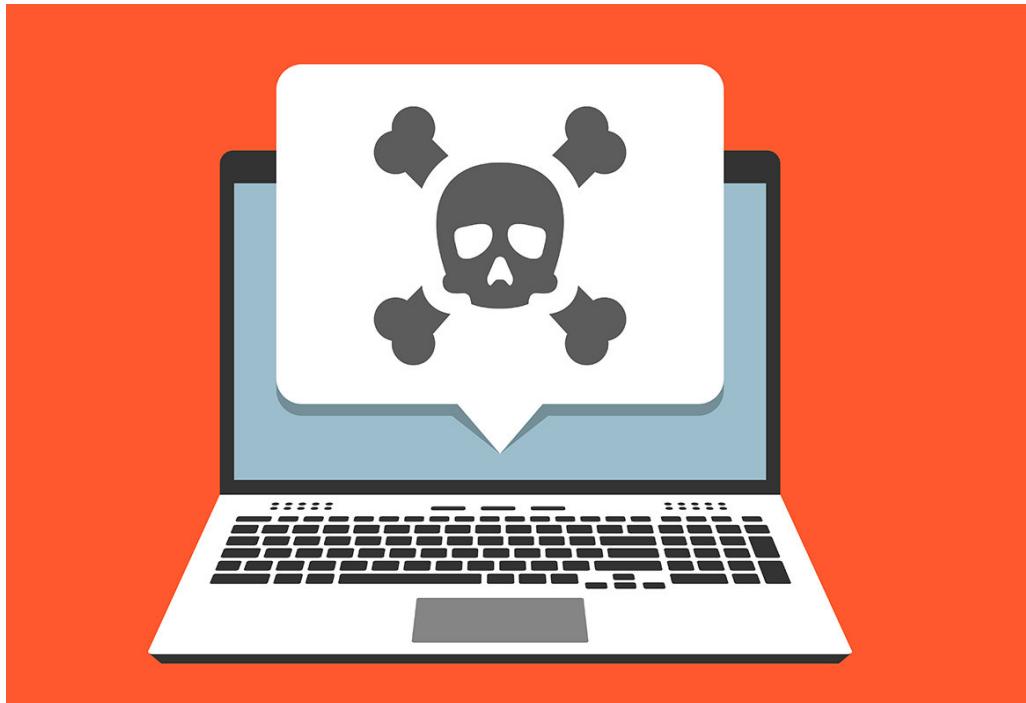
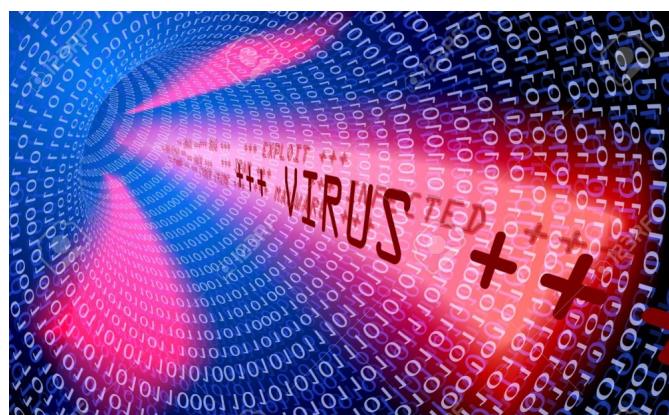


MALWARE



Dans le langage courant, on utilise le terme de “virus” pour désigner un “malware”, bien que cela ne soit pas exact. Un malware est un logiciel malveillant (ou maliciel), c'est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

Le terme de “virus” désigne plus de nos jours, une méthode d'infection, reprise par les différents types de malwares



Afin de mieux comprendre le sujet, il faut commencer par définir les termes de “ fichier hôte ”. Un fichier est un ensemble de données numériques réunies sous un même nom, enregistrées sur un support de stockage permanent. Le terme de “ fichier hôte ” désigne alors un fichier infecté par un morceau de code malveillant, pouvant nuire à l’appareil.



Parmi les nombreux types de malwares existants, on peut en retenir 5 principalement connus et vicieux : les adwares, les vers informatiques, les trojans, les ransomwares et les spywares.

