-virus

Avec le navigateur firefox, allez sur : http://www.cracksfiles.com/

Nous allons tenter de télécharger le programme piraté au titre prometteur « Kaspersky Total Security 2017 Crack Full Downloads ».

Question 1 : Quelle protection fournit le navigateur préalablement au téléchargement ?

Question 2 : Sur quoi se base la détection de cette menace ?

Question 3 : Poursuivre le téléchargement, afin d'obtenir un fichier « download.exe »

Question 4 : Installer ce programme. Contient-il le logiciel attendu ? Que se passe-t'il de visible pour un utilisateur non informé ? Essayez de télécharger depuis ce même site un autre « logiciel piraté» et comparez le fichier téléchargé (taille, diff...). Qu'en pensez-vous ? Quel est le nom de cette application (cf. cours) ?

Question 5 : Installer un anti-virus gratuit, par exemple Avast :

https://www.avast.com/fr-fr/index

Question 6 : Faire une recherche des menaces, que trouvez-vous ? (vous pourrez essayer de désinfecter cette menace en fin de TP s'il vous reste du temps)

B) Scénario classique d'infection, avec anti-virus

Question 1 : Avec l'anti-virus activé, sur le même site que en A, retentez le téléchargement et l'installation du même « programme piraté ».

Question 2 : Comment se comporte l'anti-virus ? Quels mécanismes de détection sont mis en place (essayez de penser au niveau système, en terme d'architecture logicielle et d'intégration avec l'OS) ?

Question 3 : Que penser de la pertinence de l'anti-virus en terme de « protection en temps réel » ? Comment nuancer ce propos avec le théorème de Cohen (cf. cours) ?

Question 4 : Quelles recommandations pourriez-vous faire en entreprise ? Quels éléments de politique de sécurité pourriez vous mettre en place pour augmenter la pertinence d'un système de protection en temps réel ?

Partie 2 : Performances des anti-virus

Reprenez une version propre de votre machine virtuelle, en restaurant son état initial (virtual box) ou en refaisant une importation (vmware).

Extraire sur le bureau le fichier Virus.Win.zip (clic droit, extraire ici puis sur le fichier extrait clic droit à nouveau, extraire dans le répertoire Virus.Win). Cette archive contient une sélection de virus pour mettre à l'épreuve quelques anti-virus.

Question 1) Un anti-virus libre et opensource « clamav » est déjà téléchargé et l'exécutable est sur le bureau. L'installer. Quelles sont les principales étapes de l'installation ? Pourquoi est-il nécessaire de faire une mise à jour des données ?

Question 2) Faire une « analyse personnalisée » du répertoire Virus.Win exclusivement. Combien de fichiers (donc de virus) contient le répertoire ? Combien de virus sont détectés (%) ? Quel est le temps mis par l'anti-virus (s) ? Quel est sa performance en vitesse de détection (fichiers/s) ?

Question 3) Choisir dans la liste (ou ailleurs si vous souhaitez!) un anti-virus à évaluer :http://www.commentcamarche.net/faq/35-antivirus-gratuit-lequel-choisir

Vous choisirez de préférence un anti-virus non déjà choisi (vous écrirez chacun votre choix au tableau). Certains anti-virus payants disposent

Question 4) L'installer puis choisir les options permettant une analyse personnalisée du répertoire contenant les virus. Attention, selon les options, il se peut que l'anti-virus ne détecte aucune menace... (discutez la pertinence de ce choix).

Question 5) Complétez au tableau les critères de pertinence/performance que vous aurez-obtenus

Question 6) En comparant les différents résultats, quelle première analyse faites-vous ? Faites une recherche sur internet de « classement anti-virus », comment se positionne votre analyse face aux éléments avancés dans les documents que vous avez trouvés ?

Question 7) Relancer l'analyse de la question 2, et comparez les performances (vitesse/débit). Voyez-vous un impact ?

Partie 3 : Analyse et désinfection d'une menace virale

Récupérez la VM « MACHINE_INFECTEE ». Cela correspond à la machine d'un utilisateur qui vous sollicite parce qu'il trouve que sa machine a ralenti, et qu'il y a des « choses bizarres » qui se passent parfois.

Question 1) Proposez un scénario d'analyse de cette machine qui pourrait s'appliquer de manière générique à un maximum de machines d'utilisateurs d'une entreprise.

Question 2) Appliquez vos propositions et faites l'analyse de la machine. Listez les menaces détectées.

Question 3) Faites les recherches sur internet pour comprendre le mode de fonctionnement et les risques associés aux menaces. En déduire si vous pouvez effectuer une désinfection. Si c'est le cas, procédez à la désinfection.

Question 4) En considérant le temps nécessaire à l'analyse et à la désinfection, quel moyen(s) alternatif(s) pourriez-vous mettre en œuvre dans une entreprise pour arriver à un résultat proche (discutez cette proximité de résultat et les risques éventuels) ?

Partie 4 (optionnelle) : analyse d'un virus « inconnu »

Les menaces détectées dans la partie 3 proviennent de certains exécutables disponibles dans la bibliothèque de virus. En identifier un, le renommer avec l'extension « .exe », puis utiliser les outils de débogage et de décompilation (disponibles sur le bureau dans la VM) pour tracer les points clés (mécanisme(s) de réplication, types de fichiers impactés, charge finale…).