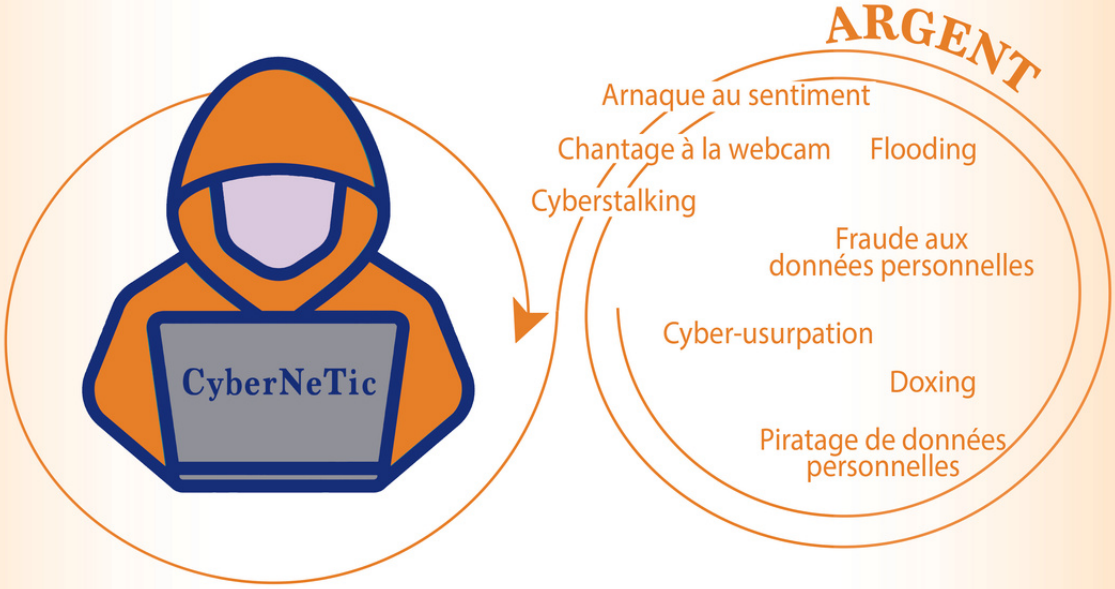
PROJET CYBERNETIC

PIRATAGE DE DONNEES PERSONNELLES

Etiologie des pratiques de cyberharcèlement



SYNONYMES

- Espionnage de données personnelles
- Accès ou maintien frauduleux dans un système de traitement automatisé des données (STAD)

Définition

Concept-clé :

Le piratage de données personnelles consiste en la compromission d'appareils numériques, comme les ordinateurs, les tablettes, les smartphones et même des réseaux complets, afin de collecter des données personnelles sur une victime ciblée.

La première motivation de cette pratique de cyberharcèlement demeure avant tout **l'espionnage**. Elle se déroule en trois temps. D'abord, il s'agit **d'infiltrer** le matériel numérique sans que l'utilisateur ne s'en aperçoive grâce à différentes techniques, puis dans un second temps à **surveiller** ses activités ou à **collecter** furtivement des informations diverses et sensibles comme ses noms d'utilisateur, ses mots de passe, ses adresses mails, l'historique de sa navigation internet, son journal de communication, ses fichiers multimédias, etc. Enfin, les mouchards s'attachent à **renvoyer** toutes les données récupérées au cyberharceleur.

Ces intrusions se déroulent généralement de trois manières sur les appareils mobiles :
-au travers d'une **mauvaise hygiène informatique** (défaut de discrétion dans les lieux publics, mot de passe non robuste, etc.) ;
-au travers des **vulnérabilités du système d'exploitation** (trous de sécurité, mises à jour non effectuées) ;
-par le biais **d'applications malveillantes** dissimulées dans les appareils numériques (contrôle des messages reçus envoyés et supprimés, géolocalisation, captures d'écran à intervalles réguliers, etc.).

Ce qu'il faut retenir...

Les **spywares** sont des logiciels malveillants espions dont les modes d'infection passent régulièrement par les **points d'accès suivants** :

Les téléchargements passifs : les victimes cliquent sur un lien ou une pièce jointe inconnus dans un e-mail, qui lance à son tour une pièce jointe exécutable ou redirige vers un site web qui télécharge et exécute un programme (clickjacking) ; elles visitent un site web malveillant et consultent une page ou une bannière publicitaire qui entraîne un téléchargement non consenti (bait and switch), etc.

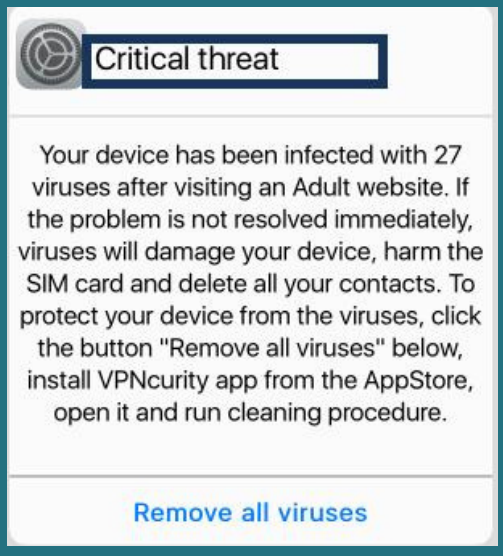
Le marketing agressif : sous prétexte de nouveaux programmes utilitaires à télécharger (des appâts qui prennent la forme de nouveaux produits de sécurité ou d'optimisateurs), les victimes installent intempestivement dans leurs appareils des logiciels espions pour avoir accès aux fonctionnalités qu'elles recherchent.

