

Virus, trojans, spywares : le panorama des logiciels malveillants

Mettre les bons mots sur les menaces : ce que fait chaque famille de malware, comment elle entre, et ce qui la bloque.

8 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/panorama-malwares

« Virus » est devenu le mot-valise de tout ce qui infecte un ordinateur — mais les familles de logiciels malveillants ont des objectifs, des modes d'entrée et des parades différents. Ce panorama met de l'ordre : savoir ce qu'on affronte aide à comprendre pourquoi les défenses recommandées (mises à jour, EDR, vigilance, sauvegardes) couvrent chacune un morceau du spectre.

1. Les familles, par objectif

- Le ransomware : chiffre et rançonne — la menace n° 1 des entreprises, traitée dans notre guide dédié
- L'infostealer (voleur d'informations) : la star montante — il aspire en quelques secondes mots de passe enregistrés, cookies de session et portefeuilles, puis disparaît ; ses butins alimentent les revendeurs d'accès
- Le cheval de Troie d'accès (RAT) : l'accès distant discret et durable — l'attaquant revient quand il veut
- Le spyware/keylogger : enregistre frappes et écrans — l'espionnage ciblé
- Le botnet : votre machine enrôlée dans une armée (spam, attaques DDoS, minage) — souvent sans autre symptôme qu'une lenteur
- L'adware et les indésirables : barres d'outils, pubs, navigateur détourné — plus pénibles que dangereux, mais signes d'hygiène défaillante
- Le ver : se propage seul de machine en machine via les failles — rare à l'échelle PME depuis la généralisation des correctifs... quand ils sont appliqués

2. Comment ça entre (toujours les mêmes portes)

- La pièce jointe et le document piégé — le canal roi
- Le téléchargement piégé : logiciel « gratuit », crack, faux installateur en tête des résultats sponsorisés — le logiciel piraté est un cheval de Troie quasi garanti
- Le phishing qui mène à l'exécution ou au vol direct
- Les failles non corrigées, surtout sur ce qui est exposé à Internet (voir mises à jour)
- Les supports USB et l'accès physique (voir nos guides)

ATTENTION

L'infostealer mérite une alarme particulière : en vogue massive, il frappe en secondes (pas d'installation durable à détecter), et son butin — les cookies de session — permet de contourner même la MFA en « rejouant » vos sessions ouvertes. Sa source principale : les téléchargements piégés et les cracks. La parade : jamais de logiciels hors sources officielles, et déconnexion/rotation des sessions au moindre doute.

3. Les symptômes qui doivent alerter

- Lenteur soudaine et durable, ventilateur en furie au repos, espace disque qui fond
- Fenêtres, barres d'outils ou page d'accueil apparues toutes seules ; antivirus désactivé « tout seul »
- Connexions et emails que vous n'avez pas faits ; contacts qui reçoivent des messages « de vous »
- Le poste qui « vit sa vie » : souris, redémarrages, activité réseau inexpliquée
- Aucun symptôme du tout : les malwares sérieux sont silencieux — d'où la supervision plutôt que la confiance au ressenti

4. Infection avérée : le traitement

- Isoler la machine du réseau, sans l'éteindre — le réflexe standard
- Changer depuis un AUTRE poste les mots de passe des comptes utilisés sur la machine, et déconnecter toutes les sessions actives (l'infostealer a peut-être déjà tout pris)
- Analyser via l'EDR/antivirus ; au moindre doute sur un malware sérieux : la réinstallation complète est la seule certitude — les « nettoyages » laissent des restes
- Chercher la porte d'entrée : quel téléchargement, quel email, quelle faille — sinon l'histoire se répète
- Restaurer les données depuis les sauvegardes, pas depuis la machine infectée

L'essentiel à retenir

- 01 Interdire les logiciels hors sources officielles (et tout crack)
- 02 Maintenir EDR actif et surveillé sur chaque machine
- 03 Appliquer les mises à jour, surtout sur l'exposé à Internet
- 04 Former aux symptômes et au réflexe d'isolement
- 05 En cas d'infection : rotation des mots de passe ET des sessions
- 06 Réinstaller plutôt que « nettoyer » en cas de doute sérieux

Questions fréquentes

Mac et Linux attrapent-ils des malwares ?

Oui — le mythe de l'immunité a vécu : les infostealers ciblent activement macOS (faux installeurs, fausses mises à jour de navigateur), et les serveurs Linux sont des cibles de choix (botnets, minage, ransomwares de serveurs). L'écart avec Windows s'est réduit à une question de volume, pas de principe. Mêmes règles partout.

Un malware peut-il survivre à une réinstallation ?

Les cas de persistance sous le système (firmware) existent mais restent exceptionnels et ciblés. Pour l'écrasante majorité des infections, la réinstallation propre depuis un support sain + les données restaurées de sauvegarde = repartir net. Le vrai point de vigilance est ailleurs : ne pas restaurer le malware AVEC les données (exécutables douteux dans les documents) et ne pas se réinfecter par la même porte.

Les malwares sur téléphone, mythe ou réalité ?

Réalité, essentiellement via les applications hors stores officiels et les fausses applications bancaires — Android plus exposé qu'iOS par ouverture. Les règles du guide mobiles couvrent le risque : stores officiels uniquement, mises à jour, permissions surveillées. Le « virus par simple SMS » reste, lui, du registre des attaques d'exception.

Pour aller plus loin

Cybermalveillance.gouv.fr — les virus informatiques — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/virus-informatiques

ANSSI — état de la menace — cyber.gouv.fr/publications

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr