École de technologie supérieure
Département de génie logiciel et des TI

Trimestre : Hiver 2018
Professeur : Chamseddine Talhi
Chargé de cours : Marc-André Drapeau
Chargé de lab. : Abderrahmane Boukliouа

GTI 619 - Sécurité des systèmes

LABORATOIRE 1

Les vers et les virus informatiques représentent une menace contre les réseaux informatiques. Ces logiciels malveillants réussissent généralement à se reproduire soit automatiquement en utilisant une vulnérabilité logicielle ou soit avec l'aide des usagers non expérimentés (ingénierie sociale).

Lorsque les premiers virus informatiques sont apparus au début des années 80, leur propagation était liée à l'échange de disquettes infectées. Ces virus pouvaient alors prendre des mois avant d'infecter un grand nombre d'ordinateurs.

Avec l'avènement de l'Internet, les logiciels malveillants réussissent maintenant à se propager très rapidement et à causer de nombreux dégâts. Par exemple, le ver ***Slammer*** a réussi à infecter la majorité des ordinateurs vulnérables (plus de 75,000) sur la planète en moins de 10 minutes[1]. De son côté, le ver ***ILoveyou*** aurait causé entre 10 et 15 milliards de dollars de dommage[2].

Divers obstacles se retrouvent sur le chemin des vers qui se propagent automatiquement en exploitant des vulnérabilités logicielles. Ces vers démontrent généralement certains comportements très typiques. Ils balaient les réseaux, en utilisant des paquets `PING echo request` ou `TCP SYN`, à la recherche d'ordinateurs vulnérables. Les adresses de ces victimes sont habituellement générées aléatoirement, ce qui cause de nombreuses connexions invalides dues à des adresses inexistantes ou inaccessibles à cause de pare-feux. Se faisant, les vers deviennent clairement identifiables et peuvent être retracés et bloqués.

Il a donc fallu « inventer » un nouveau moyen de propagation permettant d'infecter le plus d'ordinateurs possible. Ainsi, au lieu que les logiciels malveillants utilisent des moyens proactifs, ils sont devenus passifs et espèrent que les ordinateurs vulnérables viennent à eux.

En infectant un site web populaire, les logiciels malveillants n'ont simplement qu'à attendre que des personnes, utilisant des fureteurs vulnérables ou mal configurés, visitent ce site afin d'infecter ces nouveaux ordinateurs. Donc, pas de balayage, d'adresse inexistante, de pare-feu, etc. Le cas du site de *India Times* a été très médiatisé en novembre 2007[3].

Afin qu'il puisse bien répondre aux menaces que représentent les divers logiciels malveillants (vers, virus, chevaux de Troie, scripts malicieux inclus dans les pages Web, etc.), le spécialiste en sécurité se doit de bien comprendre leurs causes ainsi que leurs divers modes de fonctionnement.

---

1 D. Moore *et al*. *The Spread of the Sapphire/ Slammer Worm*

2 G. Jones, *The 10 Most Destructive PC Viruses…* , http://www.techweb.com/showArticle.jhtml?articleID=160200005

3 D. Goodin, *IndiaTimes website 'attacks visitors'*, http://www.theregister.co.uk/2007/11/10/india_times_under_attack/

Ce laboratoire a donc pour objectif d'étudier certaines facettes importantes des logiciels malveillants. Ainsi, au cours de ce laboratoire, vous devrez :

- Analyser divers logiciels malveillants et expliquer en détail leur fonctionnement respectif.

En découvrant la simplicité de certains vers et logiciels malveillants, vous comprendrez plus facilement pourquoi ces programmes sont aussi nombreux.

Ce type d'analyse se fait régulièrement dans certaines entreprises spécialisées qui cherchent à étudier les nouvelles tendances en fait de menaces informatiques afin de les contrer le plus efficacement possible.

Les justifications doivent inclure des parties des scripts.

Partie 1 – Analyse d'un ver

Le logiciel malveillant (*malware*) dont des extraits de code sont soumis à votre analyse fonctionne à la fois comme un cheval de Troie (trojan) et un *keylogger* (spyware). Selon les auteurs, la version du *malware* de laquelle sont extraits ces fragments de code fonctionne sur certains ordinateurs vulnérables des environnements XP/Vista/Seven mais aussi 2003/2003R2/2008/2008R2. Son mode opératoire est le suivant : aussitôt que l'ordinateur est infecté (copie du malware dans le "*home"* de l'utilisateur), il infecte tous les processus de l'utilisateur courant. Si l'utilisateur System est infecté alors tous les autres profils utilisateurs de l'ordinateur sont également contaminés. Chacune des copies déployées s'exécute parallèlement ce qui a d'office des conséquences sur les performances de la machine. De plus, dès l'infection, le malware se connecte à un serveur distant duquel il reçoit un fichier de configuration qui détermine son comportement sur la machine infectée. Il peut également recevoir du serveur distant des mises à jour (nouvelles versions) ou des commandes et les exécuter localement.

