ANALYSE DE MALWARE

EXERCICE 1 :

Afin de comprendre le comportement d'un malware, nous vous fournissons la capture Wireshark *capture-mal.pcap*. Cette capture provient d'une vraie analyse après une attaque d'une entreprise.

Attention : Etant donné que ce malware infecte uniquement les plateformes Windows, il est fortement conseillé de réaliser cette partie sous Linux ou MacOS.

1. Faites analyser le fichier de capture par le site VirusTotal. Quel est le résultat ?
2. Afin de faciliter l'analyse de la capture, faire un filtre sur Wireshark afin de ne garder que les colonnes *Time, Destination Address, Destination Port, Host et Info*.
3. Quelle est l'adresse IP de l'hôte infecté ?
4. Sur quels ports est échangé le trafic HTTPS et HTTP ?
5. Quel est le nom de domaine DNS contacté par malware ? que trouve-t-on dans le fichier téléchargé à partir de ce site ?
6. Trouver l'exécutable envoyé à la victime. Comment confirmer que c'est bien un fichier en .exe ?
7. Identifier les différentes tentatives de connexions après l'infection. Expliquer.
8. Le malware identifie l'adresse IP de la victime en contactant un site public. Lequel ? pourquoi cette vérification ?
9. Maintenant, le malware commence à voler et à transmettre des données de la victime vers un site distant.
    a. Quel est l'adresse et le port d'écoute de ce site ?
    b. Quelles sont les informations volées ?
10. Le malware envoie à la victime plusieurs images terminant en .png. Que trouve-t-on réellement dans ces fichiers ? Pourquoi faire et à quoi servent ces fichiers ?

EXERCICE 2 :

Chercher sur Internet des informations sur le Malware Trickbot, puis répondre aux questions suivantes :

1. A quel date le malware **Trickbot** est-il apparu ? De quel type il est ? Quel est son domaine d'action ?
2. Quels sont les dégâts possibles qui peuvent être causés par ce malware ?
3. Quelle est la méthode de diffusion la plus courante de ce Malware ?
4. Quelles sont les techniques utilisées pour inciter l'utilisateur à ouvrir le document infecté ?
5. Est-ce que ce malware peut-il faire des dégâts si l'utilisateur infecté n'est pas admin ?