Les packs logiciels : certains programmes dissimulent des modules complémentaires, des plugins, des extensions. Apparaissant à tort comme indispensables, ils peuvent également dissimuler des spywares, qui perdurent même après leur désinstallation supposée.

Les programmes malveillants : les chevaux de Troie, les virus et les portes dérobées sont autant de menaces en arrière-plan qui permettent de contourner les contrôles de sécurité et qui peuvent détecter et mémoriser les frappes de clavier (keylogging), enregistrer des vidéos, espionner des conversations vocales (eavesdropping), capturer des messages instantanés, accéder à des dossiers sauvegardés, se propager sur tous les ordinateurs connectés au réseau, etc.

> ***J'avais de toute évidence été piraté, mais comment l'expliquer et le prouver ?***

Un exemple concret :



Aux origines...

Le cheval de Troie est un programme malveillant qui subsiste car il passe inaperçu. **Caché** dans un logiciel à **l'apparence inoffensive**, il fait intrusion dans le système et **agit à l'insu** de l'utilisateur.

Son champ sémantique trouve son origine dans le **mythe du cheval de Troie** tiré du récit de **L'Énéide**. En effet, après avoir vainement assiégé Troie pendant dix ans, le stratège **Ulysse** eut l'idée ingénieuse de faire construire un **cheval** géant en bois creux, dans lequel pourraient se cacher des soldats grecs. L'espion Sinon fit croire aux Troyens qu'il s'agissait d'une offrande destinée à la déesse Athéna et qu'elle serait gage de leur victoire. Faisant preuve de peu de méfiance, ils le laissèrent entrer dans l'enceinte de la cité et commencèrent à célébrer leur triomphe. Encore enivrés des senteurs d'alcool au matin levant, ils ne s'aperçurent pas de **l'assaut** mené par les Grecs, qui profitèrent de ce moment d'**inadvertance** pour sortir du cheval, ouvrir les portes de la ville fortifiée et permettre au reste de l'armée d'entrer pour massacrer les habitants ou les réduire en esclavage.

Le concept de Cheval de Troie fut repris dans les années 70 par **Daniel J. Edwards**, chercheur en sécurité informatique auprès de la National Security Agency, qui fit une analogie entre l'histoire mythologique et le **mode de propagation** de ces nouveaux programmes d'apparence inoffensive, mais qui une fois introduit dans le système, se comportent de façon malveillante, à l'insu de l'utilisateur.

Que dit le cadre légal...

Dans le cadre d'un piratage de données personnelles, plusieurs **atteintes aux STAD** sont sanctionnées par le code pénal (**articles 323-1 à 323-3**). Nous pouvons retenir principalement :

- "**L'accès ou le maintien frauduleux dans un système de traitement automatisé de données**" qui est puni de deux ans d'emprisonnement et de 60 000 euros d'amende. Sont concernées par cette infraction toutes les personnes qui cherchent à **prendre connaissance d'informations** qu'elles soient confidentielles ou non (par le biais de connexions, de visualisations, etc.), dans un système de traitement automatisé de données, alors que l'accès leur est interdit.

- "**L'importation, la détention, l'offre, la cession ou la mise à disposition d'un équipement, un instrument, un programme informatique pour atteindre un STAD**" qui vise plus précisément à lutter contre les **moyens de prolifération des programmes et logiciels malveillants** mis en œuvre pour commettre les infractions (keylogger, cheval de Troie, vers, etc.).

Les personnes physiques coupables de ces délits encourent également des peines complémentaires telles que :
- "**L'interdiction**, pour une durée de cinq ans au plus, **des droits civiques, civils et de famille**" ;
- "**L'interdiction**, pour une durée de cinq ans au plus, **d'exercer une fonction publique** ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise" ;
- "**La confiscation** de la **chose** qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution".

Pour aller un peu plus loin...

Quelques références scientifiques :

BWELE Charles, Le cyberespionnage industriel : de la sécurité informatique à la sécurité économique, *Sécurité globale*, Volume 24, n° 2, 2013, pp. 49-58.

COTE Anne-Marie, BERUBE Maxime, DUPONT Benoit, Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité, *Réseaux*, Volume 197-198, n° 3-4, 2016, pp. 203-224.

DECLOQUEMENT Franck, Espionnage, attaques subversives et cyber sécurité : de l'impact des actions de "social engineering" et des vulnérabilités humaines sur la sécurité globale des entreprises, *Sécurité et stratégie*, Volume 22, n° 2, 2016, pp. 21-29.

DELESSE Claude, NSA *National Security Agency. L'histoire de la plus secrète des agences de renseignement*, Tallandier, 2016.

DUBUISSON François, La Cour européenne des droits de l'homme face à la surveillance de masse, *Revue trimestrielle des droits de l'Homme*, Volume 129, n° 1, 2022, pp. 123-141.

GANASCIA Jean-Gabriel, Peur du traçage - traçage de la peur, *Revue de neuropsychologie*, Volume 13, n° 2, 2021, pp. 148-152.

LANNA Maximilien, Objets connectés et protection des données à caractère personnel : vers un changement de paradigme des modalités de protection ?, *Droits*, Volume 68, n° 2, 2018, pp. 223-235.

LOVELUCK Benjamin, HOLEINDRE Jean-Vincent, Politiques du hacking : enquête sur les ruses numériques, *Quaderni*, Volume 103, n° 2, 2021, pp. 9-24.

MONGIN Pierre, TOGNINI Franck, Chapitre 4. La protection et la sécurité informatique, in MONGIN Pierre, TOGNINI Franck, *Petit manuel d'intelligence économique au quotidien. Gérer ses données à l'ère de Big Brother*, Dunod, 2015, pp. 55-69.