

# LA GALERIE DES MENACES

Qui sont les Criminels de Votre Ordinateur ?



# Votre Ordinateur est une Ville.

Imaginez votre monde numérique comme une immense métropole. Vous y avez vos quartiers préférés : les réseaux sociaux, les jeux, YouTube...

Mais comme dans chaque ville, il y a des ruelles sombres et des individus malveillants. Ces criminels numériques s'appellent les "malwares".



# Profils des Criminels les plus Recherchés

Nous allons maintenant dresser le portrait de 8 des plus grands criminels numériques. Du simple vandale au maître-chanteur, découvrez leur identité, leur mission et leur mode opératoire.



Niveau de Menace : **Gênant**



Niveau de Menace : **Indiscret**



Niveau de Menace : **Infectieux**



Niveau de Menace :



Niveau de Menace :



Niveau de Menace :



Niveau de Menace :



Niveau de Menace :



Titre du Criminel

## Le Harceleur Publicitaire

Identité

L'Adware

Niveau de Menace

Gênant

Mission

Vous inonder de publicités non désirées (pop-ups) et rediriger vos recherches.

Mode Opératoire

S'installe en tant que 'composant additionnel' de logiciels gratuits. Il injecte ensuite des scripts dans votre navigateur pour afficher des bannières publicitaires.

Dégâts

Ralentissement du navigateur et de la connexion internet.

# L'Espion Discret



**Identité : Le Spyware**

**Niveau de Menace : Indiscret**

## **Mission**

Collecter des informations sur vous, à votre insu.

## **Mode Opératoire**

Tourne en tâche de fond pour ne pas être repéré.  
Utilise des *Keyloggers* pour enregistrer chaque touche  
frappée (mots de passe, cartes bancaires) et des  
*Info stealers* pour fouiller vos dossiers.

## **Dégâts**

Violation de la vie privée, vol de comptes (réseaux  
sociaux, emails).



# Le Contamineur

**Identité : Le Virus**

**Niveau de Menace : Infectieux**

**Mission :** Infecter des fichiers sains pour se propager dans le système.

**Mode Opératoire :** S'attache à un programme ou un document (un .exe, une macro Word). Quand vous ouvrez le fichier, son code s'exécute et il réécrit une partie de vos autres logiciels pour y insérer ses propres instructions.

**Dégâts :** Corruption de fichiers, système qui ne démarre plus (Écran Bleu / BSOD).

# Le Saboteur Déguisé



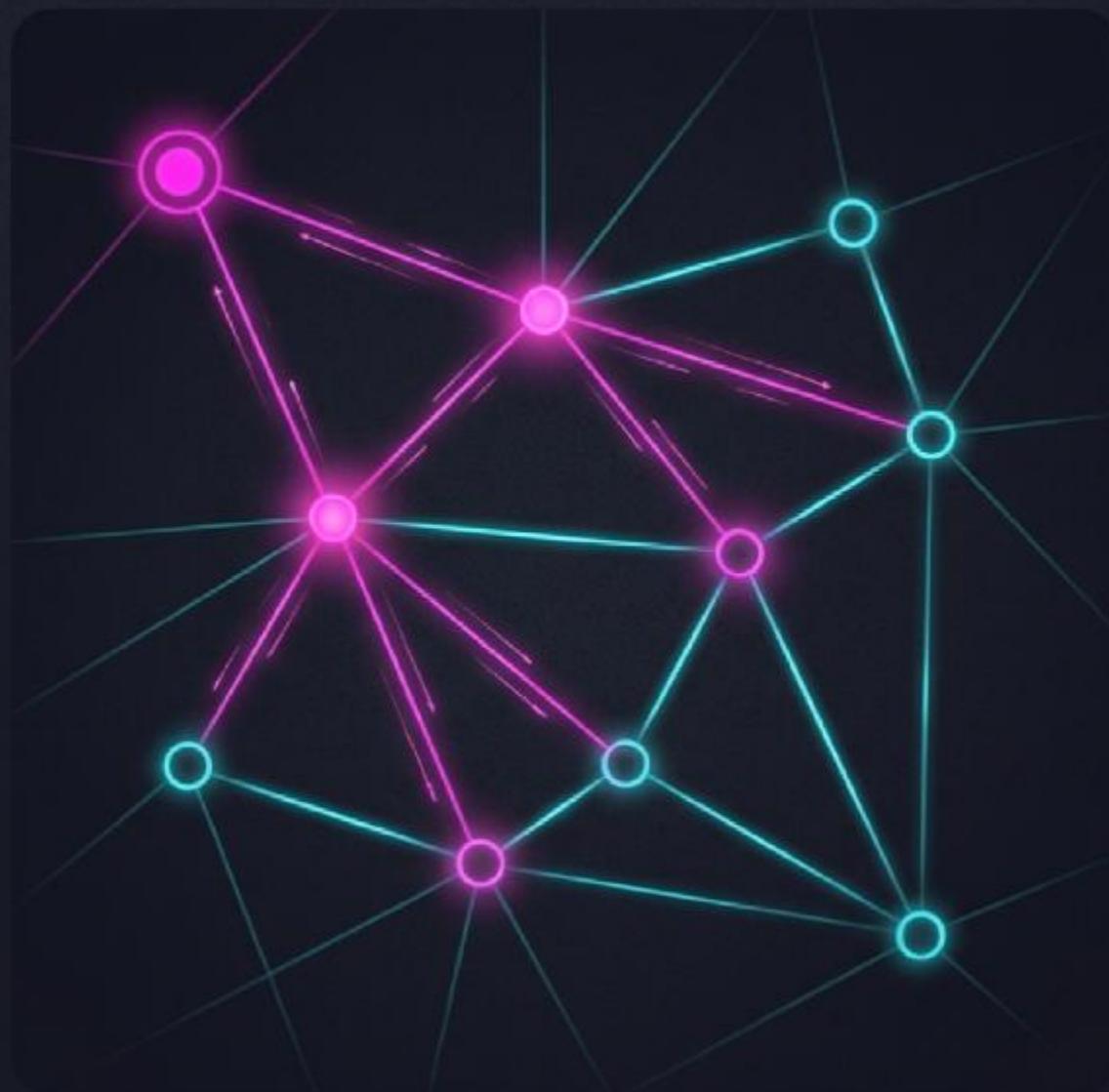
**Identité :** Le Cheval de Troie (Trojan)

