Nom : _____ Date : _____ Note : _____

# Analyse des logiciels malveillants et atténuation des menaces Guide

Chevaux de Troie, rançongiciels, logiciels espions, rootkits, bacs à sable de virtualisation, confinement

## ANALYSE DES LOGICIELS MALVEILLANTS : PRÉSENTATION

**SÉCURISÉ**
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

**CONFORME**
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

**ZERO TRUST**
POLITIQUE D'ACCÈS
Authentification multifacteur

**Bienvenue !** Ce dossier d'activités vous guide à travers l'analyse et la prévention des logiciels malveillants. Vous étudierez les logiciels espions, les chevaux de Troie, les charges utiles des rançongiciels, les outils de rétro-ingénierie, le comportement des rootkits et les stratégies de confinement.

### POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

**Ouvrir le guide VPN.com de la cybersécurité**

URL: https://www.vpn.com/fr/cybersecurite/malware/

# Votre parcours d'apprentissage : atténuation des logiciels malveillants

- Distinguer les types de logiciels malveillants : cheval de Troie, ver et rootkit.
- Mettre en œuvre une exécution virtualisée en bac à sable (sandbox) pour l'analyse du code.
- Concevoir des plans de confinement et d'assainissement face à des charges de rançongiciels actives.

## GUIDE D'ANALYSE DES LOGICIELS MALVEILLANTS : CONSIGNES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à l'atténuation des logiciels malveillants. Terminez par l'activité bonus Réflexion rapide.

## ANALYSE DES LOGICIELS MALVEILLANTS ET CONFINEMENT DES MENACES (INTRODUCTION)

Les codes malveillants comme les chevaux de Troie, les vers et les rançongiciels représentent des menaces à fort impact pour les terminaux et les serveurs. Les équipes de sécurité analysent les logiciels malveillants dans des bacs à sable virtuels et appliquent rapidement des mesures d'isolement réseau pour contenir la propagation de la charge malveillante.

**LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.**

## Point de contrôle 1 : Défi QCM

**1. Quelle est la caractéristique déterminante d'un cheval de Troie ?**

- A. Il se fait passer pour un logiciel légitime afin d'amener les utilisateurs à l'exécuter
- B. Il se réplique automatiquement sur les lignes du réseau local
- C. Il infecte les fichiers à l'intérieur de bacs à sable virtuels isolés
- D. Il intercepte le trafic du fournisseur d'accès à Internet

**2. Quel type de logiciel malveillant chiffre les fichiers et exige un paiement ?**

- A. Rançongiciel
- B. Logiciel espion
- C. Rootkit
- D. Logiciel publicitaire

**3. Qu'est-ce qui correspond à un logiciel espion ?**

- A. Logiciel malveillant conçu pour surveiller en secret les frappes au clavier et l'activité du navigateur
- B. Code de programme s'exécutant dans un conteneur virtuel isolé (bac à sable)
- C. Mises à jour anti-malware téléchargées depuis des registres de bases de données
- D. Réglage automatique de la luminosité de l'écran

**4. Pourquoi les développeurs de logiciels malveillants utilisent-ils des rootkits ?**

- A. Cacher les processus actifs et les fichiers malveillants au système d'exploitation
- B. Augmenter la vitesse de traitement du processeur sur les terminaux
- C. Pour sauvegarder les fichiers de base de données dans des coffres cloud sécurisés
- D. Pour améliorer l'autonomie de la batterie des ordinateurs portables

**5. Que signifie le sandboxing dans l'analyse des logiciels malveillants ?**

- A. Exécuter les fichiers suspects dans un coffre virtuel isolé pour observer leur comportement en toute sécurité
- B. Comparer les empreintes des fichiers aux bases de données de menaces connues
- C. Restaurer les sauvegardes de base de données après une intrusion
- D. Déconnecter les routeurs du réseau local des lignes publiques

## Point de contrôle 2 : Défi Vrai ou Faux

### 6 Question 6

6. Les vers informatiques ont besoin d'une action humaine pour se propager sur les réseaux locaux.

- ◯ Vrai
- ◯ Faux

### 7 Question 7

7. Les logiciels publicitaires (adware) sont toujours inoffensifs et ne suivent ni le comportement des utilisateurs ni l'historique du navigateur.

