LAB2 : CYBERATTACK ANALYSIS

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 Virus Total. 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. Après avoir réussi une connexion SSL, un certificat est transmis à la victime. Que remarquez-vous d'anormal dans le certificat ?
9. Le malware identifie l'adresse IP de la victime en contactant un site public. Lequel ? pourquoi cette vérification ?
10. 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 ?
11. 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 ?