Travaux pratiques – Recherche d'emploi dans le domaine de la cybersécurité (version de l'instructeur)

**Remarque à l'intention de l'instructeur**: le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

1. Objectifs

Rechercher et analyser des malwares

1. Contexte/scénario

Les malwares ou programmes malveillants désignent une variété de logiciels malveillants qui peuvent être utilisés pour causer des dommages aux systèmes informatiques, voler des données et contourner les mesures de sécurité. Les malwares peuvent également attaquer les infrastructures stratégiques, désactiver les services d'urgence, entraîner la fabrication de produits défectueux sur les chaînes de montage, désactiver des générateurs électriques et perturber les services de transport. Les experts en sécurité estiment que plus d'1 million de nouveaux malwares sont diffusés chaque jour. Selon un [rapport](http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf) de McAfee Labs, on recensait près de 500 millions de malwares connus fin 2015.

**Remarque** : vous pouvez utiliser le navigateur web de la machine virtuelle installée lors d'un TP précédent pour analyser les problèmes de sécurité. En utilisant la machine virtuelle, vous évitez d'infecter votre ordinateur avec des malwares.

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet

1. Rechercher des malwares récents
   * 1. Recherchez des malwares récents à l'aide de votre moteur de recherche préféré. Au cours de votre recherche, choisissez quatre exemples de malware, chacun d'un type différent et notez ce qu'ils font, comment ils sont transmis et leur impact, puis préparez une présentation de vos résultats.

Voici quelques types de malware : cheval de Troie, canular, logiciel publicitaire, malware, PUP, exploit et vulnérabilité. Vous trouverez ci-dessous certains sites web susceptibles de vous être utiles dans votre recherche :

[McAfee](https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard.html)

[Malwarebytes](https://blog.malwarebytes.com/threats/)

[SecurityWeek](http://www.securityweek.com/virus-threats/virus-malware)

[TechNewsWorld](http://www.technewsworld.com/perl/section/viruses-malware/)

* + 1. Lisez les informations sur les malwares trouvés au cours de votre recherche à l'étape 1a, choisissez-en un et rédigez un résumé qui explique son mode d'action, son mode de transmission et son impact.

**Les chevaux de Troie sont des malwares sournois qui utilisent la ruse pour infecter les systèmes. En se faisant passer pour des logiciels légitimes, ils trompent les utilisateurs pour les inciter à les installer. Une fois infiltrés, ils ouvrent une porte dérobée, offrant aux attaquants un accès distant au système. Leur mode de transmission peut inclure des pièces jointes de courriels et des téléchargements depuis des sources non fiables. Les impacts vont de la collecte de données à la perturbation des opérations normales du système.**