

Fichiers chiffrés ou écran de rançon

Chaque minute compte : limiter la propagation avant tout le reste.

- 1 Isoler — sans éteindre**
Débranchez le câble réseau et coupez le Wi-Fi de la machine touchée. N'éteignez pas : la mémoire contient des preuves.
- 2 Couper les accès**
Déconnectez le VPN et les accès distants. Si plusieurs machines sont touchées, isolez le réseau entier (couper le switch/la box).
- 3 Protéger les sauvegardes**
Déconnectez physiquement les sauvegardes qui ont survécu (disques, NAS) avant toute autre action.
- 4 Appeler les secours**
Votre prestataire informatique, puis votre assureur cyber. Ne tentez pas de « nettoyer » vous-même.
- 5 Préserver les preuves**
Photographiez l'écran de rançon. Ne supprimez rien, ne payez rien, ne répondez pas aux attaquants.
- 6 Déclarer**
Dépôt de plainte sous 72 h (exigé par l'assurance) et notification CNIL sous 72 h si des données personnelles sont touchées.

À retenir

Ne payez pas la rançon : aucune garantie, et cela finance les prochaines attaques. Vérifiez d'abord nomoreransom.org et restaurez depuis vos sauvegardes.

Assistance Cyberionis : 06 64 90 07 74 · contact@cyberionis.fr · cyberionis.fr