Les types de menaces

Sommaire :

Qu'est ce qu'un cheval de Troie / Qu'est ce qu'un Adware, Pornware, Riskware et le Ransomware / Virus informatiques et les mythes / Les méthodes d'infection courantes / Les signes indiquant que votre ordinateur est infecté

Qu'est ce qu'un cheval de Troie ?

Un cheval de Troie est un type de programme malveillant se faisant passer bien souvent pour un logiciel authentique. Les chevaux de Troie peuvent être utilisés par des cybercriminels et des pirates informatiques pour accéder aux systèmes des utilisateurs. Ces derniers sont généralement incités, par le biais d'une technique d'ingénierie sociale, à charger et exécuter des chevaux de Troie sur leurs systèmes. Une fois activés, les chevaux de Troie peuvent permettre aux cybercriminels de vous espionner, de dérober vos données sensibles et d'accéder à votre système à l'aide d'un backdoor. Ces actions peuvent être les suivantes :

- Suppression de données
- Blocage de données
- Modification de données
- Copie de données
- Perturbation des performances des ordinateurs ou des réseaux informatiques

Contrairement aux virus et aux vers informatiques, les chevaux de Troie ne s'auto-répliquent pas.

Quel peut être l'impact des chevaux de Troie sur vous ?

La classification des chevaux de Troie dépend du type d'action qu'ils peuvent effectuer sur votre ordinateur :

- **Backdoor**
  Un cheval de Troie utilisant les backdoors permet à un utilisateur malveillant de contrôler l'ordinateur infecté à distance. Son auteur peut alors effectuer tout ce qu'il souhaite sur l'ordinateur infecté (envoi, réception, exécution et suppression de fichiers, affichage de données et redémarrage de l'ordinateur, par exemple). Les chevaux de Troie utilisant les backdoors sont souvent employés pour regrouper des ordinateurs infectés afin de former un botnet ou un réseau zombie à des fins criminelles.
- **Failles d'exploitation**
  Les failles d'exploitation sont des programmes contenant des données ou du code qui profitent de la vulnérabilité d'une application exécutée sur votre ordinateur.

- **Rootkits**
  Les rootkits (ou dissimulateurs) sont conçus pour dissimuler certains objets ou activités dans votre système. Leur principal objectif est bien souvent d'empêcher la détection de programmes malveillants afin de prolonger la période d'exécution de ces derniers sur un ordinateur infecté.
- **Cheval de Troie bancaire**
  Ces programmes sont conçus pour dérober les données d'accès à vos comptes bancaires en ligne, comptes de paiement électronique et cartes de crédit ou de débit.
- **Cheval de Troie DDoS**
  Ces programmes lancent des attaques DoS (Denial of Service, déni de service) contre une adresse Web ciblée. L'envoi de requêtes multiples (à partir de votre ordinateur ou de plusieurs autres ordinateurs infectés) permet de submerger l'adresse ciblée jusqu'au déni de service.
- **Cheval de Troie téléchargeur**
  Ces programmes peuvent télécharger et installer de nouvelles versions de programmes malveillants sur votre ordinateur, y compris des chevaux de Troie et des adware.
- **Cheval de Troie dropper**
  Ces programmes sont utilisés par les pirates informatiques pour installer des chevaux de Troie et/ou des virus, ou pour empêcher la détection de programmes malveillants. Certains programmes antivirus ne sont pas capables d'analyser tous les composants des chevaux de Troie de ce type.
- **Cheval de Troie faux antivirus**
  Ces programmes simulent l'activité d'un logiciel antivirus. Ils sont conçus pour vous extorquer de l'argent en échange de la détection et de la suppression des menaces mais les menaces qu'ils signalent n'existent pas.
- **Cheval de Troie voleur de données de joueurs**

  Ces programmes dérobent les informations de compte des joueurs en ligne.
- **Cheval de Troie messagerie instantanée**

  Ces programmes dérobent les identifiants et mots de passe de vos messageries instantanées (ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype, etc.).
- **Cheval de Troie rançonneur**
  Ces programmes peuvent modifier les données présentes sur votre ordinateur pour entraver le fonctionnement de ce dernier ou vous empêcher d'utiliser certaines données.

Vos données ne sont débloquées ou les performances de votre ordinateur rétablies qu'après le paiement de la rançon exigée.

