Diplôme : Bac Pro Ciel			Option : Ciel
Nom:	Prénom:	Classe:	Date:

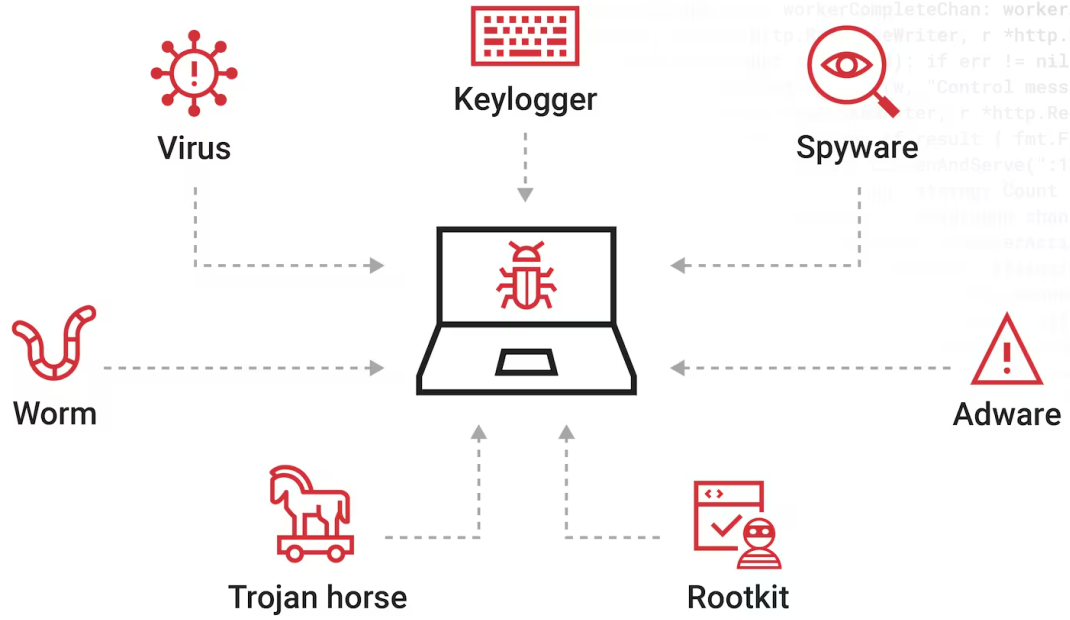
0 — 1 an — 2 ans — 3 ans

TP Cybersécurité : Les logiciels malveillants

Sous-thème : les programmes malveillants et la protection du poste de travail

Objectifs du TP

- Définir un logiciel malveillant et distinguer ses familles : virus, ver, cheval de Troie, rançongiciel, logiciel espion, botnet.
- Expliquer les modes de propagation d'un malware et reconnaître les signes d'une infection. - Appliquer les mesures de protection d'un poste de travail (mises à jour, antivirus, pare-feu, sauvegardes, bonnes pratiques).
- Connaître la procédure de réaction et de signalement en cas d'infection (réflexe professionnel CIEL).

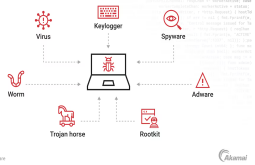


Types of malware

Akamai

BOUNGAB

TP Cybersécurité
Les logiciels malveillants



Activité 1 — Le cours à compléter

Complète les pointillés avec les mots de la transcription de la vidéo. Mots à placer :

nuire • lucratif • hôte • fichier en fichier • humaine • faille technique • 90 % • 10 minutes • accès permanent non autorisé • clés USB • pare-feu • sauvegardes • infrastructures • à l'insu

1. Un logiciel malveillant (malware) est un logiciel créé dans le but de ..... .

2. Autrefois, les virus effaçaient les données et empêchaient l'ordinateur de démarrer ; aujourd'hui, le but est surtout ..... : voler et exploiter les données.

3. Un virus est un programme pirate installé ..... de l'utilisateur : il est caché et exerce un contrôle sur les ressources de la machine.

4. Comme son homologue biologique, le virus a besoin d'un ..... : on s'infecte en cliquant un fichier ou en exécutant un programme, puis il se propage de ..... .

5. Un ver, lui, n'a besoin d'aucune intervention ..... : il exploite une ..... pour se copier de machine en machine.

6. Le ver Slammer, le 25 janvier 2003, a infecté ..... des ordinateurs vulnérables en seulement ..... .

7. Un cheval de Troie se cache dans un logiciel d'apparence légitime et crée un ..... à la machine : l'attaquant accède quand il veut aux fichiers, au carnet d'adresses et aux mots de passe.

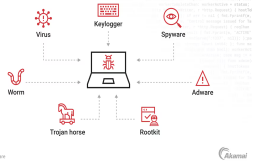
8. Les chemins de l'infection sont multiples : Internet, mais aussi les DVD, les ..... , les e-mails et les fichiers joints.

