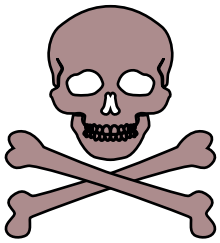
LA CRISE SANITAIRE DU COVID19 MULTIPLIE LES RISQUES DE RANSOMWARES



Un ransomware (ou rançongiciel en français) est un logiciel informatique malveillant qui prend en otage des données. Les répercussions de cette attaque sont considérables et désastreuses pour la survie économique de l'entreprise.

Vous devez être **sensibilisés** et vous **protéger.**

LES BONNES PRÉCAUTIONS
POUR UNE ACTIVITÉ SECURISÉE SUR LE NET

Soyez prudents avec les mails reçus
Parfois, ils ne paraissent pas suspects et sont parfaitement orthographiés. La pièce jointe n'est pas obligatoirement un fichier exécutable. Le destinataire peut être une adresse connue mais volée.

N'exposez pas votre bureau à distance
Utilisez un VPN pour accéder aux ressources informatiques internes tel que le bureau à distance (RDP), plutôt que de les rendre accessibles au monde entier.

Sauvegardez vos données
Sauvegardez vos données sur un disque dur externe (déconnecté) et hors-site (cloud), et testez vos sauvegardes régulièrement.

Eteignez votre appareil
Dès que vous quittez votre poste de travail (notamment pour le week-end), éteignez vos appareils informatiques.

Parez la menace avec une sandbox
Si vous doutez sur un fichier externe, ouvrez le avec une sandbox. S'il s'avère être un virus, il va rester confiné dans ce container sécurisé sans altérer votre ordinateur.

Mettez à jour vos appareils
Le système d'exploitation, les logiciels, le pare-feu, l'antivirus, l'antimalware doivent être régulièrement mis à jour.

Changez vos mots de passe
Changez souvent vos mots de passe et renforcez les avec une synthaxe sophistiquée (majuscules, minuscules, chiffres et caractères spéciaux).

Segmentez votre réseau
Segmentez virtuellement le réseau de l'entreprise en différentes zones de sécurité.

Méfiez-vous des sites incertains
Téléchargez les logiciels *via* le site officiel de l'éditeur. Méfiez-vous des sites, des programmes et des applications d'origine peu sûre.

Sensibilisez votre entourage
Sensibilisez vos collaborateurs et vos proches (notamment ceux qui ont peu de culture web) aux risques.

LES BONS GESTES
EN CAS D'ATTAQUE PAR UN RANSOMWARE

Ne payez pas la rançon
Payer la rançon ne vous garantit pas une récupération de vos données. Sur 5 entreprises qui paient la rançon, 1 n'obtient jamais ses fichiers.

Prévenez les personnes à risque
Alertez directement les personnes de votre entreprise. Il y a aussi un risque de contamination sur leur appareil. Ils doivent rester prudents.

Identifiez la source de l'attaque
Identifier l'attaque permet d'éviter de reproduire l'erreur.

Portez plainte
Porter plainte permet d'engager des poursuites pour essayer de récupérer vos données volées et d'identifier les auteurs. Cela permet également d'être dédommagé par votre assurance. Conservez des preuves de l'attaque pour les présenter aux autorités.

Isolez l'appareil infecté
Isolez l'appareil infecté du réseau (le patient zéro) pour éviter que le virus se répande. Mais surtout n'éteignez pas votre appareil!

Contactez l'aide informatique
Contactez immédiatement le service informatique pour recevoir de l'aide, et éventuellement des professionnels extérieurs.

Réinstallez les systèmes touchés
Tentez une remédiation avec la sauvegarde existante en réinstallant les systèmes touchés, après s'être assuré que l'ordinateur et le réseau soient sécurisés.

Décryptez les données
Tentez de décrypter les fichiers grâce à des outils de déchiffrement (plusieurs antivirus en proposent directement).

LE COVID 19, UNE ACCROCHE
UTILISÉE PAR LES RANSOMWARES POUR SE PROPAGER

MÉFIEZ-VOUS DES SITES INTERNET NON-OFFICIELS.

NE TÉLÉCHARGEZ PAS DES APPLICATIONS OU DES LOGICIELS NON VÉRIFIÉS.

SÉPAREZ LE PROFESSIONNEL DU PERSONNEL SUR DIFFÉRENTS APPAREILS.

SENSIBILISEZ LE CORPS MÉDICAL EN LEUR PARTAGEANT CES INFORMATIONS.

N° gendarmerie : 17
https://www.cybermalveillance.gouv.fr/

GROUPEMENT DE GENDARMERIE DÉPARTEMENTALE DE LA GIRONDE

mmi BORDEAUX