- **Cheval de Troie SMS**
  Ces programmes peuvent vous coûter de l'argent en utilisant votre appareil mobile pour envoyer des SMS vers des numéros de téléphone surtaxés.
- **Cheval de Troie espion**
  Ces programmes peuvent espionner votre ordinateur, par exemple, enregistrer les données que vous saisissez sur votre clavier, effectuer des captures d'écran ou récupérer la liste des applications que vous utilisez.
- **Cheval de Troie récupérateur d'adresses électroniques**
  Ces programmes peuvent récupérer les adresses électroniques enregistrées sur votre ordinateur.
- **Autres types de chevaux de Troie :**
  - Cheval de Troie bombe d'archives
  - Cheval de Troie cliqueur
  - Cheval de Troie notificateur
  - Cheval de Troie proxy
  - Cheval de Troie voleur de mots de passe

Comment vous protéger contre les chevaux de Troie ?

Un bon logiciel de protection contre les programmes malveillants vous permettra de protéger vos appareils (PC, ordinateurs portables, Mac, tablettes et smartphones) contre les chevaux de Troie. Une solution rigoureuse de protection contre les programmes malveillants, comme Kaspersky Anti-Virus, détectera et préviendra les attaques de chevaux de Troie sur votre PC, tandis que Kaspersky Mobile Security protégera efficacement vos smartphones Android des virus. Kaspersky Lab propose des produits de protection contre les programmes malveillants qui défendent les appareils suivants contre les chevaux de Troie :

- PC Windows
- Ordinateurs Linux
- Mac Apple
- Smartphones
- Tablettes

Qu'est ce qu'un Adware, Pornware, Riskware ?

Le terme « adware » désigne les programmes conçus pour afficher des publicités sur votre ordinateur, rediriger vos demandes de recherche vers des

sites publicitaires et recueillir des données marketing vous concernant (par exemple, types de sites Internet que vous consultez) afin de vous adresser des publicités personnalisées.

Les adware qui recueillent des données avec votre autorisation ne doivent pas être confondus avec des chevaux de Troie espions qui recueillent des informations à votre insu. Si l'adware recueille des informations à votre insu, il est considéré comme malveillant (programme malveillant présentant le comportement d'un cheval de Troie espion, par exemple).

Quel peut être l'impact des adware sur vous ?

Outre l'affichage de publicités et le recueil de données, les adware ne signalent généralement pas leur présence. Le plus souvent, le programme n'apparaît pas sur la barre d'état système et rien n'indique que des fichiers ont été installés sur votre ordinateur.

Les adware peuvent s'installer sur votre ordinateur de deux façons :

- **Via un freeware ou un shareware**
  Des adware peuvent être inclus dans certains freeware ou shareware afin de générer légalement des revenus publicitaires permettant de financer le développement et la distribution du logiciel en question.
- **Sites Internet infectés**
  Toute consultation d'un site Internet infecté peut entraîner l'installation non autorisée d'adware sur votre ordinateur. Des technologies de piratage informatique sont souvent utilisées. Par exemple, l'adware peut s'introduire sur votre ordinateur via une vulnérabilité du navigateur, et des chevaux de Troie conçus pour s'installer furtivement peuvent être utilisés. Les adware qui agissent ainsi sont souvent appelés Browser Hijackers (pirates de navigateur).

Comment vous protéger contre les adware ?

Généralement, les adware ne sont dotés d'aucune fonctionnalité de désinstallation et ils peuvent employer des technologies semblables à celles utilisées par les virus pour s'introduire sur votre ordinateur et s'y exécuter à votre insu. Toutefois, dans la mesure où l'adware peut avoir été légalement installé sur votre ordinateur, les solutions antivirus ne permettent pas toujours de déterminer s'il représente une menace. Les produits de Kaspersky Lab vous permettent d'activer ou de désactiver l'option de détection des adware, et de choisir le mode de réaction :

- **Suppression d'un adware**
  Différentes raisons peuvent vous amener à soupçonner un programme adware détecté par le moteur antivirus de Kaspersky Lab d'être une menace, notamment si vous n'avez pas autorisé l'installation du programme et que vous ignorez d'où il vient, ou si vous avez lu une description de ce programme sur le site Internet de Kaspersky Lab et que

vous vous inquiétez pour votre sécurité. Dans ce cas, le logiciel antivirus de Kaspersky Lab vous aidera à vous débarrasser du programme adware.

