

Documents piégés : macros, faux PDF et pièces jointes malignes

Le fichier Word qui demande d'« activer le contenu », le PDF qui n'en est pas un : comment les documents attaquent, et comment s'en prémunir.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/macros-documents-pieges

La pièce jointe reste le cheval de Troie favori des attaquants — et le document piégé a ses grands classiques : la macro Office qui « doit être activée pour afficher le document », le PDF qui est en réalité un exécutable, l'archive ZIP qui cache le tout. Comprendre ces mécanismes transforme chaque collaborateur en filtre efficace, car le document piégé a presque toujours besoin d'une action de votre part pour nuire.

1. Les pièges classiques, décodés

- La macro Office : un document Word/Excel contient du code exécutable ; le bandeau jaune « Activer le contenu » est LA porte — l'activer sur un document reçu, c'est exécuter le programme de l'attaquant
- Le faux document : « facture.pdf.exe », l'icône PDF sur un exécutable, le fichier .html ou .iso déguisé — l'extension réelle est masquée par défaut sous Windows
- L'archive-écran : le ZIP (parfois protégé par un mot de passe donné dans l'email — précisément pour passer les filtres antivirus) qui contient le piège
- Le lien déguisé en pièce jointe : « le document est trop volumineux, téléchargez-le ici » — la page imite un partage OneDrive/Drive et vole les identifiants
- Le raccourci malin : les fichiers .lnk, .js ou .vbs envoyés comme « documents » — aucun document légitime n'arrive sous ces formats

2. Les protections techniques qui font le gros du travail

- Le blocage des macros venant d'Internet : Microsoft l'applique désormais par défaut — vérifiez que personne ne l'a « débloqué », et gérez les rares besoins légitimes par des emplacements de confiance définis
- L'affichage des extensions de fichiers activé sur tous les postes : « facture.pdf.exe » se démasque d'un coup d'œil
- L'ouverture en mode protégé (lecture seule) des documents reçus — le réglage Office par défaut, à ne pas contourner par confort
- Un EDR qui surveille les comportements : Word qui lance PowerShell est son signal d'alarme favori
- Le filtrage des pièces jointes en amont (détonation en bac à sable) inclus dans les offres Microsoft 365/Workspace adaptées

ATTENTION

La règle d'or à afficher : un document reçu qui demande d'« activer les macros », d'« activer le contenu » ou d'« activer la modification » pour être lisible est un piège, à de très rares exceptions près. Un vrai document se lit tel quel. Cette seule règle, connue de tous, neutralise l'une des chaînes d'infection les plus utilisées au monde.

3. Les réflexes humains

- La cohérence avant le clic : ce fournisseur envoie-t-il d'habitude des factures ? attendais-je ce document ? — les réflexes anti-phishing s'appliquent aux pièces jointes
- Le doute se lève par un autre canal : un appel au numéro connu de l'expéditeur supposé
- Jamais de mot de passe d'archive suivi aveuglément : le ZIP chiffré non attendu est un signal en soi
- Le document douteux ne s'ouvre pas « pour voir » : il se signale — l'ouverture dans le doute se fait par le référent, dans un cadre maîtrisé

4. Et vos propres documents sortants

- Envoyez des PDF plutôt que des documents Office modifiables quand la modification n'est pas nécessaire : plus léger, plus sûr, plus professionnel
- Purgez les métadonnées des documents publiés (auteur, chemins, historique) — elles racontent votre organisation (voir notre guide OSINT)
- Pas de macros dans les documents envoyés aux clients : vous les entraîneriez à cliquer sur « Activer » — le contre-exemple absolu
- Pour les gros fichiers : un lien de partage maîtrisé plutôt que la pièce jointe lourde — et vos destinataires apprennent vos canaux légitimes

L'essentiel à retenir

01 Vérifier le blocage des macros d'origine Internet sur tous les postes

02 Afficher les extensions de fichiers partout

03 Conserver le mode protégé d'ouverture des documents reçus

04 Ancrer la règle : « activer le contenu » = piège

05 Filtrer les pièces jointes en amont (bac à sable)

06 Envoyer des PDF sans macros et purger les métadonnées

Questions fréquentes

Nous utilisons des macros légitimes en interne. Comment concilier ?

Par les emplacements et signatures de confiance : vos classeurs à macros vivent dans des dossiers de confiance définis (ou sont signés numériquement), où ils fonctionnent normalement — tout le reste reste bloqué. C'est un réglage standard des outils d'administration Microsoft, qui préserve l'usage métier sans rouvrir la porte aux documents reçus.

Un PDF peut-il vraiment être dangereux ?

Le vrai PDF malveillant exploitant une faille du lecteur existe mais vise surtout des cibles de valeur avec des lecteurs non à jour — d'où l'importance des mises à jour. Le danger courant est ailleurs : le « PDF » qui n'en est pas un (exécutable déguisé) et le PDF porteur d'un lien de phishing. Lecteur à jour + extensions affichées + réflexe lien = l'essentiel est couvert.

Que faire d'un document suspect qu'on doit pourtant traiter (candidature, devis) ?

Les métiers qui reçoivent des documents d'inconnus (RH, achats) méritent un circuit : ouverture dans un environnement en ligne (les aperçus web de Microsoft/Google affichent sans exécuter), postes particulièrement à jour et surveillés, et le réflexe de demander le renvoi en PDF via un canal de dépôt maîtrisé. Le confort de l'expéditeur ne prime jamais sur la sécurité du destinataire.

Pour aller plus loin

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

Microsoft — le blocage des macros expliqué — learn.microsoft.com/fr-fr/deployoffice/security/internet-macros-blocked

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

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