Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

Sécurité des Usages TIC

Examen — mai 2015

Durée : 2h — Tous documents autorisés

1 – 6pts Article paru dans CNETFrance :

Lenovo : Superfish, un logiciel de publicité indésirable incrusté dans le système

Le fabricant chinois avoue installer au sein de ses systèmes un programme qui affiche des publicités dans les pages web, il pourrait également poser problème sur les connexions sécurisées.

Par Guillaume Bonvoisin @gbonvoisin
jeudi 19 février 2015 à 14:58

Ce n'est pas nouveau, les fabricants d'ordinateurs qui préinstallent Windows sur leurs machines modifient le système pour y ajouter des logiciels : les bloatware. Personnalisation, auto-promotion, logiciel tiers... etc, ces ajouts sont aussi gênants pour l'utilisateur que pénalisant pour la rapidité du système. Aujourd'hui c'est Superfish, un logiciel intégré par Lenovo qui est au cœur d'une polémique.
En plus d'afficher de la publicité, il pourrait poser des problèmes avec la sécurité.

Interception des connexions sécurisées
Le problème ne se situe pas seulement au niveau du comportement publicitaire indésirable mais pourrait également poser problème au niveau de la sécurité des connexions. Techniquement, pour afficher ces publicités, Superfish intercepte les connexions SSL/TLS pour imposer ses propres certificats, même dans le cas de connexion à un site bancaire, une information confirmée par un spécialiste de la sécurité Google. Si la connexion sécurisée est bien maintenue, le comportement nommée dans la sécurité informatique comme "attaque de l'homme du milieu" (man in the middle attack ou MITM), est inquiétant.

a. Quelles sont les avantages pour Lenovo d'utiliser SuperFish ? *(0,5pt)*

b. Pourquoi un «spécialiste de la sécurité Google» est-il concerné par cette attaque ? *(0,5pt)*

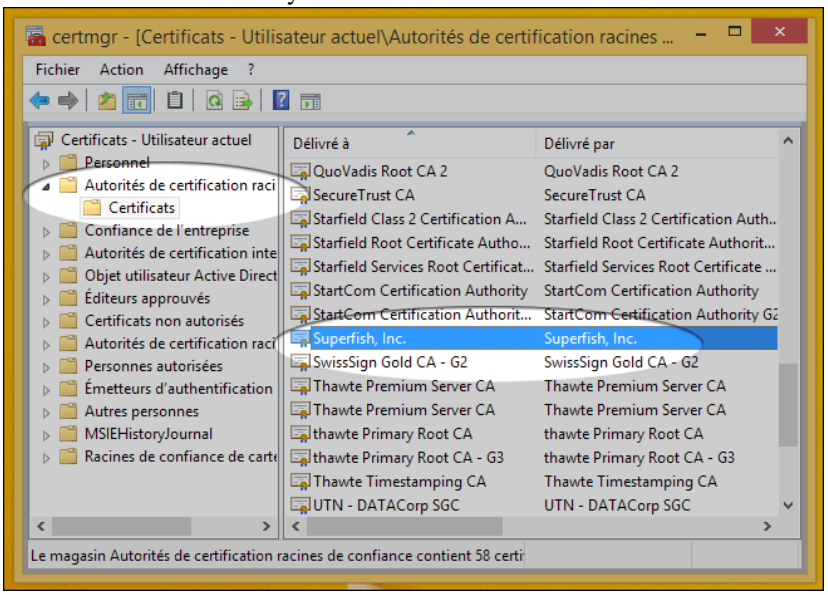
c. Quels critères parmi les «DICT» sont touchés par cette attaque ? *(1pt)*

d. L'outil s'appellant «SuperFish», y a-t-il un lien avec le «*phishing*» ? *(1pt)*
Justifiez votre réponse

e. Décrivez techniquement le déroulement de l'attaque quand l'utilisateur charge une page sécurisée par SSL dans son navigateur et qu'il obtient cette page avec un contenu publicitaire choisi par Lenovo. *(1,5pts)*

f. Décrivez une solution logicielle de «*test de vulnérabilité*» qui pourrait permettre de détecter une attaque MITM sur SSL telle que décrite dans «l'attaque Superfish». Vous préciserez les données et les éventuelles connexions réseau nécessaires à sa mise en œuvre. *(1,5pts)*

2 – Le certificat suivant a été trouvé dans le système d'une victime :
4pts



a. Comment ce certificat a-t-il pu être installé dans le système ? *(1pt)*

b. Quelle est la nature de ce certificat et quels sont ses usages ? *(1pt)*

c. Comment Windows peut-il le «désactiver» ? *(1pt)*

d. Est-ce que deux certificats appartenant à la même entité peuvent être «valides» simultanément ? *(1pt)*

3 – Entropie
6pts

a. Donnez en une définition. *(1pt)*

b. Comment intervient-elle en cryptographie : *(1pt)*
   - ◇ symétrique ?
   - ◇ asymétrique ?

c. À quelle(s) étape(s) du déroulement d'un protocole de communication sécurisé doit-elle être prise en compte ? *(1pt)*

d. Comment contribue-t-elle à la réussite d'attaques ? *(1pt)*

e. Donnez un exemple de procédé technique **augmentant** cette entropie. *(1pt)*

f. Donnez un exemple de procédé technique **diminuant** cette entropie. *(1pt)*

4 – Questions diverses :
4pts

a. Expliquez le «SALT» et ses avantages. *(1pt)*

b. Dans l'objectif d'une analyse de risque, comparez une PKI avec une solution de type Kerberos ? *(2pts)*
Vous vous limiterez aux critères DICT.

c. Dans l'envoi d'un courrier est-il préférable de «chiffrer puis compresser» ou de «compresser puis chiffrer» ? *(1pt)*