- **Non-détection des adware**
  Lorsque des adware que vous avez autorisés sont détectés, vous pouvez estimer qu'ils ne représentent aucune menace pour vos ordinateurs, appareils ou données. Les produits Kaspersky Lab vous permettent de désactiver l'option de détection de ces programmes ou d'ajouter des programmes spécifiques à une liste d'exceptions afin que le moteur antivirus ne les désigne pas comme malveillants.

De nombreux freeware et shareware cessent d'afficher les publicités à l'issue de l'enregistrement ou de l'achat d'un programme. Certains programmes utilisent cependant des adware tiers qui, dans certains cas, peuvent rester installés sur votre ordinateur après l'enregistrement ou l'achat du programme. En outre, la suppression du programme adware peut parfois entraîner un dysfonctionnement du programme.

Le pornware :

Le terme « pornware » désigne une catégorie de programmes qui affiche du contenu pornographique sur un ordinateur ou périphérique. Outre les programmes que certains utilisateurs peuvent délibérément installer sur leurs ordinateurs et périphériques mobiles pour rechercher et afficher du contenu pornographique, le terme « pornware » désigne également les programmes installés de façon malveillante à l'insu des utilisateurs. L'objectif d'un pornware indésirable est souvent de promouvoir des sites Web et services pornographiques gratuits.

Quel peut être l'impact des pornware sur vous ?

Les développeurs de programmes malveillants peuvent exploiter les vulnérabilités des applications et systèmes d'exploitation les plus courants pour installer un pornware sur l'ordinateur, la tablette ou le smartphone d'un utilisateur. En outre, les chevaux de Troie téléchargeurs et dropper peuvent être utilisés pour infecter un appareil avec un pornware.
Exemples de pornware :

- **Composeurs de numéros pornographiques**
  Ces programmes composent des numéros de téléphone ou de services proposant des « contenus pour adultes » et/ou un code spécial. Contrairement aux programmes malveillants, ils avertissent l'utilisateur de leurs actions.
- **Téléchargeurs de contenus pornographiques**
  Ces programmes téléchargent des fichiers multimédias pornographiques sur l'ordinateur de l'utilisateur à partir d'Internet. Contrairement aux programmes malveillants, ils avertissent l'utilisateur de leurs actions.

- **Outils pornographiques**
  Ces programmes recherchent et affichent sur l'ordinateur de l'utilisateur des contenus pornographiques tels que des barres d'outils pour navigateurs Internet et des lecteurs vidéo spéciaux.

Comment vous protéger contre les pornware ?

Dans la mesure où le pornware peut avoir été délibérément téléchargé par l'utilisateur, les solutions antivirus ne permettent pas toujours de déterminer s'il représente une menace pour son ordinateur ou son périphérique.
Les produits de Kaspersky Lab permettent aux utilisateurs d'activer ou de désactiver l'option de détection des pornware, et de choisir le mode de réaction :

- **Détection et suppression de pornware**
  Différentes raisons peuvent amener l'utilisateur à soupçonner un pornware détecté par le moteur antivirus de Kaspersky d'être une menace, notamment s'il n'a pas autorisé l'installation du programme et qu'il ignore d'où il vient, ou encore s'il a lu une description de ce programme sur le site Web de Kaspersky et qu'il s'inquiète pour sa sécurité. Dans ce cas, le logiciel antivirus de Kaspersky aidera l'utilisateur à se débarrasser du pornware.
- **Non-détection des pornware**
  Lorsque des pornware délibérément téléchargés par l'utilisateur sont détectés, ce dernier peut estimer qu'ils ne représentent aucune menace pour ses ordinateurs, périphériques ou données. Les produits Kaspersky permettent à l'utilisateur de désactiver l'option de détection de ces programmes ou d'ajouter des programmes spécifiques à une liste d'exceptions afin que le moteur antivirus ne les désigne pas comme malveillants.