Le malware récolte des données sur l'ordinateur infecté et les envoie vers un serveur distant (dans un format crypté) en utilisant le protocole HTTP. Les données récoltées sont variées et découlent de plusieurs applications et services. A cet effet, les auteurs évoquent par exemple la collecte de :

▪ logins à partir des clients FTP suivants : CoreFTP, CuteFTP, FAR Manager, FileZilla, FlashFXP, FTP Commander, SmartFTP, Total Commander, WinSCP, WsFTP; ▪ cookies de : Adobe (Macromedia) Flash Player, wininet.dll, Mozilla FireFox; ▪ certificats (import) à partir du gestionnaire de certificats de Windows.

Comme le suivi des touches clavier appuyées (*keylogging*), plusieurs autres fonctionnalités sont également connues de ce malware.

1. En analysant le fichier inject.txt, montrez ou expliquez comment le malware arrive à infecter tous les processus d'un utilisateur donné. Justifiez
2. Comment fait-il pour ne pas réinfecter un processus déjà infecté ? Justifiez
3. En analysant le code contenu dans le fichier requete.txt, expliquez comment le malware réussit à exécuter une injection HTTP (Par exemple, comment il arrive à utiliser une requête de votre session pour poster d'autres liens infectés) ? Justifiez

Pour toutes vos réponses, utilisez des parties annotées du code des fichiers inject.txt et requete.txt. Afin de vous faciliter la compréhension du code, vous pouvez utiliser les liens suivants. Ils fournissent plus d'information sur l'API de Windows:

- https://msdn.microsoft.com/library/windows/desktop/hh920508.aspx
- WinInet:https://msdn.microsoft.com/en-us/library/windows/desktop/aa383630(v=vs.85).aspx

Partie 2 – Analyse d'un ver – *mass-mailer*

De nombreux vers utilisent l'ingénierie sociale pour se propager. Ces vers parviennent à convaincre certains récipiendaires de courriels de lancer un fichier joint à ces messages malveillants. ***Ver-A*** en est un bon exemple. On assume ici que le vecteur d'infection est un courriel avec un attachement. L'attachement est un fichier contenant du code VBA.

Votre tâche est d'analyser ce ver en fonction des éléments suivants :

1. La méthode d'infection : a) Comment s'installe-t-il sur un ordinateur vulnérable? b) comment le ver parvient-il à infecter de nouveaux fichiers ou comment arrive-t-il à s'exécuter pour infecter de nouveaux fichiers? Justifiez vos réponses
2. La méthode de propagation : comment le ver parvient-il à se propager d'un ordinateur à l'autre? Justifiez
3. La méthode de détection de cible : Comment le malware cible-t-il les fichiers à infecter? Justifiez
4. Documentation claire des étapes d'infection : Indiquez clairement le fonctionnement général du vers. (7 fonctionnalités au minimum à inclure).

On recommande aux étudiants d'utiliser un éditeur de texte en ligne afin de ne pas alerter leur logiciel anti-virus (https://www.editpad.org/).

Pour toutes vos réponses, utilisez des parties annotées du code du fichier Ver-A. Une explication des routines utilisées est nécessaire. Vous pouvez utiliser la librairie VBA : https://msdn.microsoft.com/fr-ca/vba/office-shared-vba/articles/office-vba-object-library-reference

Partie 3 – Analyse d'un logiciel malveillant mystérieux – Plus difficile

L'objectif de cette partie du laboratoire est d'analyser en détail le mode de fonctionnement d'un logiciel malveillant écrit en JavaScript. Pour vous aider dans votre analyse, voici trois sites intéressants :

- http://jsbeautifier.org/
- http://relentless-coding.org/projects/jsdetox
- http://www.utilities-online.info/urlencode/#.Vo83gxXhDIU/
- https://jsfiddle.net/

Votre tâche est d'analyser ce logiciel malveillant en utilisant la même approche que celle utilisée pour la première partie. Ainsi :

1. Code du logiciel malveillant : Présentez le code désobfusqué du logiciel malveillant tout en expliquant la démarche qui a permis d'obtenir le code final.
2. Description du mécanisme de protection du virus : quels sont les éléments mis en place qui rendent l'analyse du virus plus complexe? Expliquez les mécanismes de protection du virus. (avec capture d'écran)

----------Avertissement----------

Pour les trois premières parties, les fichiers disponibles sur le site fournissent le code de programmes malveillants. L'étude devra se faire **SANS EXECUTER** les codes puisque cela pourrait avoir des conséquences fâcheuses.