- ◯ Vrai
- ◯ Faux

### 8 Question 8

8. Restaurer des sauvegardes hors ligne saines permet aux victimes de récupérer leurs fichiers chiffrés sans payer la rançon.

- ◯ Vrai
- ◯ Faux

### 9 Question 9

9. Un antivirus à signatures arrête de manière fiable un logiciel malveillant zero-day avant même qu'une signature n'existe pour lui.

- ◯ Vrai
- ◯ Faux

### 10 Question 10

10. Les logiciels malveillants sans fichier exécutent des scripts malveillants dans la mémoire du système, sans écrire de fichiers sur le disque.

- ◯ Vrai
- ◯ Faux

## Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Un logiciel malveillant déguisé en utilitaire inoffensif est un _____ .

2. Les charges malveillantes qui verrouillent les systèmes de bases de données contre de l'argent relèvent du _____ .

3. Les enregistreurs de frappe qui capturent secrètement les mots de passe sont un type de _____ .

4. Se dissimuler au cœur du noyau du système d'exploitation nécessite un _____ .

5. Analyser des fichiers suspects dans un coffre isolé fait appel à un _____ virtuel.

6. Stopper la propagation de charges malveillantes actives exige un _____ immédiat du réseau.

**BANQUE DE MOTS DE VOCABULAIRE**

BAC À SABLE | CHEVAL DE TROIE | CONFINEMENT | LOGICIEL ESPION | RANÇONGICIEL | ROOTKIT | SANS FICHIER | VER INFORMATIQUE

**Écrivez vos réponses ici :**

1. 
2. 
3. 
4. 
5. 
6. 

# Point de contrôle 4 : Association de notions sur la sécurité

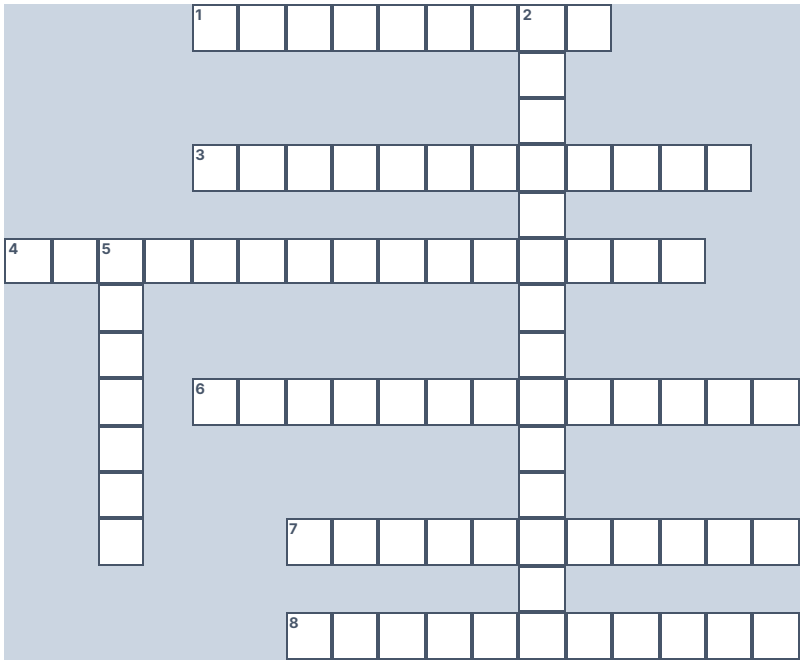
## ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

