RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

COMPRENDRE LES RISQUES

LES VIRUS INFORMATIQUES

Un virus est un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire. Il existe différents types de virus comme le rançongiciel, le cheval de Troie, le logiciel espion… Les virus peuvent s'infiltrer dans un système informatique par l'ouverture d'un message (mail, MMS, chat), d'une pièce jointe ou d'un clic sur un lien frauduleux, par exemple. Il peut aussi s'introduire en naviguant sur un site malveillant, en s'installant dans un appareil ou un logiciel non mis à jour, par l'absence d'utilisation d'un antivirus, l'installation d'une application piratée, etc. Les symptômes d'une infection par un virus peuvent se manifester par une alerte de l'antivirus, un ralentissement ou un blocage anormal de l'appareil, des fenêtres ou des messages d'erreur qui s'affichent sans raison, la modification de logiciels ou programmes, etc.

BUT RECHERCHÉ

Prendre le contrôle d'un système informatique pour en faire un usage frauduleux, espionner l'utilisateur, dérober des données personnelles et/ou confidentielles, attaquer d'autres appareils, chiffrer les fichiers et demander une rançon, etc.

SI VOUS ÊTES VICTIME

DÉCONNECTEZ L'ÉQUIPEMENT INFECTÉ D'INTERNET OU DU RÉSEAU pour éviter que le virus ne se propage à d'autres appareils.

IDENTIFIEZ LA SOURCE DE L'INFECTION ET SON ÉTENDUE (faille de sécurité, message malveillant) et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

RÉCUPÉREZ OU TENTEZ DE FAIRE RÉCUPÉRER PAR UN PROFESSIONNEL LES PREUVES DISPONIBLES. Séquestrez la ou les machines touchées ou réalisez-en une copie physique complète.

Avant de remettre en état votre système, et en fonction du préjudice subi, **DÉPOSEZ PLAINTE** au commissariat de police ou à la brigade de gendarmerie ou en adressant votre plainte au procureur de la République du tribunal judiciaire dont vous dépendez.

Après avoir vérifié que votre antivirus est en état de fonctionnement et à jour, **FAITES UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN) DE VOS APPAREILS** et supprimez les virus.

CHANGEZ AU PLUS VITE VOS MOTS DE PASSE au moindre doute sur leur piratage.

RESTAUREZ VOTRE SYSTÈME si les symptômes de l'infection continuent de se manifester.

RÉINITIALISEZ OU RÉINSTALLEZ COMPLÈTEMENT VOTRE APPAREIL EN DERNIER RECOURS si le virus persiste toujours.

MESURES PRÉVENTIVES

Utilisez un antivirus et mettez-le à jour régulièrement.

Mettez régulièrement à jour votre appareil, votre système d'exploitation ainsi que les logiciels et applications installés.

N'installez pas de logiciels, programmes, applications ou équipements « piratés » 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 de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

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

Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute (tous nos conseils pour gérer vos mots de passe).

N'utilisez pas de supports amovibles dont vous ne connaissez pas la provenance (clé USB trouvée, etc.).

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 sept ans d'emprisonnement et de 100 000 à 300 000 euros d'amende.

- **En cas de rançongiciel :**
  De tels procédés relèvent de l'**extorsion de fonds** et non de l'escroquerie. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire. L'**article 312-1 du code pénal** dispose que : « *l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende* ».

- **En cas d'usage d'une identité volée et/ou d'utilisation de données personnes volées à la victime :**
  L'**article 226-4-1 du code pénal** créé par LOI n° 2011-267 du 14 mars 2011 - art. 2 dispose que « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.* »

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

V230417