9. Pour se protéger : mettre à jour le système et les logiciels, installer un antivirus et un ..... , ne pas ouvrir les pièces jointes suspectes et faire des ..... régulières.

10. Les conséquences d'une attaque : perte de données, destruction de programmes, arrêt des ..... , vol de documents confidentiels et perte de réputation.

BOUNGAB

TP Cybersécurité
Les logiciels malveillants



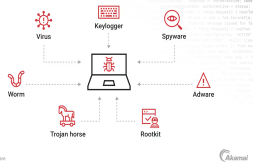
Activité 2 — Je complète le glossaire (étape 3 du cours)

Écris la définition de chacun des 8 termes ci-dessous (avec un exemple quand c'est possible) :

- **Logiciel malveillant (malware)**
- **Virus**
- **Ver (worm)**
- **Cheval de Troie (trojan)**
- **Rançongiciel (ransomware)**
- **Logiciel espion (spyware / keylogger)**
- **Botnet (ordinateur zombie)**
- **Antivirus et mises à jour**

BOUNGAB

TP Cybersécurité
Les logiciels malveillants



Activité 3 — Je complète le glisser-déposer (étape 5 du cours)

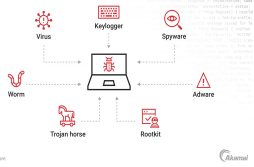
Replace les 10 termes techniques dans les bonnes phrases :

logiciel malveillant • virus • ver • cheval de Troie • rançongiciel • logiciel espion • botnet • mise à jour • antivirus • sauvegarde

- Un ..... est un programme conçu pour nuire à ton ordinateur.
- Un ..... a besoin qu'un fichier soit exécuté pour se propager.
- Un ..... se propage tout seul par le réseau, en exploitant une faille.
- Un ..... se cache dans un logiciel d'apparence légitime.
- Un ..... chiffre les fichiers et réclame une rançon.
- Un ..... enregistre tes frappes au clavier et tes données.
- Un ..... est un réseau d'ordinateurs zombies contrôlés à distance.
- Une ..... corrige les failles de sécurité du système.
- Un ..... détecte et supprime les programmes malveillants.
- La ..... permet de restaurer tes fichiers après une attaque.

BOUNGAB

TP Cybersécurité
Les logiciels malveillants



Activité 4 — Je rédige le résumé (étape 9 du cours)

Complète ce résumé avec tes propres mots :

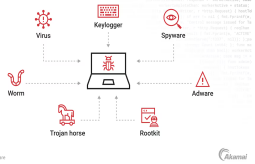
- Un logiciel malveillant, c'est .....
- Les principales familles de malwares sont .....
- On s'infecte surtout par .....
- Les signes qui doivent m'alerter sont .....
- Pour protéger mon poste de travail, je dois .....
- Si un poste est infecté, je dois .....
- En entreprise (réflexe professionnel CIEL), je dois .....

Activité 5 — Questions ouvertes d'approfondissement (étape 8 du cours)

1. Explique avec tes mots ce qu'est un logiciel malveillant et cite trois exemples différents.

BOUNGAB

TP Cybersécurité
Les logiciels malveillants



2. Quelle est la différence entre un virus et un ver ? Explique comment chacun se propage.

3. Ton camarade a téléchargé un jeu « craqué » : son ordinateur est très lent et des fenêtres s'ouvrent seules. Décris ce qui a pu se passer et ce qu'il doit faire.

4. Pourquoi les mises à jour et les sauvegardes sont-elles les meilleures protections contre les rançongiciels ?

5. Dans une entreprise, quel est le rôle du technicien informatique face à un poste infecté ? Cite trois actions professionnelles.

BOUNGAB

FICHE SYNTHESE

TP Cybersécurité — Les logiciels malveillants



➢ **A RETENIR** *Compléter*

Aide-mémoire — à retenir

Les 6 réflexes qui protègent un poste de travail :
1. Je mets à jour le système et les logiciels (les mises à jour corrigent les failles exploitées par les malwares).
2. Je garde un antivirus ET un pare-feu actifs et à jour : un antivirus périmé ne sert à rie
3. Je ne télécharge que sur les sites officiels (jamais de logiciels « craqués » ni de faux jeux
4. Je n'ouvre pas les pièces jointes ni les liens d'un message inhabitue
5. Je fais des sauvegardes régulières : c'est la seule vraie parade contre un rançongicie
6. Je ne me fie jamais à l'icône ou au nom d'un fichier : un logiciel malveillant sait se cache

Un poste est infecté ? (réflexe professionnel CIEL)
- J'isole la machine du réseau (je débranche le câble / je coupe le Wi-Fi) sans l'éteindre brutalement.
- Je préviens immédiatement mon enseignant ou le référent informatique : je ne cache rien.
- Je consigne l'incident (heure, symptômes, fichiers concernés) sur la fiche de suivi.
- Je lance une analyse antivirus, puis je restaure une sauvegarde saine si nécessaire.
- Je ne paye JAMAIS de rançon et je signale sur cybermalveillance.gouv.fr

BOUNGAB