| | | | |
|---|---|---|---|
| ☐ | 1. CHEVAL DE TROIE | A | Programme conçu pour surveiller et enregistrer secrètement l'activité et les saisies de l'utilisateur. |
| ☐ | 2. RANÇONGICIEL | B | Logiciel malveillant s'exécutant directement en RAM pour échapper aux analyseurs de disque. |
| ☐ | 3. LOGICIEL ESPION | C | Confinement des terminaux infectés pour empêcher la propagation des charges malveillantes. |
| ☐ | 4. ROOTKIT | D | Logiciel malveillant déguisé en programme utilitaire inoffensif ou utile. |
| ☐ | 5. BAC À SABLE | E | Logiciel malveillant auto-réplicatif qui se propage sur les réseaux sans intervention humaine. |
| ☐ | 6. CONFINEMENT | F | Logiciel malveillant qui chiffre le stockage du système et exige un paiement pour fournir la clé. |
| ☐ | 7. VER | G | Environnement virtuel isolé utilisé pour analyser des fichiers malveillants en toute sécurité. |
| ☐ | 8. SANS FICHIER | H | Logiciel malveillant furtif qui se cache au cœur du noyau du système pour conserver le contrôle administrateur. |

## Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.




### HORIZONTALEMENT

**1. Environnement virtuel isolé servant à analyser des fichiers malveillants en toute sécurité. (9)**

**3. Logiciel malveillant qui chiffre le stockage du système et exige un paiement en échange de la clé. (12)**

**4. Logiciel malveillant auto-répliquant qui se propage sur les réseaux sans intervention humaine. (15)**

**6. Logiciel malveillant déguisé en utilitaire inoffensif ou utile. (13)**

**7. Logiciel malveillant qui s'exécute directement en RAM pour échapper aux analyseurs de disque. (11)**

**8. Restriction des terminaux infectés pour empêcher la propagation des charges malveillantes. (11)**

### VERTICALEMENT

**2. Programme conçu pour surveiller et enregistrer secrètement l'activité et les saisies de l'utilisateur. (14)**

**5. Logiciel malveillant furtif dissimulé au cœur du noyau du système pour conserver un contrôle administrateur. (7)**

# Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

## HORIZONTALEMENT

**1 horizontal: Environnement virtuel isolé servant à analyser des fichiers malveillants en toute sécurité. (9 lettres):**

**3 horizontal: Logiciel malveillant qui chiffre le stockage du système et exige un paiement en échange de la clé. (12 lettres):**

**4 horizontal: Logiciel malveillant auto-répliquant qui se propage sur les réseaux sans intervention humaine. (15 lettres):**

**6 horizontal: Logiciel malveillant déguisé en utilitaire inoffensif ou utile. (13 lettres):**

**7 horizontal: Logiciel malveillant qui s'exécute directement en RAM pour échapper aux analyseurs de disque. (11 lettres):**

**8 horizontal: Restriction des terminaux infectés pour empêcher la propagation des charges malveillantes. (11 lettres):**

## VERTICALEMENT

**2 vertical: Programme conçu pour surveiller et enregistrer secrètement l'activité et les saisies de l'utilisateur. (14 lettres):**

**5 vertical: Logiciel malveillant furtif dissimulé au cœur du noyau du système pour conserver un contrôle administrateur. (7 lettres):**

## Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

E A F O K N D V N C D H I B A
I P R L P T W E T I L Y F Y S
O G X W H I F R R T O N U K R
R D T S C K L I P L G M L S H
T K S P O T H N Y P I L E W U
E N A Y N O Q F Q B C A I L B
D P N M F O B O L I I F C I A
L N S Y I R B R Z Z E Y I B C
A N F V N X M M C F L P G W A
V Q I Q E X H A E Y E C N W S
E L C F M G H T Z W S C O O A
H R H J E X X I R K P Z C A B
C N I R N Z R Q M G I S N W L
G L E W T J B U Y C O C A Y E
O U R Z O Z U E T B N H R V P

**LISTE DE MOTS DE VOCABULAIRE**

CHEVALDETROIE RANCONGICIEL LOGICIELESPION ROOTKIT BACASABLE
CONFINEMENT VERINFORMATIQUE SANSFICHIER

## Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

| TERMES DE VOCABULAIRE |
| --- |
| A. CHEVALDETROIE |
| B. RANCONGICIEL |
| C. LOGICIELESPION |
| D. ROOTKIT |
| E. BACASABLE |
| F. CONFINEMENT |
| G. VERINFORMATIQUE |
| H. SANSFICHIER |