Le riskware :

Le terme « riskware » désigne des programmes légaux susceptibles de causer des préjudices lorsqu'ils sont exploités par des utilisateurs malintentionnés en vue de supprimer, bloquer, modifier ou copier des données, et perturber les performances des ordinateurs ou des réseaux. Les riskware peuvent englober différents types de programmes couramment utilisés à des fins légales :

- Utilitaires d'administration distants
- Clients IRC
- Numéroteurs
- Téléchargeurs de fichiers
- Logiciels de suivi de l'activité
- Utilitaires de gestion des mots de passe
- Services de serveurs Internet tels que FTP, Web, proxy et Telnet

Ces programmes ne sont pas conçus pour être malveillants, mais ils sont dotés de fonctions qui peuvent être utilisées à des fins malveillantes.

Quel peut être l'impact des riskware sur vous ?

Compte tenu du grand nombre de programmes légaux que les utilisateurs malintentionnés peuvent employer à des fins illégales, il peut être difficile pour les utilisateurs d'identifier les programmes susceptibles de représenter un risque. Par exemple, des programmes d'administration distants sont souvent utilisés par les administrateurs systèmes et par les services d'assistance pour diagnostiquer et résoudre les problèmes qui surviennent sur les ordinateurs des utilisateurs. Toutefois, si un tel programme a été installé à votre insu sur votre ordinateur par un utilisateur malintentionné, celui-ci pourra accéder à votre ordinateur à distance. Dès qu'il aura pris le contrôle de votre ordinateur, cet utilisateur pourra l'utiliser comme bon lui semble.

- Kaspersky Lab a répertorié des incidents au cours desquels des programmes d'administration distants légaux (comme WinVNC) ont été secrètement installés dans le but d'accéder à distance à un ordinateur.
- Autre exemple, l'utilitaire mIRC (client réseau IRC légal) peut être utilisé à des fins malveillantes par des utilisateurs malintentionnés. Des chevaux de Troie utilisant les fonctions de mIRC pour transmettre des charges malveillantes à l'insu de l'utilisateur sont régulièrement identifiés par Kaspersky. Les programmes malveillants installent souvent le client mIRC pour une utilisation malveillante ultérieure. Dans ce cas, mIRC est généralement enregistré dans le dossier Windows et dans ses sous-dossiers. Par conséquent, la présence de mIRC dans ces dossiers indique généralement que l'ordinateur a été infecté par un programme malveillant.
- Les riskware peuvent englober les comportements suivants :
    - Client-IRC
    - Client-P2P
    - Client-SMTP
    - Numéroteur
    - Téléchargeur
    - Outil de fraude
    - des vulnérabilités
    - NetTool
    - PSWTool
    - RemoteAdmin
    - RiskTool
    - Serveur-FTP
    - Serveur-Proxy
    - Serveur-Telnet
    - Serveur-Web
    - Barre d'outils Internet

Comment vous protéger contre les riskware ?

Dans la mesure où le riskware peut avoir été légalement installé sur votre ordinateur, les solutions antivirus ne permettent pas toujours de déterminer s'il représente une menace. Les produits de Kaspersky vous permettent d'activer ou de désactiver l'option de détection des riskware, et de choisir le mode de réaction :

- **Détection et suppression des riskware**
  Différentes raisons peuvent vous amener à soupçonner un riskware détecté par le moteur antivirus de Kaspersky d'être une menace, notamment si vous n'avez pas autorisé l'installation du programme et que vous ignorez d'où il vient, ou si vous avez lu une description de ce programme sur le site Web de Kaspersky et que vous vous inquiétez pour votre sécurité.
- **Non-détection des riskware**
  Lorsque des riskware que vous avez autorisés sont détectés, vous pouvez estimer qu'ils ne représentent aucune menace pour vos ordinateurs, périphériques ou données. Les produits Kaspersky vous permettent de désactiver l'option de détection de ces programmes ou d'ajouter des programmes spécifiques à une liste d'exceptions afin que le moteur antivirus ne les désigne pas comme malveillants.

Qu'est ce qu'un Ransomware (Rançonlogiciel) ?

