Le Malware

1/ Définition du Malware

Le terme malware est un terme générique qui désigne tout type de logiciel malveillant (de l'anglais « malicious software ») conçu pour s'infiltrer dans votre appareil à votre insu. Il existe de nombreux types de malwares et chacun poursuit ses objectifs malfaisants selon une approche différente. Cependant, toutes les variantes de malwares ont deux caractéristiques communes : elles sont sournoises et elles vont à l'encontre de vos intérêts.

Les adwares, spywares, virus, botnets, chevaux de Troie, vers informatiques, rootkits et ransomwares relèvent tous de la définition de malware. Il est important de noter que les malwares ne sont pas une menace uniquement pour votre PC : les Mac et les appareils mobiles peuvent également être des cibles.

2/Fonctionnement d'un malware

Indépendamment de leur type, à la base, tous les malwares suivent le même schéma : L'utilisateur télécharge ou installe sans le vouloir le malware, qui infecte l'appareil.

La plupart des infections de malwares se produisent lorsque vous effectuez par inadvertance une action entraînant le téléchargement du logiciel malveillant. Par exemple, vous cliquez sur un lien contenu dans un e-mail ou vous vous rendez sur un site Web malveillant. Dans d'autres cas, les pirates informatiques propagent des malwares via des services de partage de fichiers peer-to-peer et des offres de téléchargement de logiciels gratuits. L'intégration d'un malware dans un torrent ou un téléchargement populaire est un moyen efficace de le diffuser sur une large base d'utilisateurs.Les appareils mobiles peuvent également être infectés via des SMS.

Une autre technique consiste à charger des logiciels malveillants dans le micrologiciel d'une clé USB. Étant donné que le malware est chargé sur le matériel interne de l'appareil (plutôt que sur son stockage de fichiers), il est peu probable que votre appareil parvienne à le détecter. C'est pourquoi vous ne devez jamais insérer de clé USB inconnue dans votre ordinateur.

Une fois le logiciel malveillant installé, il infecte votre appareil et commence à tout mettre en œuvre pour atteindre les objectifs du pirate. Ce qui distingue les différents types de malware les uns des autres est la façon de laquelle ils procèdent.

3/ Objectifs d'un malware

Le ransomware est la forme de malware la plus nocive et la plus directe. Alors que d'autres types fonctionnent sans être détectés, le ransomware fait immédiatement remarquer sa présence, en exigeant un paiement en échange de la restitution de l'accès à votre appareil ou à vos fichiers .

Certains types de malware n'ont aucun autre objectif que celui de nuire, effaçant des données importantes des machines infectées. En l'absence de fraude ou de vol, la seule récompense du hacker est la frustration et les revers subis par ses victimes.

4/ Stratégies de cybersécurité

Les malwares sont utilisés par les cybercriminels pour gagner de l'argent mais peuvent aussi être utilisés à des fins de sabotage, pour des motivations politiques. Stuxnet, par exemple, a été conçu pour perturber des équipements industriels très spécifiques.
De nombreuses attaques à motivation politique se sont répandues et ont fermé de grands réseaux IT.

5/ Différents de types de Malware

Spywares : ou logiciels espion : Ces programmes sont conçus pour surveiller la navigation sur le web des utilisateurs. Les spywares ne se propagent pas comme des virus ; ils sont généralement installés en exploitant les failles de sécurité. Ils peuvent également être cachés et empaquetés avec des logiciels non apparentés installés par l'utilisateur.

Ramsomwares: Ces malwares affectent d'une manière ou d'une autre un Système Informatique et exigent un paiement pour le ramener à son état normal. Par exemple, des programmes tels que CryptoLocker cryptent les fichiers en toute sécurité et ne les décryptent que sur paiement d'une somme d'argent importante.