Partie 4 – Analyse d'un script malicieux

De plus en plus, les logiciels malveillants se propagent de façon passive. En infectant une page Web, il est possible d'infecter tout visiteur de cette page. Divers scripts peuvent alors être exécutés de façon automatique et compromettre l'ordinateur du visiteur.

L'objectif de cette partie du laboratoire est d'analyser une page Web contenant divers scripts. Ces scripts ne sont pas malicieux. La page Web peut donc être téléchargée dans un fureteur. Ainsi, il faut entre autres choses :

- Découvrir les divers scripts inclus dans la page Web;
- Déterminer le mode de fonctionnement, c'est-à-dire le résultat produit ainsi que les causes. Par exemple, si le script exploite une faille, il est important de le mentionner.
- Déterminer le comportement des fureteurs en présence de ces scripts. Démontrer si les scripts fonctionnent sous les navigateurs suivants : Chrome, Firefox et Internet Explorer (Edge)
    - Par la suite, installer l'extension NoScript, répéter l'expérience et expliquer le fonctionnement de NoScript

Il n'est pas suffisant de télécharger cette page dans un fureteur. Il faut analyser attentivement le code de la page HTML. Dépendamment du fureteur, le comportement est différent. Une capture d'écran du code de chacun des scripts ainsi qu'une explication de leur mode de fonctionnement est nécessaire.

Partie 5 –Analyse mystère

Dans cette partie, vous avez à manipuler un autre type d'obfuscation JavaScript. À partir de la ligne de code fournie, veuillez répondre aux questions suivantes (explication de 10 lignes maximum pour chaque question):

1. Expliquez pourquoi et comment le navigateur arrive à comprendre et exécuter ces caractères. (3 pts)
2. Expliquez de manière concrète le fonctionnement du script. (2 pts)

   Conseils :

   - **Pour cette partie, il faudra désobfusquer le script avant de l'analyser.**
   - **Effectuez une recherche sur la méthode d'encodage JJEncode.**

Information

- Lisez très attentivement la grille de correction qui suit. Celle-ci vous indiquera les sections auxquelles vous devrez répondre ainsi que la pondération de chaque section de votre rapport.

- Deux séances sont dédiées à ce laboratoire.
- Le rapport de laboratoire devra être :
  - concis et ne pas dépasser 15 pages (max. 1 page pour l'introduction et 1 page pour la conclusion).
  - remis **avant le début** du laboratoire 2
- Le rapport doit être remis sous format papier.
  - Une copie électronique doit être envoyée au chargé de laboratoire.
- Pénalité de 10% par jour de retard.
- Pénalité jusqu'à 15% pour un travail non professionnel (qualité du français, présentation du rapport, …).

Grille d'évaluation

Parties et Description	Pondération
Introduction (5 points)	
Introduction sur les objectifs du laboratoire et les différentes parties.	/5
Partie 1 – Analyse de *Samy* (20 points)	
Description de la méthode d'infection de tous les processus	/7
Description de l'approche qui permet d'éviter la réinfection de processus déjà infectés	/5
Description de l'injection HTTP	/8
Partie 2 – Analyse d'un ver *mass-mailer* (15 points)	
Description de la méthode d'infection	/3
Description de la méthode de propagation	/3
Description de la méthode de détection	/3
Description de la charge du ver (potentiel destructif)	/3
Documentation claire et exhaustive des étapes importantes	/3
Partie 3 – Analyse du script malicieux (20 points) - Difficile	
Code du logiciel malveillant	/5
Documentation claire et exhaustive des étapes importantes	/10
Description di mécanisme de protection du logiciel malveillant	/5
Partie 4 – Analyse du script malicieux (30 points)	
Découvrir les divers scripts	/5
Expliquer leur mode de fonctionnement	/10
Décrire les différents comportements des scripts dans au moins quatre (4) fureteurs ou versions de fureteurs différents.	/8
Décrire le mode de fonctionnement de *NoScript* (points forts et points faibles) – max. 1 page	/7
Partir 5 – Analyse mystère (5 points)	
Question 1	/2
Question 2	/3
Conclusion (5 points)	
Conclusion	/5