DÉFINITION DE SÉCURITÉ

Les ransomware sont des logiciels malveillants qui infectent votre ordinateur et affichent des messages demandant de verser une certaine somme afin que votre système fonctionne à nouveau. Cette catégorie de programmes malveillants est une arnaque lucrative et criminelle qui peut être installée en cliquant sur des liens trompeurs dans un e-mail, via la messagerie instantanée ou un site Internet. ***acité de verrouiller l'écran d'un ordinateur ou de***

Exemples de ransomware

Scareware est le type de ransomware le plus simple. Il utilise la peur ou l'intimidation pour inciter les victimes à payer. Il peut prendre la forme d'un faux logiciel antivirus dans lequel un message s'affiche soudainement, prétendant que votre ordinateur a plusieurs problèmes et qu'il est nécessaire de procéder à un paiement en ligne pour les résoudre !

Le niveau de ce type d'attaques varie. Parfois, les utilisateurs sont sans cesse bombardés de messages pop-up et d'avertissements. D'autres fois, l'ordinateur ne fonctionnera plus du tout. Il existe encore un autre type de ransomware, qui peut se faire passer pour un organe de répression en ouvrant une page qui semble provenir du bureau local d'un organe de répression et qui indique que l'utilisateur de l'ordinateur a été pris en train d'exercer des activités illégales

sur Internet. Les fichiers sont par la suite bloqués dans des dossiers chiffrés et difficiles à décoder, de sorte que les utilisateurs ne puissent pas récupérer leurs données sans payer la rançon.

En général, les attaques typiques demandent 100 à 200 dollars. D'autres attaques peuvent viser plus haut, notamment si le pirate sait que les données retenues en otage peuvent engendrer une perte financière directe et significative pour l'entreprise. Par conséquent, les cybercriminels qui mettent au point ces arnaques peuvent gagner d'importantes sommes d'argent.

Quel que soit le scénario, même si la rançon est payée, il n'est nullement garanti que les utilisateurs de l'ordinateur pourront à nouveau accéder à leur système dans son intégralité. Bien que certains pirates informatiques demandent aux victimes de payer via Bitcoin, MoneyPak ou d'autres méthodes en ligne, ils peuvent également demander les données relatives aux cartes de crédit, entraînant ainsi des pertes financières plus élevées.

Histoire des ransomware

Les premiers cas ont été signalés en Russie en 2005. Depuis lors, les arnaques se sont propagées dans le monde entier, avec de nouveaux types qui réussissent encore à cibler leurs victimes. En septembre 2013, CryptoLocker a fait surface et a ciblé toutes les versions de Windows ! Il a réussi à infecter des centaines de milliers d'ordinateurs de particuliers et de systèmes informatiques d'entreprises. Les victimes ont sans le savoir ouvert des e-mails provenant soi-disant des services d'assistance à la clientèle de FedEx, UPS, DHS et d'autres sociétés. Une fois activé, le chronomètre que le programme malveillant affiche à l'écran demandait un paiement moyen de 300 dollars dans les 72 heures. Certaines versions ont affecté les fichiers locaux et les supports amovibles. L'organisme américain CERT (Computer Emergency Response Team) a prévenu que le programme malveillant était capable de passer d'une machine à l'autre et a conseillé aux utilisateurs d'ordinateurs infectés de déconnecter immédiatement leurs machines des réseaux.

Les experts en sécurité de Kaspersky Lab ont réussi à déchiffrer les données piratées, mais ils ont admis que cela n'était pas toujours possible en cas de chiffrement complexe, comme c'est le cas avec CryptoLocker. Il est essentiel que les particuliers et les entreprises fassent régulièrement des sauvegardes de leurs ordinateurs pour prévenir la perte de données importantes.

Prévention et suppression

Les utilisateurs d'ordinateurs doivent s'assurer que leurs pare-feu sont activés, éviter les sites douteux et faire preuve de précaution en ouvrant les e-mails suspects. Le fait de choisir un logiciel antivirus d'une société de renom peut vous aider à protéger votre ordinateur contre les ransomware les plus récents.

Les différents virus informatiques :

Les utilisateurs de PC, de Mac, de smartphones et de tablettes sont exposés à l'évolution constante des menaces que représentent les virus informatiques et les programmes malveillants. Prendre des mesures de protection signifie comprendre ce à quoi vous êtes exposé. Voici un aperçu des principaux types de programmes malveillants et de leur impact potentiel.

1. Virus informatiques

Les virus informatiques ont acquis ce nom en raison de leur capacité à « infecter » plusieurs fichiers sur un ordinateur. Ils se propagent sur les autres machines lorsque des fichiers infectés sont envoyés par e-mail ou lorsque des utilisateurs les transportent sur des supports physiques tels que des clés USB ou des disquettes (au début). Selon le National Institute of Standards and Technology (NIST), le premier virus informatique, appelé « Brain », a été développé en 1986. Lassés de voir les clients pirater les logiciels de leur magasin, deux frères prétendent avoir conçu le virus permettant d'infecter le secteur d'amorçage des disquettes des voleurs, propageant ainsi le virus lors de leur copie.

2. Vers

Contrairement aux virus, les vers ne nécessitent pas d'intervention humaine pour se propager et infecter les ordinateurs : il s'agit d'un programme capable d'utiliser des réseaux informatiques pour infecter les autres machines connectées sans l'aide des utilisateurs. En exploitant les vulnérabilités des réseaux telles que les failles des programmes de messagerie électronique, les vers peuvent se répliquer des milliers de fois en vue d'infecter de nouveaux systèmes dans lesquels le processus se reproduira. Bien que de nombreux vers utilisent simplement les ressources système, réduisant ainsi les performances, la plupart d'entre eux contiennent des « charges utiles » malveillantes conçues pour dérober ou supprimer des fichiers.

3. Adware

Les adware représentent l'une des nuisances les plus couramment rencontrées en ligne. Les programmes envoient automatiquement des publicités aux ordinateurs hôtes. Les types de programmes adware courants incluent des publicités contextuelles sur les pages Web et des publicités intégrées au programme qui accompagnent bien souvent un logiciel « gratuit ». Bien que certains adware soient relativement sans danger, d'autres variantes utilisent des outils de suivi permettant de récupérer des informations sur votre site ou sur votre historique de navigation et affichent des publicités ciblées sur votre écran. Comme le fait observer BetaNews, une nouvelle forme d’adware capable de désactiver votre logiciel antivirus a été détectée. Le programme adware étant installé avec le consentement des personnes après les en avoir informé,

de tels programmes ne peuvent donc pas être appelés programmes malveillants : ils sont généralement identifiés en tant que « programmes potentiellement indésirables ».

4. Logiciels espions

Un logiciel espion agit comme son nom l'indique, à savoir, espionner ce que vous faites sur votre ordinateur. Il recueille des données telles que les saisies clavier, vos habitudes de navigation et vos informations de connexion qui sont alors envoyées à des tiers, généralement des cybercriminels. Il peut également modifier des paramètres de sécurité spécifiques sur votre ordinateur ou interférer avec les connexions réseau. TechEye révèle que de nouvelles formes de logiciels espions peuvent permettre à des entreprises de suivre le comportement des utilisateurs sur plusieurs appareils, à leur insu.

5. Ransomware

Les ransomware infectent votre ordinateur, puis chiffrent des données sensibles telles que des documents personnels ou des photos, puis demandent une rançon pour les récupérer. Si vous refusez de payer, les données sont supprimées. Certaines variantes de ransomware verrouillent l'accès à votre ordinateur. Ils peuvent prétendre provenir d'organismes légitimes chargés de faire appliquer la loi et suggérer que vous vous êtes fait prendre pour avoir mal agi. En juin 2015, Internet Crime Complaint Center du FBI a reçu des plaintes d'utilisateurs signalant 18 millions de dollars de pertes dues à un ransomware courant appelé CryptoWall.

6. Robots

Les robots sont des programmes conçus pour exécuter automatiquement des opérations spécifiques. Ils sont utilisés à de nombreuses fins légales, mais ont été redéfinis comme un type de programme malveillant. Une fois dans l'ordinateur, les robots peuvent faire en sorte que la machine exécute des commandes spécifiques sans que l'utilisateur ne les autorise ou n'en soit informé. Les pirates informatiques peuvent également tenter d'infecter plusieurs ordinateurs avec le même robot afin de créer un « botnet » (contraction des termes « robot » et « network » (réseau), qui peut alors être utilisé pour gérer à distance des ordinateurs infectés (pour dérober des données sensibles, espionner les activités de la victime, distribuer automatiquement des spams ou lancer des attaque DDoS dévastatrices sur des réseaux informatiques).