| DÉFINITIONS ET CHAMPS D'ASSOCIATION |
| --- |
| _____ 1. Logiciel malveillant furtif dissimulé au cœur du noyau du système pour conserver un contrôle administrateur. |
| _____ 2. Restriction des terminaux infectés pour empêcher la propagation des charges malveillantes. |
| _____ 3. Logiciel malveillant qui s'exécute directement en RAM pour échapper aux analyseurs de disque. |
| _____ 4. Logiciel malveillant auto-répliquant qui se propage sur les réseaux sans intervention humaine. |
| _____ 5. Logiciel malveillant qui chiffre le stockage du système et exige un paiement en échange de la clé. |
| _____ 6. Programme conçu pour surveiller et enregistrer secrètement l'activité et les saisies de l'utilisateur. |
| _____ 7. Logiciel malveillant déguisé en utilitaire inoffensif ou utile. |
| _____ 8. Environnement virtuel isolé servant à analyser des fichiers malveillants en toute sécurité. |

## Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. DETILHERCOE AV
2. COIGEOLILNS PEI
3. BASABEALC
4. OUTIEMAFER QIVRN
5. AIIGLNOCNRE C
6. IOKRTTO
7. MICOETENNN F
8. ICRINSFAEHS

# Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

| | | | | |
|---|---|---|---|---|
| 1 | Endroits où télécharger des applications sûres | | | |
| 2 | Appareils qui peuvent être piratés | | | |
| 3 | Choses que vous sauvegardez | | | |
| 4 | Signaux d'alerte dans un e-mail | | | |
| 5 | Signes qu'un téléphone contient un logiciel malveillant | | | |
| 6 | Types de logiciels malveillants que vous connaissez | | | |
| 7 | Types de fichiers dont il faut se méfier | | | |
| 8 | Façons dont un logiciel malveillant arrive sur un PC | | | |
| 9 | Bonnes habitudes de sécurité à adopter dès aujourd'hui | | | |
| 10 | Mots liés à la cybersécurité | | | |
| 11 | Choses à faire après une fuite de données | | | |
| 12 | Raisons de mettre à jour les logiciels | | | |
| 13 | Animaux ou personnages dont le nom évoque un logiciel malveillant | | | |
| 14 | Choses qu'un logiciel malveillant peut voler | | | |
| 15 | Choses à faire si vous avez cliqué sur le mauvais lien | | | |

# Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

## ÉTUDE DE CAS 1 : CONFINEMENT D'UNE CHARGE DE RANÇONGICIEL EN ENTREPRISE



**Scénario : le réseau local d'une entreprise a été compromis par un rançongiciel actif.** Sur des serveurs de fichiers clés, des fichiers commencent à apparaître avec l'extension .locked. Établissez des politiques de confinement.

**Question de discussion :** Détaillez les étapes de confinement et décrivez le protocole de récupération des données.

## ÉTUDE DE CAS 2 : INJECTION EN MÉMOIRE D'UN MALWARE SANS FICHIER



**Scénario :** Un analyste détecte, à l'aide d'outils d'administration standard, des schémas de scripts suspects qui s'exécutent directement dans la RAM volatile du système, alors qu'aucun fichier malveillant n'existe sur le disque.

**Question de discussion :** Expliquez la stratégie d'analyse de la mémoire et précisez les outils permettant de bloquer l'exécution sans fichier.

## Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

**CLÉ DE CHIFFREMENT LETTRE-CHIFFRE**

**A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10**

**K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20**

**U=21 V=22 W=23 X=24 Y=25 Z=26**

| 4 | 5 | 20 | 5 | 3 | 20 | 5 | 26 | | 12 | 5 | 19 | | 3 | 8 | 1 | 18 | 7 | 5 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | |

| 16 | 1 | 18 | | 1 | 14 | 1 | 12 | 25 | 19 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

| 3 | 15 | 13 | 16 | 15 | 18 | 20 | 5 | 13 | 5 | 14 | 20 | 1 | 12 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | |

**Message déchiffré :**

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

# Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

### Q1: Qu'est-ce qu'un logiciel malveillant ?

Logiciel malveillant conçu par des acteurs malveillants pour endommager, détourner ou voler des données sur des appareils et des réseaux.