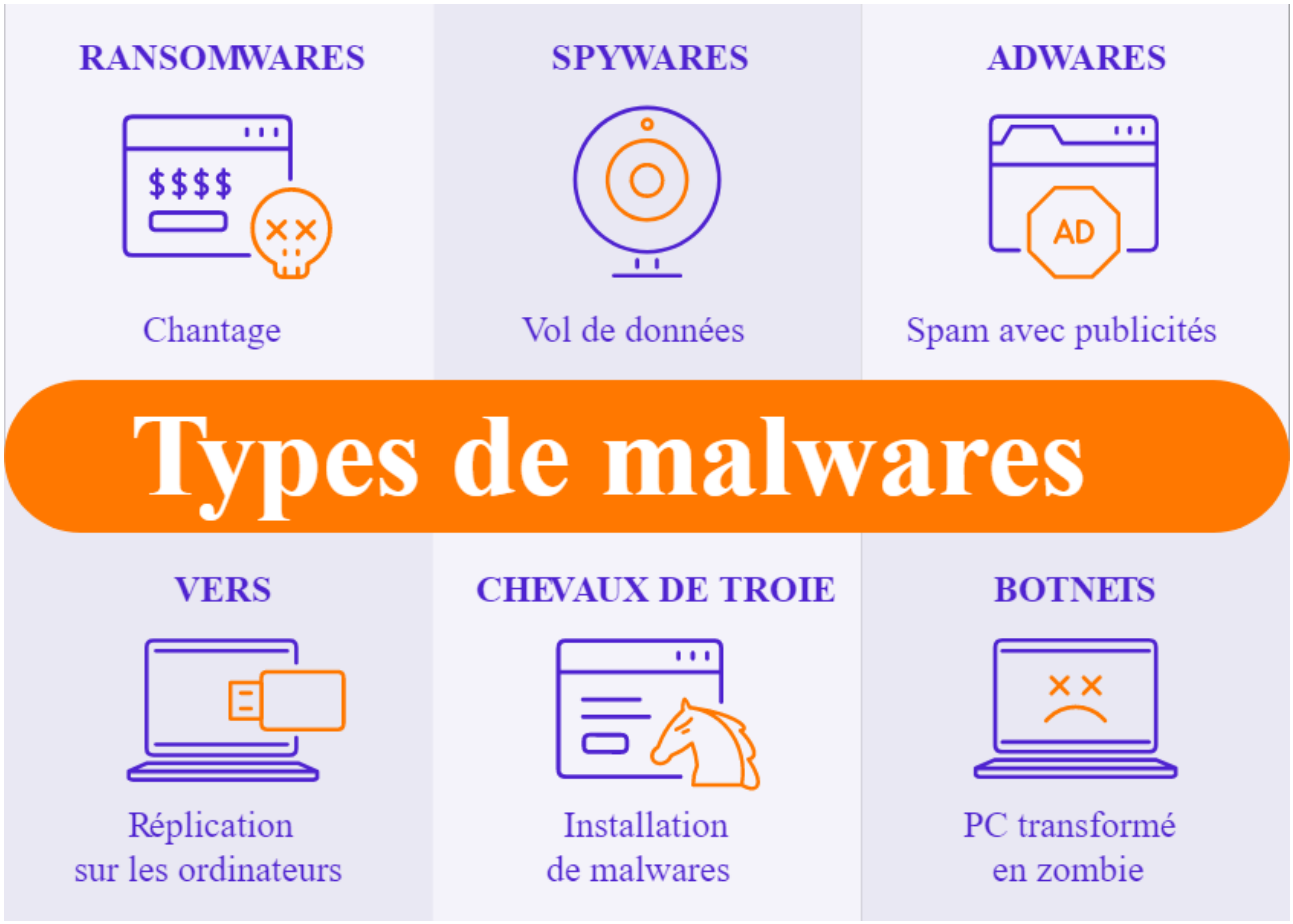
Vers informatique : Les vers poursuivent un seul et unique objectif : proliférer. Un ver infecte un ordinateur, puis s'auto-réplique et se propage vers d'autres appareils tout en restant actif sur toutes les machines qu'il infecte. Certains vers agissent un peu comme des livreurs et installateurs de malware. D'autres types sont conçus uniquement pour se propager, sans endommager intentionnellement leurs machines hôtes, mais ils continuent d'encombrer les réseaux en consommant la bande passante.