7. Rootkits

Les rootkits autorisent un tiers à accéder ou contrôler à distance un ordinateur. Ces programmes permettent aux professionnels de l'informatique de résoudre à distance des problèmes de réseau mais ils peuvent également devenir malveillants : une fois installés sur votre ordinateur, les pirates peuvent prendre le contrôle de votre machine pour dérober des données ou installer d'autres composants du programme malveillant. Les rootkits sont conçus pour passer inaperçus et masquer activement leur présence. La détection de ce type de code malveillant nécessite la surveillance manuelle de comportements inhabituels ainsi que l'application régulière de correctifs sur votre système d'exploitation et vos logiciels afin d'éliminer les chemins d'accès potentiels d'infection.

8. Chevaux de Troie

Ces programmes se fondent en se faisant passer pour des fichiers ou des logiciels légitimes. Une fois téléchargés et installés, ils modifient un ordinateur et conduisent des activités malveillantes, à l'insu de la victime.

9. Bugs

Les bugs ou failles d'un code logiciel ne correspondent pas à un type de programme malveillant mais à des erreurs commises par un programmeur. Ils peuvent avoir des conséquences néfastes sur votre ordinateur : blocage, panne ou réduction des performances. Les bugs de sécurité, quant à eux, permettent aisément aux pirates de passer outre vos défenses et d'infecter votre machine. Bien qu'un meilleur contrôle de la sécurité côté développeur facilite l'élimination des bugs, il est également essentiel d'appliquer des correctifs qui corrigent les bugs spécifiques en circulation.

Mythes et réalités

Il existe un certain nombre de mythes courants concernant les virus informatiques :

- **Tous les messages d'erreur informatiques révèlent un virus.**
  C'est faux. Les messages d'erreur peuvent également être dus à un matériel défaillant ou des bugs logiciels.
- **Les virus et les vers nécessitent systématiquement une interaction de l'utilisateur.**
  C'est faux. Le code doit être exécuté pour qu'un virus infecte un ordinateur mais l'utilisateur ne doit pas nécessairement interagir. Prenons l'exemple d'un ver il peut se propager automatiquement si l'ordinateur d'un utilisateur présente certaines vulnérabilités.

- **Les pièces jointes envoyées par des expéditeurs connus sont sans danger.**
  C'est inexact parce qu'elles peuvent avoir été infectées par un virus et être utilisées pour propager l'infection. Même si vous connaissez l'expéditeur, n'ouvrez aucune pièce jointe dont vous n'êtes pas certain de la fiabilité.
- **Les programmes antivirus bloqueront toutes les menaces.**
  Bien que les fournisseurs d'antivirus s'efforcent de rester au fait des développements de programmes malveillants, il est fondamental d'exécuter une solution de sécurité Internet complète qui intègre des technologies spécialement conçues pour bloquer les menaces de manière proactive. Il n'en demeure pas moins que rien ne vaut une sécurité à 100 pour cent. Il est donc important de faire preuve de bon sens en ligne pour diminuer le risque d'attaque.
- **Les virus peuvent causer des dommages physiques à votre ordinateur.**
  Et si un code malveillant entraînait la surchauffe de votre machine ou détruisait des puces électroniques critiques ? Les fournisseurs d'antivirus ont démystifiés cette théorie à de nombreuses reprises en indiquant qu'un tel dommage est tout simplement impossible.

En parallèle, l'augmentation des appareils interconnectés sur l'Internet des objets (IoT) soulève d'autres possibilités intéressantes : et si un véhicule infecté quitte la route ou un four « intelligent » infecté reçoit l'ordre de chauffer au maximum jusqu'à saturation ? L'avenir des programmes malveillants risque de faire de ce type de dommage physique une réalité.

Il existe un certain nombre d'idées fausses que se font les gens concernant les programmes malveillants, notamment supposer que l'infection est évidente. Bien souvent, les utilisateurs partent du principe qu'ils sauront si leur ordinateur a été infecté. Généralement, le programme malveillant ne laisse, toutefois, pas de trace et votre système n'affichera aucun signe d'infection.