### Q2: Quelle est la différence entre un virus et un ver ?

Un virus a besoin d'une action humaine (comme l'ouverture d'un fichier) pour se propager, alors qu'un ver se propage automatiquement sur les réseaux.

### Q3: Comment un cheval de Troie infecte-t-il un ordinateur ?

Il trompe les utilisateurs en se faisant passer pour un programme inoffensif ou sûr, tout en dissimulant sa charge malveillante à l'intérieur.

### Q4: Qu'est-ce qu'un rançongiciel ?

Un type de logiciel malveillant qui chiffre les fichiers du système ciblé et exige un paiement en échange de la clé de déchiffrement. [1]

### Q5: Qu'est-ce qu'un logiciel espion ?

Logiciel malveillant qui enregistre secrètement les frappes au clavier, les mots de passe et les habitudes de navigation de l'utilisateur pour les envoyer aux attaquants.

# Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

### Q6: Que signifie le sandboxing ?

Exécution de fichiers suspects dans un environnement virtuel sécurisé et isolé afin d'observer leur comportement sans risque pour les systèmes de production.

### Q7: Qu'est-ce qu'un logiciel malveillant sans fichier ?

Logiciel malveillant qui s'exécute directement dans la mémoire système (RAM) en utilisant des utilitaires légitimes, sans écrire de fichiers sur le disque, afin de contourner les analyseurs de base.

### Q8: Comment un rootkit protège-t-il un logiciel malveillant ?

Il dissimule des processus et des fichiers malveillants, souvent en détournant le noyau du système d'exploitation, de sorte que les antivirus peuvent ne pas les détecter.

### Q9: Qu'est-ce que la surveillance dynamique des comportements ?

Analyse antivirus qui surveille les processus actifs en temps réel afin de bloquer les actions typiques des logiciels malveillants, comme le chiffrement massif de fichiers.

### Q10: Pourquoi le confinement est-il urgent lors de la réponse à un incident ?

Isoler les terminaux compromis empêche les charges actives de logiciels malveillants de se propager aux autres appareils du réseau.

# Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

### Q1: Comment les développeurs de logiciels malveillants contournent-ils les antivirus fondés sur les signatures ?

Ils utilisent le polymorphisme : le hachage et la structure du code du fichier changent à chaque infection, tandis que le comportement malveillant reste le même.

### Q2: Quel est le risque des outils à double usage dans les campagnes de logiciels malveillants ?

Les attaquants utilisent des outils d'administration légitimes (comme PowerShell ou Sysinternals) pour se fondre dans le trafic réseau normal, ce qui rend la détection difficile.

### Q3: Comment le process hollowing exécute-t-il des charges malveillantes ?

Elle lance un processus système légitime à l'état suspendu, remplace son code en mémoire par un logiciel malveillant, puis reprend l'exécution.

### Q4: Quel est le rôle d'un serveur de commande et de contrôle (C2) ?

Un serveur distant exploité par des pirates pour envoyer des instructions et des charges utiles aux logiciels malveillants installés sur des machines compromises.

### Q5: Pourquoi l'enregistrement des frappes (keylogging) est-il difficile à détecter ?

Les enregistreurs de frappe basiques consomment très peu de ressources processeur et cachent leurs processus dans des utilitaires légitimes de l'espace utilisateur.

# Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

### Q6: Comment l'obfuscation du code retarde-t-elle l'analyse des logiciels malveillants ?

Il chiffre ou réorganise le code source, ce qui le rend illisible pour les outils d'analyse et les analyseurs de sécurité.

### Q7: Quelle est la fonction d'un bootkit ?

Un rootkit qui infecte le processus de démarrage (le MBR, le secteur d'amorçage ou le firmware UEFI), de sorte qu'il s'exécute avant le chargement du système d'exploitation.

### Q8: Comment l'analyse heuristique identifie-t-elle les menaces zero-day ?

Il recherche des schémas de code suspects et des commandes d'administration au lieu de chercher une empreinte correspondante dans une base de données.

### Q9: Quelle est la menace du détournement de DLL ?

Forcer une application légitime à charger une bibliothèque de liens dynamiques (DLL) malveillante en la plaçant dans le répertoire de l'application.

