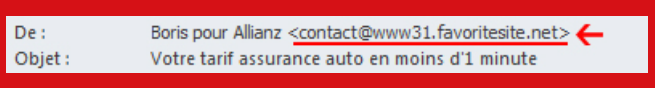
6 SIGNAUX D'ALERTE QUI SEMBLENT CACHER UNE CYBERATTAQUE

Ransomware : un terme archaïque qui fait certes écho à une menace mais dont le fonctionnement vous semble flou ?

Décryptage rapide : un ransomware est un logiciel malveillant qui, lorsqu'il s'installe sur votre ordinateur, prend « en otage » vos données. Le ransomware chiffrera alors et empêchera l'accès à vos fichiers en demandant une rançon. En échange, il fourni généralement une clé permettant de déchiffrer et récupérer vos données.

1. UN EXPÉDITEUR MYSTÈRE

Vous avez reçu un email inhabituel ? Votre assurance vous a écrit un e-mail sur votre adresse professionnelle ? Ne vous fiez pas à au nom d'envoi affiché, mais observez plutôt l'adresse e-mail de votre expéditeur :



Un doute ? Ne cliquez sur aucun lien et n'ouvrez pas les pièces jointes. Soyez attentifs, parfois les hackers peuvent être plus subtils : il peut s'agir d'une seule lettre erronée dans l'adresse email !

2. UN OBJET TRÈS ALARMISTE

Une technique assez répandue dans les cyberattaques, consiste à mettre en alerte l'individu en mentionnant un caractère urgent ou alarmant. Les objets de type "Votre compte a été piraté" ou "Vous avez un message urgent" doivent surtout vous mettre en alerte contre une cyberattaque.

3. UNE PIÈCE JOINTE INATTENDUE

Une facture reçue de la part d'un fournisseur inconnu alors que vous travaillez au service commercial ? Méfiez-vous, les attaques malveillantes peuvent aujourd'hui se cacher dans un simple document Word ou Excel , avec l'extension .doc ou .xls

4. UNE DEMANDE INHABITUELLE

Vous avez tout vérifié : l'adresse e-mail est correcte, il n'y a pas de pièce jointe… Par contre, cet email de votre proche qui vous fait part de ses problèmes d'argent par email semble tellement inhabituel. Il vous demande de lui répondre uniquement par email ? C'est un signal d'alerte : votre proche semble être victime de "spoofing" soit d'usurpation d'identité. Prévenez le par tout autre moyen de communication dès que possible et ne cliquez sur aucun lien !

5. UN SITE INCONNU,SOI DISANT «SÉCURISÉ»

Il a souvent été entendu que les sites web commençant par "https" étaient de confiance. Attention à l'amalgame ! Un site en HTTPS est un site web avec des données chiffrées, ce qui ne signifie pas toujours "sécurisé". Les cybercriminels aiment cacher des contenus malveillants au sein de sites HTTPS. Un lien suspect à rallonge commençant par https doit vous alerter. Par exemple :

✔ https://www.vistaprint.fr/
✖ https://atjvdff5665v3cfdgf8fd474fd4df77.ru

6. QUAND C'EST TROP BEAU POUR ÊTRE VRAI...

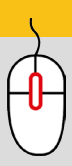
Un site web vous annonce que vous êtes leur 100 000ème visiteur et vous offre un voyage aux Maldives en cliquant simplement sur leur lien ? Vous connaissez ce fameux adage : «Quand c'est trop beau pour être vrai...»

OUPS...TROP TARD !

Vous avez déjà cliqué sur le lien Internet ou la pièce jointe suspecte, mais vous réalisez que c'était probablement une attaque ? Contactez votre service informatique sans plus attendre et prévenez vos collègues qui seraient susceptibles de se retrouver dans la même situation que vous.

J'AI LA SOLUTION !

Un écran vous demandant de payer une rançon s'affiche sur votre écran et vous pensez ainsi récupérer toutes vos données, l'air de rien ? C'est une fausse bonne idée, ne payez pas ! D'une part vous n'avez aucune certitude de récupérer vos données et d'autre part vous financez les entreprises de développement de ces codes malveillants ! Ce fut le cas par exemple de l'attaque mondiale Petya qui s'est avérée être un "wiper" et non un ransomware. Cela signifie qu'après paiement de la rançon, les entreprises n'ont pas pu récupérer leurs données car cela n'était pas prévu dans le code source...



A PROPOS D'OLFEO

Olfeo est éditeur de logiciel, expert de la sécurité web et du filtrage de contenus depuis 14 ans. Chez Olfeo, nous croyons que la sécurité positive est le meilleur moyen de vous protéger contre les nouvelles menaces tout en accompagnant les nouveaux usages web.

Il est dans notre ADN de considérer les projets de sécurité web au-delà des seuls aspects fonctionnels et techniques. Nous proposons aux organisations exigeantes la seule passerelle de sécurité web qui réunit à la fois : l'expertise technologique, la conformité légale & culturelle ainsi que le facteur Humain.

Et n'oubliez pas : les cybercriminels comptent sur votre aide pour répandre leurs attaques informatiques, ne leur donnez pas satisfaction !

Olfeo
La sécurité positive