De la même manière, ne pensez pas que tous les sites Internet de renom sont fiables. Si des pirates peuvent compromettre des sites Internet légitimes à l'aide d'un code infecté, les utilisateurs seront davantage susceptibles de télécharger des fichiers ou de communiquer leurs informations personnelles ; SecurityWeek révèle que c'est exactement ce qui s'est passé pour la Banque mondiale. Dans le même esprit, de nombreux utilisateurs pensent que leurs données personnelles (photos, documents et fichiers) n'ont aucune valeur pour les créateurs de programmes malveillants. Les cybercriminels exploitent les données publiques disponibles pour cibler des individus ou recueillir des renseignements leur permettant de créer des e-mails de phishing ciblé pour pénétrer à l'intérieur d'entreprises.

Méthodes d'infection courantes

Comment votre ordinateur est-il infecté par des virus informatiques ou des programmes malveillants ? Il existe plusieurs moyens d'y parvenir : cliquer sur des liens vous dirigeant vers des sites Internet malveillants à partir d'e-mails ou de messages sur les réseaux sociaux, visiter un site Internet infecté (technique du téléchargement intempestif) et connecter une clé USB infectée à votre ordinateur. Grâce aux vulnérabilités présentes dans les systèmes d'exploitation et dans les applications, les cybercriminels n'ont aucun mal à installer des programmes malveillants sur les ordinateurs. Il est, par conséquent, indispensable d'exécuter les mises à jour de sécurité dès leur publication afin de réduire votre exposition aux risques.

Les cybercriminels utilisent bien souvent l'ingénierie sociale pour vous inciter à faire quelque chose qui compromet votre sécurité ou celle de l'entreprise pour laquelle vous travaillez. Les e-mails de phishing sont l'une des méthodes les plus courantes. Vous recevez un e-mail en apparence légitime qui vous persuade de télécharger un fichier infecté ou de visiter un site Internet malveillant. Dans ce cas, les pirates informatiques cherchent à vous convaincre : alerte concernant la présence d'un prétendu virus, notification de votre banque ou message d'un vieil ami.

Les cybercriminels ciblent en priorité les données confidentielles telles que les mots de passe. Outre l’utilisation de programmes malveillants pour capturer les mots de passe, les cybercriminels recueillent également les mots de passe à partir de sites Internet et d'autres ordinateurs qu'ils ont piratés. C'est la raison pour laquelle il est impératif d'utiliser un mot de passe unique et fort pour chaque compte en ligne. Il doit notamment comporter 15 caractères au minimum et être composé de lettres, de chiffres et de caractères spéciaux. Ainsi, si l'un des comptes est piraté, les cybercriminels ne peuvent pas accéder à tous les autres comptes en ligne. Il est évident que si vous utilisez des mots de passe faciles à deviner, les cybercriminels risquent de ne pas avoir besoin d'infecter votre machine ou le site Internet d'un fournisseur en ligne. Malheureusement, la majorité des utilisateurs utilisent des mots de passe faibles. Plutôt que d'utiliser des mots de passe forts, difficiles à mémoriser, ils s'appuient sur des alternatives classiques telles que « 123456 » ou « motdepasse123 » que les pirates peuvent facilement deviner. Même les questions de sécurité peuvent ne pas s'avérer être une protection efficace parce que de nombreuses personnes fournissent la même réponse : à la question « Quel est votre plat favori ? », la réponse courante aux États-Unis est « Pizza ».

Signes indiquant que votre ordinateur est infecté

Bien que la plupart des programmes malveillants ne révèlent aucun signe avant-coureur et n'empêchent pas votre ordinateur de fonctionner normalement, des signes peuvent parfois révéler une infection. La réduction des performances arrive en tête de liste (exécution lente des processus, chargement plus long des fenêtres et programmes en apparence aléatoires fonctionnant en arrière-plan). Vous pouvez également observer une modification des pages d'accueil Internet dans votre navigateur ou des pop-ups publicitaires plus fréquents que d'habitude. Dans certains cas, le programme malveillant peut aussi avoir une incidence sur des fonctionnalités informatiques plus basiques : Windows peut ne pas s'ouvrir du tout et vous risquez de ne pas être en mesure de vous connecter à Internet ou d'accéder à des fonctionnalités de contrôle du système de plus haut niveau. Si vous suspectez une infection sur votre ordinateur, analysez votre système immédiatement. Si aucune anomalie n'est détectée mais que vous avez encore des doutes, demandez un deuxième avis en exécutant une autre solution antivirus.