### Q10: Comment les chaînes d'analyse automatisée des logiciels malveillants utilisent-elles la virtualisation ?

Ils exécutent les fichiers suspects sur plusieurs machines virtuelles de différents systèmes d'exploitation, en générant automatiquement des journaux de comportement et des fichiers PCAP du réseau.

# Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

**1. APERÇU SÉCURITÉ**

Les chevaux de Troie restent un moyen d'infection courant, car ils cachent du code malveillant dans des programmes d'apparence anodine.

**2. APERÇU SÉCURITÉ**

L'IC3 du FBI a reçu plus de 3 600 plaintes liées aux rançongiciels en 2025, pour des pertes déclarées dépassant 32 millions de dollars. [3]

**3. APERÇU SÉCURITÉ**

Les vers peuvent se propager rapidement sur les réseaux en exploitant des vulnérabilités de protocole non corrigées, comme EternalBlue dans SMB.

**4. APERÇU SÉCURITÉ**

Les logiciels malveillants sans fichier sont difficiles à détecter, car ils s'exécutent en mémoire au moyen d'outils légitimes et laissent peu de traces sur le disque.

**5. APERÇU SÉCURITÉ**

Les bacs à sable d'analyse reviennent généralement à un instantané sain après chaque exécution, de sorte que chaque test part d'un état connu.

**6. APERÇU SÉCURITÉ**

Les rootkits peuvent modifier les appels système du noyau et renvoyer de faux résultats de diagnostic aux analyseurs anti-malware.

**7. ZOOM SUR LA SÉCURITÉ**

L'obfuscation du code utilise des outils de compression (packers) pour compresser et masquer la véritable structure binaire de la charge malveillante.

**8. ZOOM SUR LA SÉCURITÉ**

Un logiciel malveillant polymorphe modifie son code, et donc l'empreinte (hash) de son fichier, à chaque nouvelle copie pour échapper aux contrôles de signature.

**9. ZOOM SUR LA SÉCURITÉ**

Le détournement de DLL exploite la configuration de l'ordre de recherche dans les systèmes d'exploitation courants comme Windows.

**10. APERÇU SÉCURITÉ**

Les éditeurs de sécurité découvrent chaque jour un très grand nombre de nouveaux échantillons de logiciels malveillants, c'est pourquoi les signatures doivent être mises à jour en permanence.

# Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

## RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

## Corrigé : Point de contrôle 1 – Choix multiple

### 1 Question 1

**Bonne réponse : A**

#### NOTE PÉDAGOGIQUE

Quelle est la caractéristique déterminante d'un cheval de Troie ? → Il se fait passer pour un logiciel légitime afin d'amener les utilisateurs à l'exécuter

### 2 Question 2

**Bonne réponse : A**

#### NOTE PÉDAGOGIQUE

Quel type de logiciel malveillant chiffre les fichiers et exige un paiement ? → Rançongiciel [1]

### 3 Question 3

**Bonne réponse : A**

#### NOTE PÉDAGOGIQUE

Qu'est-ce qui correspond à un logiciel espion ? → Logiciel malveillant conçu pour surveiller en secret les frappes au clavier et l'activité du navigateur

### 4 Question 4

**Bonne réponse : A**

#### NOTE PÉDAGOGIQUE

Pourquoi les développeurs de logiciels malveillants utilisent-ils des rootkits ? → Cacher les processus actifs et les fichiers malveillants au système d'exploitation

### 5 Question 5

**Bonne réponse : A**

#### NOTE PÉDAGOGIQUE

Que signifie le sandboxing dans l'analyse des logiciels malveillants ? → Exécuter les fichiers suspects dans un coffre virtuel isolé pour observer leur comportement en toute sécurité

## Corrigé : Point de contrôle 2 – Vrai ou faux

### 6 Question 6

**Bonne réponse : Faux**

**NOTE PÉDAGOGIQUE**

Faux : les vers se répliquent d'eux-mêmes et se propagent sur les réseaux sans aucune action de l'utilisateur.

### 7 Question 7

**Bonne réponse : Faux**

**NOTE PÉDAGOGIQUE**

Faux : les logiciels publicitaires ne sont pas toujours inoffensifs ; beaucoup suivent la navigation pour cibler les publicités.

