RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

PIRATAGE D'UN SYSTÈME INFORMATIQUE

Un système informatique désigne tout appareil, ou ensemble d'appareils, permettant de traiter et stocker des données : ordinateur, tablette, téléphone mobile… Le piratage d'un système informatique se définit comme l'accès non autorisé à ce système par un tiers. En pratique, les cybercriminels peuvent s'introduire dans un système informatique, par l'utilisation d'une faille de sécurité ou d'un défaut de configuration de l'appareil ; l'infection par un logiciel malveillant (virus) ; le vol d'identifiants de connexion suite à un appel ou un message frauduleux (hameçonnage) ; en devinant un mot de passe trop simple ou un mot de passe par défaut qui n'aurait pas été changé… Une fois introduit, le cybercriminel peut chercher à se propager dans les autres appareils du système.

BUT RECHERCHÉ

Prendre le contrôle de l'appareil et dérober des informations personnelles ou confidentielles pour en faire un usage frauduleux : usurpation d'identité, espionnage, fraude bancaire, etc.

SI VOUS ÊTES VICTIME

DÉCONNECTEZ L'APPAREIL d'Internet ou du réseau informatique.

IDENTIFIEZ LA SOURCE DE L'INTRUSION (faille de sécurité, message malveillant…) pour la corriger afin qu'elle ne puisse pas se reproduire.

IDENTIFIEZ TOUTE ACTIVITÉ INHABITUELLE : nouveaux comptes utilisateurs ou administrateurs, programmes ou processus inconnus…

ÉVALUEZ L'ÉTENDUE DE L'INTRUSION à d'autres appareils.

RÉCUPÉREZ LES PREUVES. Mettez de côté les machines touchées à disposition des enquêteurs.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie dont vous dépendez avec toutes les preuves en votre possession.

RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN) des appareils touchés afin de vérifier qu'ils ne sont pas affectés par un virus.

SAUVEGARDEZ VOS DONNÉES PERSONNELLES (photos, vidéos, documents personnels, etc.) sur un autre support (disque dur, clef USB…).

RÉINSTALLEZ LE SYSTÈME à partir d'une sauvegarde antérieure à l'attaque.

CHANGEZ LES MOTS DE PASSE d'accès aux appareils touchés.

Après la réinstallation de votre système **METTEZ À JOUR LES LOGICIELS ET APPAREILS**.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS SPÉCIALISÉS que vous pourrez trouver sur www.cybermalveillance.gouv.fr.

MESURES PRÉVENTIVES

Mettez à jour régulièrement votre appareil, votre système d'exploitation et ses logiciels.

Utilisez un antivirus et mettez-le à jour régulièrement.

N'installez pas de logiciels, programmes, applications « piratées » ou dont l'origine ou la réputation sont douteuses.

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens provenant d'expéditeurs inconnus ou dont le contenu est inhabituel.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons ou certains sites pornographiques qui peuvent infecter votre machine en cours de navigation.

N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

Faites des sauvegardes régulières et déconnectées de vos données et de votre système pour pouvoir le réinstaller au besoin.

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute.

Éteignez votre machine lorsque vous ne vous en servez pas.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- L'infraction d'**atteinte à un système de traitement automatisé de données (STAD)** peut être retenue. Les **articles 323-1 à 323-7 du code pénal** disposent notamment que : « *le fait d'accéder ou de se maintenir frauduleusement* » dans un STAD, « *la suppression ou la modification de données contenues dans le système* », « *le fait [...] d'extraire, de détenir, de reproduire, de transmettre [...] les données qu'il contient* » ou l'« *altération du fonctionnement de ce système* » sont passibles de trois à cinq ans d'emprisonnement et de 100 000 à 150 000 euros d'amende.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V230417