Université de Tlemcen Année Universitaire 2020-2021 Faculté des Sciences Département Informatique	Module Sécurité Informatique L3

TD2 Logiciels Malveillants

Exercice 1

- Quels sont les symptômes qui peuvent faire penser que votre ordinateur est infecté par un logiciel malveillant ?
- Votre ordinateur est infecté par un logiciel malveillant, mais votre antivirus ne le détecte pas, quels pourrait être les raisons ?
- Un logiciel malveillant (ver, virus, etc.) s'installe sur une machine, mais ne présente aucun signe d'atteinte aux données de l'utilisateur (vol de fichiers, destruction de fichiers, etc.). Selon vous, quel est son but donc ?
- Ma machine est déconnecté de tout réseau, est ce que je suis immunisé contre les logiciels malveillant ?
- Pourquoi une porte dérobée présente une opportunité pour un attaquant ? Comment peut-on détecter dans certains cas l'existence d'une porte introduite par un attaquant ?
- Un programme malveillant a comme charge utile d'exécuter une boucle infinie de création de processus avec fork (en C). Selon vous quel est son objectif ? quel besoin en sécurité a était affecté ?

Exercice 2

- Sur quels principes se fonde la réalisation d'attaques informatiques ?
- Quels sont les points communs entre un virus, un cheval de Troie, une bombe logique et un logiciel espion ?
- Qu'est-ce qu'un « ransomware » ?
- Parmi les infrastructures qui composent un système d'information laquelle ne peut être concernée par une attaque informatique ?
  A) Matérielle B) Réseau C) Logicielle D) Humaine E) Organisationnelle

- Parmi les attaques informatiques suivantes quelle est celle qui peut être qualifiée d'attaque passive ?
  A) Modification B) Interception C) Fabrication D) Interruption E) Destruction
- Les utilisateurs ne peuvent pas accéder à un serveur d'entreprise. Les journaux système indiquent que le serveur fonctionne lentement en raison du nombre élevé des fausses requêtes de service qu'il reçoit. De quelle technique d'attaque s'agit-il ?
- Un directeur du service informatique lance une compagne pour rappeler aux utilisateurs d'éviter d'ouvrir tout courriel d'origine suspecte. De quelle technique d'attaque le directeur du service d'informatique tente-t-il de protéger les utilisateurs ?
- Pourquoi et comment un pays peut être considéré comme un paradis digital ?

Exercice 3

Pour **attaquer un réseau** d'entreprise, l'attaquant envoie un message, à un utilisateur de ce réseau d'entreprise par le client de messagerie Outlook , grâce à des fichiers attachés contenant des programmes permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes chaque seconde à tous ces destinataires. Ce message reproduisait trop vite sur le réseau. De plus, tous ces messages ont créé une saturation au niveau de la bande passante, ce qui a obligé l'entreprise à arrêter les *connexions réseaux* pendant une journée.

1. De quel type d'attaque s'agit-t-il ?
2. Quelle est la technique d'attaque s'agit-t-il ?
3. Quel est l'objectif de *l'attaquant* ?
4. Quel type de programme d'infection s'agit-t-il ?

Corrigé type

Exercice 1

- Quels sont les symptômes qui peuvent faire penser que votre ordinateur est infecté par un logiciel malveillant ?
- ***Réponse :*** **ordinateur fonctionne au ralenti, PC est incontrôlable (**Des programmes démarrent ou se ferment automatiquement ? Impossible d'ouvrir certaines applications ? **), Internet ne fonctionne plus ou mal (**Un malware peut se connecter à des sites malveillants à votre insu et réduise ainsi la bande passante disponible. Le débit est alors fortement ralenti ou le réseau inaccessible**), Plus de trace de votre antivirus ou de votre firewall(**Votre antivirus a soudainement disparu et votre firewall a été désactivé sans votre intervention**), Impossible d'accéder à votre disque dur et/ou à vos périphériques, Votre ordinateur fonctionne seul(**Votre PC agit sans même votre intervention ou se bloque. Votre modem ou votre disque dur fonctionne sans raison apparente. Vous constatez que des emails ont été envoyés sans jamais les avoir rédigés, que des fenêtres web s'ouvrent ou se ferment d'elles-mêmes. Votre ordinateur s'éteint brusquement, redémarre sans arrêt ou ne démarre plus normalement. Il est probable qu'un logiciel malveillant en a pris possession.**)**

- Votre ordinateur est infecté par un logiciel malveillant, mais votre antivirus ne le détecte pas, quels pourrait être les raisons ?