**Niveau de Menace :** Traître

**Mission :** Vous faire installer une "porte dérobée" (backdoor) pour laisser entrer un pirate.

**Mode Opératoire :** Se déguise en logiciel utile (jeu gratuit, crack, fausse mise à jour). Il ne se propage pas lui-même, mais une fois installé, il désactive l'antivirus et ouvre des ports de communication pour que le pirate prenne le contrôle.

**Dégâts :** Votre PC devient un "zombie" contrôlé à distance, potentiellement enrôlé dans un Botnet pour attaquer des sites web.



# L'Envahisseur de Réseau

**Identité :** Le Ver (Worm)

**Niveau de Menace :** Envahissant

**Mission :** Se propager de manière autonome et explosive à travers un réseau.

**Mode Opératoire :** Il scanne le réseau (Wi-Fi, Internet) à la recherche d'ordinateurs avec une faille de sécurité. Dès qu'il en trouve un, il s'y copie et recommence le processus, se répliquant massivement.

**Dégâts :** Saturation complète du réseau (la connexion internet 'tombe'), propagation massive d'autres malwares.



## Le Preneur d'Otages Numérique

**Identité :** Le Ransomware (Rançongiciel)

**Niveau de Menace :** **Destructeur**

**Mission :** Chiffrer vos données personnelles et exiger une rançon pour les débloquer.

**Mode Opératoire :** Utilise un algorithme de chiffrement de niveau militaire (AES-256) pour transformer vos photos, vidéos et documents en charabia illisible. Il supprime ensuite les sauvegardes automatiques de Windows et affiche un message avec un compte à rebours exigeant un paiement en Bitcoin.

**Dégâts :** Perte définitive de toutes vos données.

# Escalade de la Menace : Du Visible à l'Invisible

Nous sommes passés du simple GÈNEUR au DESTRUCTEUR. Mais les criminels les plus dangereux ne sont pas ceux que l'on voit arriver. Ce sont ceux qui agissent dans l'ombre.





# Le Fantôme dans le Système

Identité : Le Rootkit

Niveau de Menace : Invisible

**Mission** : Devenir l'administrateur secret de la machine, sans jamais être détecté.

**Mode Opératoire** : S'installe au cœur du système d'exploitation (le 'noyau'). Il peut alors intercepter les demandes de l'antivirus et lui mentir, cachant sa propre présence. Il modifie les fonctions de base de Windows pour rester invisible.

**Dégâts** : Le pirate a un accès total et permanent à votre machine. La seule solution est souvent de réinstaller complètement le système.

