clic&connect

Les 5 principales cybermenaces

Tags

#cybercriminel #cybersécurité #Sécurité

Résumé

Le piratage de certains sites Internet ou de certaines entreprises peut conduire au vol de données, dont des bases de données utilisateurs avec de nombreuses informations personnelles potentiellement sensibles.

Ce tutoriel a pour objectif de présenter les méthodes pour vérifier que ses données personnelles n'ont pas fuitées en ligne avec le site Firefox Monitor.

Difficulté

Débutant

Prérequis

- Pas de prérequis identifiés
- Pour tous les supports

L'art d'exploiter les vulnérabilités humaines

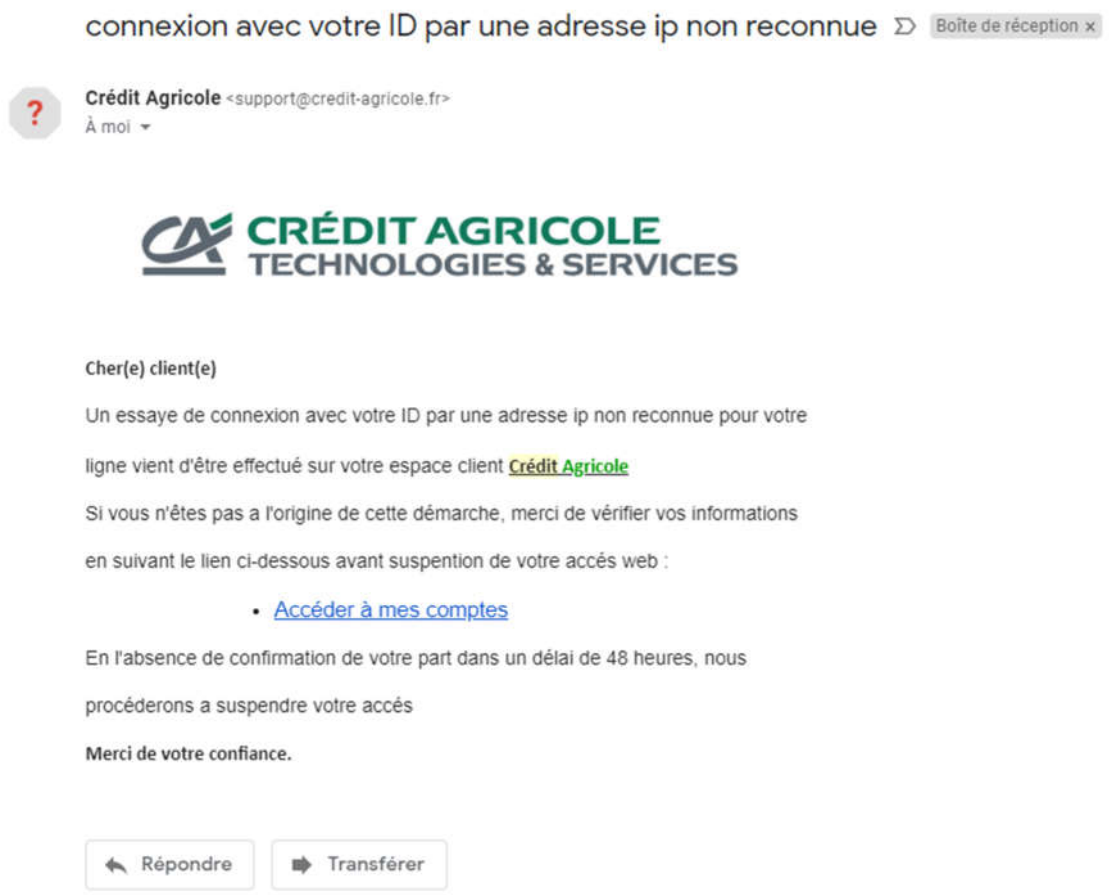
L'humain est le maillon le plus vulnérable dans une attaque informatique. Les **attaques par ingénierie sociale** consistent à pratiquer la manipulation psychologique (menace, peur, imitation d'organisme légitime) pour soutirer des informations personnelles ou de l'argent auprès des victimes.