  Réponse : *il s'agit d'*Un **virus polymorphe** qui est un **virus informatique** qui, lors de sa réplication, modifie sa représentation, ce qui empêche un logiciel antivirus de l'identifier par sa signature.
  Le virus n'est pas encore répertorié (ne contient pas la signature du virus dans sa base virale)
  Signature virus= suite d'octet permettant au virus de détecter si un fichier est déjà infecté

- Un logiciel malveillant (ver, virus, etc.) s'installe sur une machine, mais ne présente aucun signe d'atteinte aux données de l'utilisateur (vol de fichiers, destruction de fichiers, etc.). Selon vous, quel est son but donc ?
  Réponse *: utiliser ma machine pour attaquer d'autres machines*

- Ma machine est déconnecté de tout réseau, est ce que je suis immunisé contre les logiciels malveillant ?

  Réponse : *non car elle peut être infectée via un disque amovible déjà infecté*

- Pourquoi une porte dérobée présente une opportunité pour un attaquant ? Comment peut-on détecter dans certains cas l'existence d'une porte introduite par un attaquant ?

Réponse : *car elle lui permet de prendre le contrôle de la machine à distance à l'insu de l'utilisateur légitime*

Détection : Soit analyser (avec un sniffeur IP) les flux réseaux générés par l'application vers l'extérieur (internet), ce qui au demeurant ne sera efficace que si le tiers accède au système pendant les opérations de surveillance réseau.

Soit analyser le fonctionnement interne des logiciels. Pour ce faire, il est nécessaire de lire le code source ce qui requiert des connaissances pointues en programmation informatique. En réalité le code source n'est rendu public que pour les logiciels libres (*open source*) ; pour les autres logiciels, dits « propriétaires », l'analyse sera précédée d'une phase de rétro-ingénierie (*reverse engineering*), c'est-à-dire de la décompilation permettant d'obtenir un code source reconstitué, cette pratique est non seulement complexe (le code obtenu étant non documenté) mais de plus contrevient aux dispositions contractuelles des licences utilisateurs

- Un programme malveillant a comme charge utile d'exécuter une boucle infinie de création de processus avec fork (en C). Selon vous quel est son objectif ? quel besoin en sécurité a était affecté ?

Réponse : *charger le CPU, objectif affecté : disponibilité*

Exercice 2

- Sur quels principes se fonde la réalisation d'attaques informatiques ?

Réponse : La réalisation d'attaques informatiques se fonde sur le leurre, l'usage abusif des technologies, l'exploitation des failles et vulnérabilités, l'usurpation d'identité

- Quels sont les points communs entre un virus, un cheval de Troie, une bombe logique et un logiciel espion ?

Réponse : Il s'agit de logiciels malveillants dont la charge et le mode de réalisation varient en fonction de la finalité. Un cheval de Troie ne se duplique pas, tandis que la réplication caractérise un virus. Une bombe logique est un virus dont la charge malveillante se déclenche à une date ou selon un événement particulier.

- Qu'est-ce qu'un « ransomware » ?

Réponse : est un logiciel malveillant qui prend en otage des données personnelles

- Parmi les infrastructures qui composent un système d'information laquelle ne peut être concernée par une cyberattaque ?
  B) Matérielle B) Réseau C) Logicielle D) Humaine E) Organisationnelle

Réponse : E

- Parmi les attaques informatiques suivantes quelle est celle qui peut être qualifiée d'attaque passive ?
  A) Modification B) Interception C) Fabrication D) Interruption E) Destruction

Réponse : B

- Les utilisateurs ne peuvent pas accéder à un serveur d'entreprise. Les journaux système indiquent que le serveur fonctionne lentement en raison du nombre élevé des fausses requêtes de service qu'il reçoit. De quelle technique d'attaque s'agit-il ?

Réponse : Dos

- Un directeur du service informatique lance une compagne pour rappeler aux utilisateurs d'éviter d'ouvrir tout courriel d'origine suspecte. De quelle technique d'attaque le directeur du service d'informatique tente-t-il de protéger les utilisateurs ?

Réponse : hameçonnage ou phishing

- Pourquoi et comment un pays peut être considéré comme un paradis digital ?

Réponse : quand dans un pays, il n'existe pas de cadre légal applicable condamnant les actions cybercriminelles, un système de justice et de police efficace pour lutter contre la cybercriminalité, ce pays est qualifié de paradis digital (à l'instar des paradis fiscaux). Ainsi des serveurs hébergés dans de tels pays peuvent piloter des réseaux de botnet, héberger des logiciels malveillants, propager des virus et des spams… sans que leurs auteurs soient inquiétés par la justice. De tels serveurs sont qualifiés de « bullet free » car aucun policier ne viendra déloger les programmes ou les données sauvegardés dans ces serveurs. Pourquoi : par inconscience, par incompétence, par rentabilité économique, par corruption, par manque de moyens et de volonté politique.

Exercice 3

1. De quel type d'attaque s'agit-t-il ? ingénierie sociale
2. Quelle est la technique d'attaque s'agit-t-il ? hameçonnage
3. Quel est l'objectif de *l'attaquant* ? perturber le bon fonctionnement du réseau, saturer le réseau (disponibilité affectée)
4. Quel type de programme d'infection s'agit-t-il ? ver