# L'Assassin Insaïsissable



**Identité :** Le Malware "Sans Fichier" (Fileless)

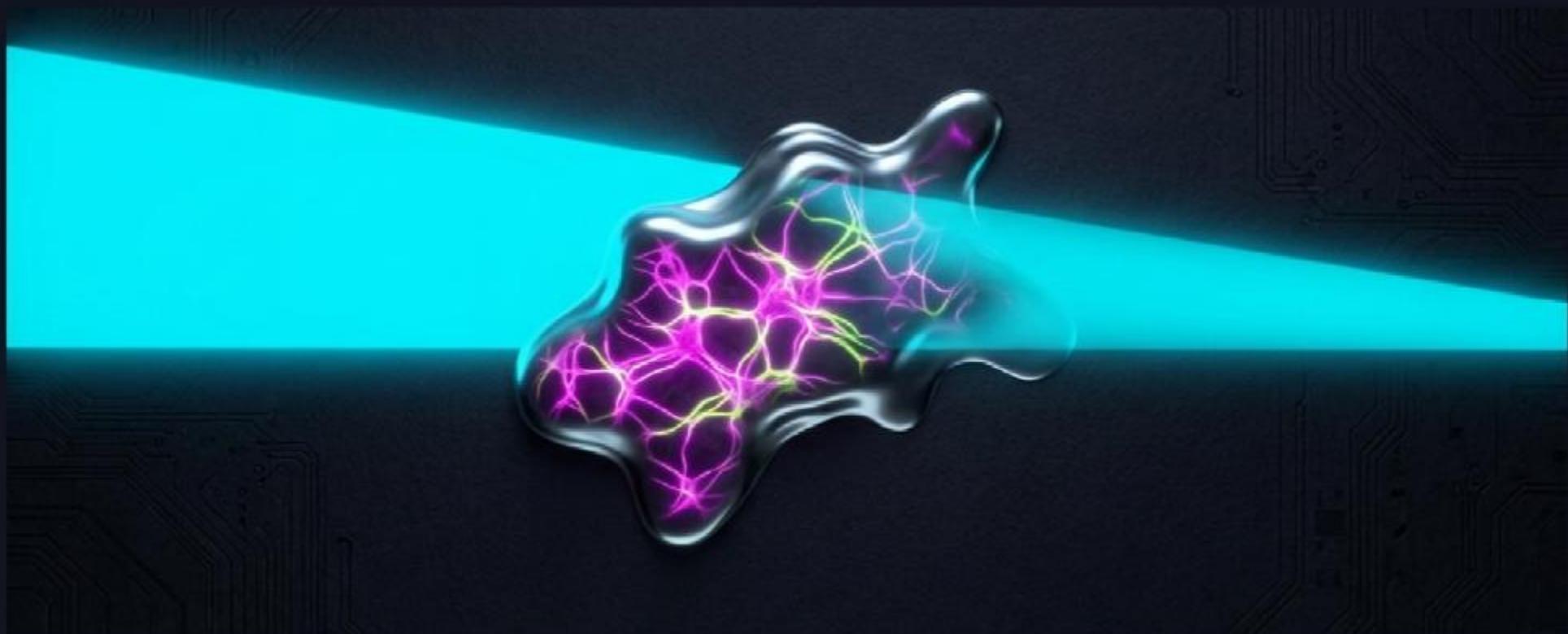
**Niveau de Menace :** Ultra-Invasif

**Mission :** Attaquer sans laisser de traces sur le disque dur.

**Mode Opératoire :** N'enregistre aucun fichier malveillant. Il injecte son code directement dans la mémoire vive (RAM) en utilisant des outils légitimes de Windows (comme PowerShell). C'est une 'exécution fantôme' : il agit, puis disparaît au redémarrage.

**Dégâts :** Presque impossible à détecter par les méthodes traditionnelles.

# Et Demain ? Le Criminel devient Intelligent.



L'évolution ne s'arrête pas. D'ici 2026, certains malwares utiliseront l'Intelligence Artificielle (IA) pour s'adapter en temps réel à vos défenses, comme un caméléon qui change de couleur pour échapper à un prédateur.

# Connaître son Ennemi est la Première Défense

Chaque menace parie sur une de vos faiblesses.



Le Harceleur Publicitaire  
Harcèlement



L'Espion Discret  
Indiscrétion



Le Contamineur  
Contamination



Le Saboteur Déguisé  
Tromperie



L'Envahisseur  
de Réseau  
Faille



Le Preneur d'Otages  
Numérique  
Chantage



Le Fantôme dans  
le Système  
Dissimulation



L'Assassin  
Insaisissable  
Furtivité

# Le Meilleur Antivirus, c'est Vous.



La protection la plus efficace n'est pas un logiciel. C'est **votre curiosité et votre prudence**. En comprenant comment pensent ces criminels, vous devenez **le meilleur gardien** de votre ville numérique.