Les plus répandues sont **le phishing**, **les e-mails de chantage**, **le faux support technique**, ou encore **le faux dirigeant ou salarié**.

Top 1 – Le phishing : imiter des organismes officiels

Le **phishing**, appelé "hameçonnage" en français est extrêmement répandu. D'après cette étude de Proofpoint, **90% des organisations** dans le monde **ont connu des attaques** de phishing ciblées en 2020.

Le principe est simple mais redoutable. Les pirates **reproduisent le site Internet** ou le design **d'un service public ou d'une entreprise**. **La victime pense saisir ses informations sur un site fiable**, mais ce sont les pirates qui récupéreront ces données (informations de connexion, numéro de carte de crédit…).


connexion avec votre ID par une adresse ip non reconnue Boîte de réception ×

Crédit Agricole <support@credit-agricole.fr>
À moi

CRÉDIT AGRICOLE TECHNOLOGIES & SERVICES

Cher(e) client(e)

Un essaye de connexion avec votre ID par une adresse ip non reconnue pour votre ligne vient d'être effectué sur votre espace client Crédit Agricole

Si vous n'êtes pas a l'origine de cette démarche, merci de vérifier vos informations en suivant le lien ci-dessous avant suspention de votre accés web :

- Accéder à mes comptes

En l'absence de confirmation de votre part dans un délai de 48 heures, nous procéderons a suspendre votre accés

Merci de votre confiance.

Répondre Transférer

Si vous recevez un e-mail d'un organisme officiel demandant de fournir des informations sensibles, **contactez-le** directement.
Si vous avez un doute, **supprimez-le**.

Si vous avez déjà rempli et envoyé des informations via un formulaire frauduleux :

- **prenez contact avec votre banque** si vous avez transmis votre numéro de carte bancaire pour faire opposition ;
- **modifiez vos mots de passe** si vous avez transmis un identifiant et contactez les services ciblés ;
- **déposez plainte** au commissariat de police ou à la gendarmerie.

Transmettez à l'organisme en question l'e-mail frauduleux et **signalez-le** sur le site Signal Spam et Phishing Initiative.

Top 2 – Les mails de chantage

Ce type de menace est en recrudescence ces derniers mois.

Le pirate fait croire à la victime qu'il est en possession de documents compromettants (photos intimes, découverte de failles sur son site Internet…).

Dans la majorité des cas, il ne dispose d'aucune information contre la victime et s'appuie sur sa crédulité.

Vous ne me connaissez pas et vous vous demandez probablement pourquoi vous recevez ce mail, non?
Je suis un hackeur qui a piraté vos appareils il y a quelques mois.
Je vous ai envoyé un e-mail depuis VOTRE compte piraté.
J'ai mis en place un virus sur le site pour adulte (porno) et devinez quoi, vous avez visité ce site pour vous amuser (vous savez ce que je veux dire).
Pendant que vous regardiez des vidéos, votre navigateur internet a commencé à fonctionner comme un RDP (contrôle à distance) ayant un keylogger, ce qui m'a donné l'accès à votre écran et votre webcam.
Après cela, mon logiciel a obtenu tous vos contacts et fichiers.

Vous avez entré vos mots de passes sur les sites que vous avez visités, et je les ai interceptés.

Bien sûr, vous pouvez les modifier, ou alors vous les avez déjà changés.
Mais ça n'a pas d'importance, mon virus l'a mis à jour à chaque fois.

Qu'ai-je fait ?
J'ai créé une vidéo en double écran. La 1ère partie montre la vidéo que vous regardiez (vous avez de bons goûts ahahah...), et la deuxième partie montre votre webcam.
N'essayez pas de trouver et de détruire mon virus ! (Toutes vos données sont déjà téléchargés vers un serveur distant)
– N'essayez pas d'entrer en contact avec moi
– Les antivirus ou services de sécurité;
Formater votre disque ou détruire l'ordinateur ne vous aidera pas non plus, puisque vos données se trouvent déjà sur un serveur distant.

Je vous garantis que je ne vous dérangerai plus après votre paiement, car vous n'êtes pas ma seule victime.
C'est le code d'honneur des hackeurs.