### 8 Question 8

**Bonne réponse : Vrai**

**NOTE PÉDAGOGIQUE**

Vrai : des sauvegardes hors ligne saines permettent de restaurer les fichiers chiffrés sans payer, même si les données volées peuvent tout de même fuiter.

### 9 Question 9

**Bonne réponse : Faux**

**NOTE PÉDAGOGIQUE**

Faux : les scanners à signatures ont besoin d'un échantillon connu, donc un logiciel malveillant zero-day tout nouveau peut passer entre les mailles.

### 10 Question 10

**Bonne réponse : Vrai**

**NOTE PÉDAGOGIQUE**

Les logiciels malveillants sans fichier exécutent des scripts malveillants dans la mémoire du système, sans écrire de fichiers sur le disque.

# Corrigés du vocabulaire et grille d'évaluation

**Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).**

## POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

| | | | |
|---|---|---|---|
| D 1. CHEVAL DE TROIE | F 2. RANÇONGICIEL | A 3. LOGICIEL ESPION | H 4. ROOTKIT |
| G 5. BAC À SABLE | C 6. CONFINEMENT | E 7. VER | B 8. SANS FICHIER |

## POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

| | | | |
|---|---|---|---|
| 1 CHEVAL DE TROIE | 2 RANÇONGICIEL | 3 LOGICIEL ESPION | 4 ROOTKIT |
| 5 BAC À SABLE | 6 CONFINEMENT | | |

## POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

| | | | |
|---|---|---|---|
| 1 D – ROOTKIT | 2 F – CONFINEMENT | 3 H – SANSFICHIER | 4 G – VERINFORMATIQUE |
| 5 B – RANCONGICIEL | 6 C – LOGICIELESPION | 7 A – CHEVALDETROIE | 8 E – BACASABLE |

## NOTES DE DISCUSSION POUR LES ENSEIGNANTS

**Termes clés :**
Vérifiez que les élèves savent expliquer CHEVAL DE TROIE, RANÇONGICIEL et LOGICIEL ESPION avec leurs propres mots et donner un exemple pour chacun.

**Études de cas :**
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

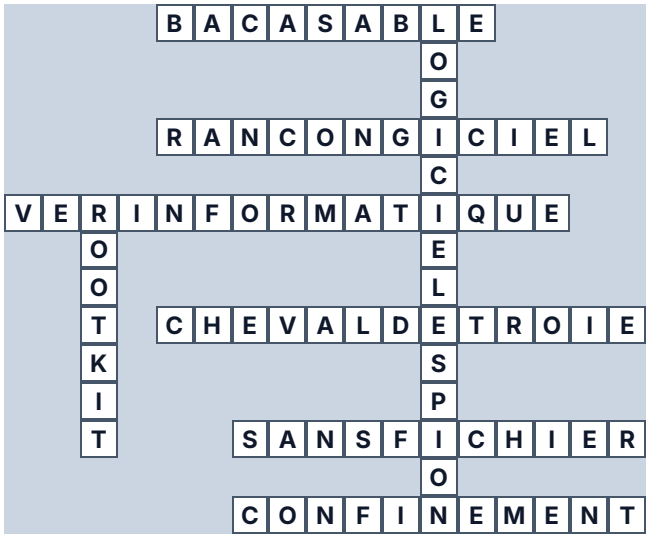
**Évaluation des sources :**
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