Adwares : Le rôle des adwares est de générer des revenus pour leur développeur en forçant la victime à voir des publicités indésirables. Les types d'adwares courants comprennent des jeux gratuits ou des barres d'outils de navigateur. Ils collectent des données personnelles sur la victime, puis les utilisent pour personnaliser les publicités qu'ils affichent. Bien que la plupart des adwares soient installés légalement, ils ne sont pas moins gênants que les autres types de malwares.

Les chevaux de Troie : Selon la légende qui nous est contée par les poètes grecs de l'Antiquité, les guerriers athéniens, cachés dans un gigantesque cheval en bois, en sont ressortis lorsque les Troyens ont tiré le cheval à l'intérieur des murs de la ville. Un cheval de Troie est donc une sorte de véhicule pour les pirates cachés. Le malware de types Cheval de Troie s'infiltre dans l'appareil d'une victime sous l'apparence d'un logiciel légitime. Une fois installé, le cheval de Troie s'active, allant parfois jusqu'à télécharger des malwares supplémentaires.

Botnets : Un botnet n'est pas un type de malware, il s'agit plutôt d'un réseau d'ordinateurs ou un code informatique en mesure de créer ou de lancer un malware. Les pirates infectent un groupe d'ordinateurs à l'aide de logiciels malveillants appelés «bots», qui sont capables de recevoir des

commandes de leur contrôleur. Ces ordinateurs forment ensuite un réseau, permettant au contrôleur d'accéder à une puissance de traitement collective importante, qui peut être utilisée pour coordonner les attaques, envoyer du spam, voler des données et créer de fausses publicités sur votre navigateur.



7) Appareils pouvant être contaminés par un malware

Aucun appareil n'est à l'abri des malwares. Tout comme les PC, les appareils Android et Mac peuvent faire l'objet d'une attaque de malware. Et bien que les malwares iOS sient rares, les iPhones et iPads sont sensibles aux menaces de sécurité.

8) Comment savoir si l'appareil a été infecté ?

Votre appareil est plus lent que de coutume. Si vous avez remarqué un ralentissement soudain sans cause apparente, cela pourrait être dû à une infection par un malware. Lorsque le malware s'empare des ressources de traitement de votre appareil, la puissance disponible pour tout le reste diminue.

- Vous constatez un manque d'espace de stockage disponible. De nombreux types de malwares téléchargent et installent des fichiers et du contenu supplémentaires sur votre appareil. Une diminution soudaine de l'espace de stockage disponible peut être le signe que vous avez été infecté par un malware.
- Des fenêtres contextuelles et des programmes indésirables apparaissent sur votre appareil. Il s'agit de l'un des signes les plus marquants d'une infection de malware. Si vous êtes submergé de fenêtres publicitaires intempestives ou si vous trouvez de nouveaux

programmes étranges sur votre appareil, il est probable que les malwares soient les coupables.

9) Se débarraser d’un malware

Cependant, certains malwares peuvent être très difficiles à supprimer une fois qu'ils sont solidement ancrés dans un système. Un outil d’élimination de malware est le moyen le plus simple et le plus fiable de s'assurer que les malwares ont disparu pour de bon. Ils sont spécialement conçus pour détecter automatiquement les logiciels malveillants et les éliminer de votre appareil.

10) Se protéger d’un malware

Le moyen le plus sûr de se protéger des malwares est de se doter d'un programme antivirus solide obtenu auprès d'un fournisseur fiable comme Avast. Notre antivirus gratuit est régulièrement qualifié d’« excellent » par les experts du secteur, et selon AV Comparatives, il s’agit de l’« antivirus ayant le plus faible impact sur les performances des ordinateurs ». Nous sommes fiers de protéger chacun des plus de 400 millions d’utilisateurs qui confient leur sécurité et leur vie privée à Avast.

Sources : https://www.oracle.com/fr/cloud/malware-logiciel-malveillant.html#:~:text=Un%20malware%2C%20ou%20logiciels%20malveillants,%2C%20adware%2C%20scareware%2C%20etc.