Sécurité des systèmes d'informations
AHMADI Amir
18/02/2024

Victime d’une attaque cybercriminelle et les conséquences

Un cybercriminel est un individu qui se livre à des activités criminelles aussi bien que des groupes organisés et utilisent des techniques telles que le phishing, attaques par déni de service (DDoS), malware etc.

Quels sont les différents types de cybercrimes ?

- Fraude par email et Internet.
- L'usurpation d'identité (lorsque des renseignements personnels sont volés et utilisés).
- Le vol de coordonnées bancaires ou de données financières.
- Le vol et la vente de données d'entreprise.
- La cyber extorsion (exiger de l'argent pour empêcher la concrétisation d'une menace d'attaque).
- Les attaques de ransomwares (un type de cyber extorsion).
- Le crypto jacking (lorsque des pirates extraient de la cryptomonnaie à partir de ressources qu'ils ne possèdent pas).
- Le cyberespionnage (lorsque les pirates accèdent aux données du gouvernement ou d'entreprises).
- Perturber les systèmes d'une manière qui compromet la sécurité d'un réseau.
- Violer les droits d'auteur.

Il existe encore plusieurs d’autres types d'attaques cybercriminelles et plusieurs techniques différentes dont il faut se protéger lorsqu'on navigue sur Internet.

Personnellement je crois qu’on était plus au moins victime de cybercriminelles directement ou indirectement, directement quand on a cliqué inconsciemment ou non volontairement sur un lien ou d’autres types, indirectement comme on a volé nos coordonnées depuis un service qu’on leur a communiqué, résultat nous sommes tous concernée.
Récemment un ami a été victime du vol coordonnées bancaires, apparemment il a cliqué sur des liens frauduleux qui lui a mené sur une site web de la post ou d’autres qu’il connaissait bien pour payer la facture d’un coli qu’il attendait depuis quelques jours, on peut dire qu’il été victime de phishing.
L'attaque de phishing est une technique utilisée par des cybercriminels pour tromper les utilisateurs et leur faire divulguer des informations personnelles ou sensibles telles que des identifiants de connexion, des mots de passe, des numéros de carte de crédit ou des informations bancaires.
Les conséquences de cette attaque sont nombreux si on change pas les mot de passe régulièrement et qu’on se méfie pas aux messages ou liens non sécurisés, parmis les résultats de ce genre d’attaque on peut citer quelques un :

- **Réception d'un e-mail ou d'un message frauduleux :** Les cybercriminels envoient encore des e-mails ou des messages textuels qui semblent provenir d'une source légitime et digne de confiance, telle qu'une institution financière, d'une entreprise ou d'un service en ligne.
- **Contenu trompeur** : Il peut envoyer un mail ou du message conçu pour inciter la victime à agir rapidement, en utilisant des techniques telles que la peur, l'urgence ou la curiosité. Par exemple, l'e-mail peut prétendre qu'il y a un problème avec le compte de la victime et l'encourager à se connecter pour le résoudre.
- **Incitation à cliquer sur un lien ou à télécharger une pièce jointe** : Le message contient généralement un lien hypertexte ou une pièce jointe malveillante. L'utilisateur est incité à cliquer sur le lien pour accéder à un site web frauduleux où il lui sera demandé de saisir ses informations sensibles, ou à télécharger une pièce jointe qui peut contenir un malware.

Les exemples précédents peuvent encore se produire si on ne soit pas conscient, puisque les cybercriminels ont sauvegardé nos données et ils lancent leur dé de temps en temps pour piéger à nouveau les victimes fragiles.
il existe plusieurs types de cybercriminelles qu'on a pas beaucoup de temps de les indiqués et donner des exemples, mais les conséquences sont des fois très lourde voir irréversible dans certains cas comme perd total de son financement personnelle ou d'une entreprise, la mort d'une personne, Destruction d'une famille ou encore pire destruction d'un pays.