# Corrigés des jeux et notes pour l'enseignant

## SOLUTION DES MOTS CACHÉS

| E | A | F | O | K | N | D | V | N | C | D | H | I | B | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | P | R | L | P | T | W | E | T | I | L | Y | F | Y | S |
| O | G | X | W | H | I | F | R | R | T | O | N | U | K | R |
| R | D | T | S | C | K | L | I | P | L | G | M | L | S | H |
| T | K | S | P | O | T | H | N | Y | P | I | L | E | W | U |
| E | N | A | Y | N | O | Q | F | Q | B | C | A | I | L | B |
| D | P | N | M | F | O | B | O | L | I | I | F | C | I | A |
| L | N | S | Y | I | R | B | R | Z | Z | E | Y | I | B | C |
| A | N | F | V | N | X | M | M | C | F | L | P | G | W | A |
| V | Q | I | Q | E | X | H | A | E | Y | E | C | N | W | S |
| E | L | C | F | M | G | H | T | Z | W | S | C | O | O | A |
| H | R | H | J | E | X | X | I | R | K | P | Z | C | A | B |
| C | N | I | R | N | Z | R | Q | M | G | I | S | N | W | L |
| G | L | E | W | T | J | B | U | Y | C | O | C | A | Y | E |
| O | U | R | Z | O | Z | U | E | T | B | N | H | R | V | P |

## SOLUTION DES MOTS CROISÉS




## GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

### HORIZONTALEMENT

**1 horizontal: BACASABLE** Environnement virtuel isolé servant à analyser des fichiers malveillants en toute sécurité. (9 lettres)

**3 horizontal: RANCONGICIEL** Logiciel malveillant qui chiffre le stockage du système et exige un paiement en échange de la clé. (12 lettres)

**4 horizontal: VERINFORMATIQUE** Logiciel malveillant auto-répliquant qui se propage sur les réseaux sans intervention humaine. (15 lettres)

**6 horizontal: CHEVALDETROIE** Logiciel malveillant déguisé en utilitaire inoffensif ou utile. (13 lettres)

**7 horizontal: SANSFICHIER** Logiciel malveillant qui s'exécute directement en RAM pour échapper aux analyseurs de disque. (11 lettres)

**8 horizontal: CONFINEMENT** Restriction des terminaux infectés pour empêcher la propagation des charges malveillantes. (11 lettres)

### VERTICALEMENT

**2 vertical: LOGICIELESPION** Programme conçu pour surveiller et enregistrer secrètement l'activité et les saisies de l'utilisateur. (14 lettres)

**5 vertical: ROOTKIT** Logiciel malveillant furtif dissimulé au cœur du noyau du système pour conserver un contrôle administrateur. (7 lettres)

# Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

### CORRIGÉ DES MOTS MÉLANGÉS

1. DETILHERCOEAV — **CHEVALDETROIE**
2. COIGEOLILNSPEI — **LOGICIELESPION**
3. BASABEALC — **BACASABLE**
4. OUTIEMAFERQIVRN — **VERINFORMATIQUE**
5. AIIGLNOCNREC — **RANCONGICIEL**
6. IOKRTTO — **ROOTKIT**
7. MICOETENNNF — **CONFINEMENT**
8. ICRINSFAEHS — **SANSFICHIER**

### CORRIGÉ DU DÉFI DU CODE SECRET

**"DETECTEZ LES CHARGES PAR ANALYSE COMPORTEMENTALE"**

# Corrigé des études de cas

## A Étude de cas 1 : Confinement d'une charge de rançongiciel en entreprise

Corrigé de l'enseignant

### CONSIGNE DE NOTATION

**Les réponses des élèves doivent couvrir les points suivants :**

- Analyse de scénario : le réseau local d'une entreprise a été compromis par un rançongiciel actif. Des serveurs de fichiers essentiels commencent à afficher des fichiers avec l'extension .locked. Définissez des politiques de confinement.
- Stratégie et solution recommandées : déconnecter tous les serveurs touchés du réseau local. Mettre fin aux sessions d'administration actives. Restaurer les fichiers non compromis à partir d'un système de sauvegarde hors ligne sécurisé et verrouillé en écriture.

## B Étude de cas 2 : Injection en mémoire d'un malware sans fichier

Corrigé de l'enseignant

### CONSIGNE DE NOTATION

**Les réponses des élèves doivent couvrir les points suivants :**

- Analyse de scénario : un analyste détecte des schémas de scripts suspects exécutés directement dans la RAM volatile du système à l'aide d'outils d'administration standard, mais aucun fichier malveillant n'existe sur le disque.
- Stratégie et solution recommandées : isolez d'abord les terminaux touchés et réalisez une image de la mémoire. Examinez les journaux PowerShell et WMI, bloquez les scripts non approuvés avec AppLocker, puis redémarrez pour éliminer la charge malveillante.