Ne m'en voulez pas, chacun son travail.
Vous voulez savoir ce que vous pouvez faire ?

Eh bien, à mon avis, 520 EURO est un juste prix pour notre petit secret. Vous effectuerez le paiement par Bitcoin (si vous ne connaissez pas, recherchez "comment acheter des Bitcoins" sur Google).

L'adresse de mon portefeuille Bitcoin:

18TyDpyTwXcawJe7pmEgzUJzD5SMeDjSRj

Si vous recevez ce type d'e-mail, **supprimez-le immédiatement.**
S'il contient des informations personnelles telles qu'un mot de passe, cela signifie qu'elles ont sûrement fuité lors d'un piratage d'un site Internet que vous utilisez.
Changez-le immédiatement et dans tous les cas, **ne payez jamais** !

Top 3 – Les arnaques au faux support technique

La victime voit apparaître sur son écran une fenêtre indiquant que son ordinateur est infecté et qu'elle doit appeler un support technique pour le nettoyer.

Il s'agit en réalité d'une publicité qui simule une alerte. **Le support technique indiqué** prendra surtout le temps **d'espionner votre ordinateur**, d'y installer des logiciels potentiellement nuisibles, et d'alléger votre portefeuille de quelques centaines d'euros.

Si vous voyez une alerte de ce type, fermez la fenêtre, ou éteignez votre ordinateur. **N'appelez pas le numéro de téléphone** et **faites une analyse antivirus** avec un logiciel recommandé tel que Windows Defender, ou une suite reconnue.

Top 4 – Les logiciels malveillants

Les **logiciels malveillants** (ou **malware**) sont des programmes informatiques dont l'objectif est :

- **d'espionner** les actions et saisies sur votre ordinateur (appelé keylogger),

- **d'afficher de la publicité** indésirable (appelé aussi adware),
- **de récupérer des documents** sur votre ordinateur (cheval de Troie).

Les **rançongiciels** (ou **ransomware**) chiffrent l'ensemble des données sur un appareil ou un réseau informatique. Les pirates demandent alors le paiement d'une rançon en échange de la clé de déchiffrement. Ces ransomwares **se propagent par e-mail**, en ouvrant une pièce-jointe infectée, ou une page Internet piégée.

Si vous êtes victime d'un rançongiciel :

- **déconnectez l'appareil** du réseau informatique, **ne l'éteignez surtout pas**, et ne payez pas la rançon demandée ;
- **déposez plainte** auprès du commissariat de police ;
- **choisissez un prestataire de sécurité** référencé sur le site Cybermalveillance pour remettre en place votre système d'information.

L'**exploitation de vulnérabilités** consiste à exploiter les failles non corrigées d'un logiciel pour introduire du code malveillant et **infecter un poste de travail** ou l'ensemble d'un réseau informatique, en vue de le **paralyser ou d'exfiltrer des données.**

Top 5 – Les piratages et fuites de données

Vos comptes en ligne, comme vos comptes de messagerie, sur les réseaux sociaux ou sur des services administratifs **sont des cibles**

intéressantes.
Les pirates les utilisent pour faire du chantage, diffuser leur arnaque, véhiculer de fausses informations, ou simplement nuire à votre image.

L'origine de ces piratages est souvent liée à **un mot de passe peu sécurisé**.

Rendez vos mots de passe robustes et verrouillez à double tour vos comptes avec l'authentification multifacteurs (processus de sécurité de compte nécessitant deux ou plusieurs étapes distinctes pour prouver son identité) quand cela est possible.

Ces piratages entraînent des **vols et fuites de données** issues de base de données de site Internet, ou de système d'information d'entreprise en général.

Les pirates revendent ou réutilisent les données pour perfectionner leurs attaques informatiques (par exemple pour rendre plus crédible un e-mail de chantage).

Vérifiez si des informations personnelles sont en ligne avec des outils comme Firefox Monitor. Si tel est le cas, changez vos mots de passe et restez vigilants sur les e-mails reçus d'organismes piratés.

Pour aller plus loin

Plateforme Cybermalveillance du gouvernement
Quelles sont les cybermenaces ? Formation France Num

Licence