Plan du sujet :

Adware

- Définition
- Fonctionnement
- Risque

Vers Informatique

- Qu'est-ce que c'est ?
- Fonctionnement
- Risques

Cheval de Troie

- Définition
- Impact
- Détection
- Illustration

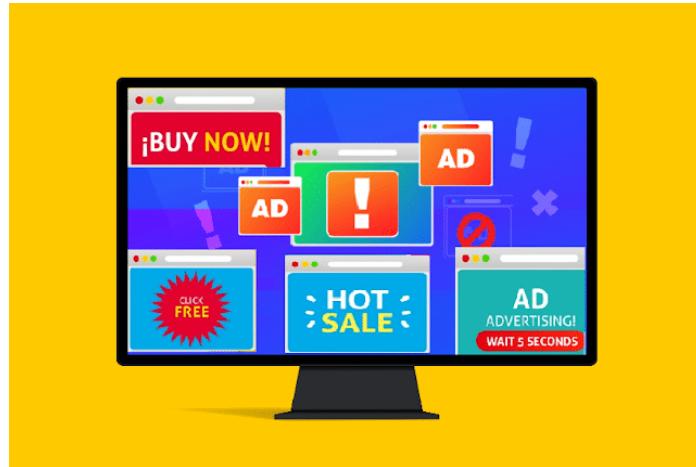
Ransomware

- Définition
- Les différents types
- Les plus connues
- Illustration

Spyware

- Définition
- Mode d'infection
- Les différents type

ADWARE



Définition

Les adware représentent l'une des nuisances les plus couramment rencontrées en ligne. Un adware est un logiciel nuisible conçu pour afficher des publicités intempestives sur nos écrans, la plupart du temps dans un navigateur web.

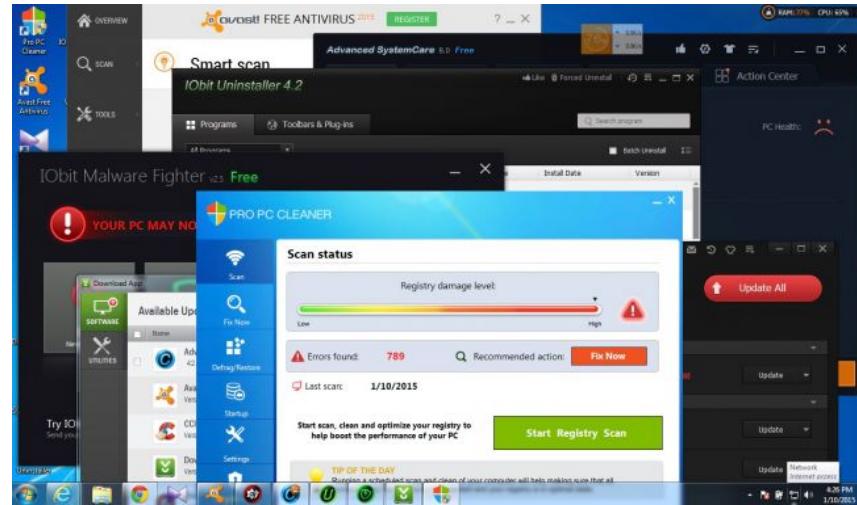
Fonctionnement

Les programmes envoient automatiquement des publicités aux ordinateurs infectés. Les adwares incluent des publicités contextuelles sur les pages Web et des publicités intégrées au programme qui accompagnent bien souvent un logiciel « gratuit ».

Risque

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.



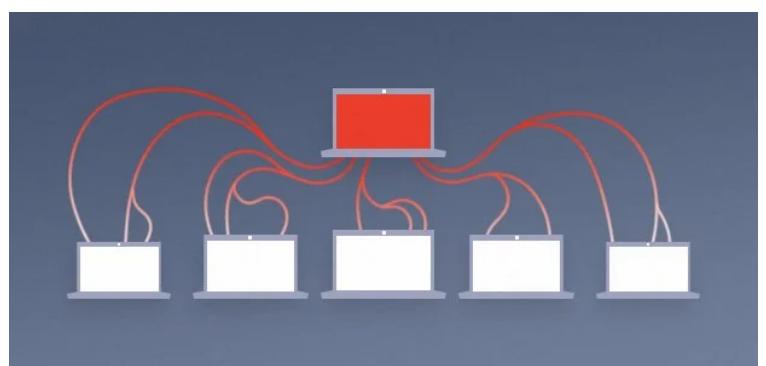
Vers Informatiques



Qu'est-ce que c'est ?

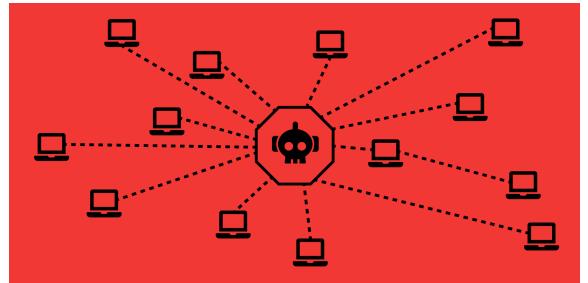
Un ver informatique est un programme autonome qui ne nécessite pas d'infecter un logiciel ou des fichiers pour fonctionner.

Son but est d'infecter les réseaux auxquels son hôte se connecte et ainsi parasiter encore plus d'appareils. Les performances d'un appareil infecté par un ver sont fortement dégradées car celui-ci est toujours actif.



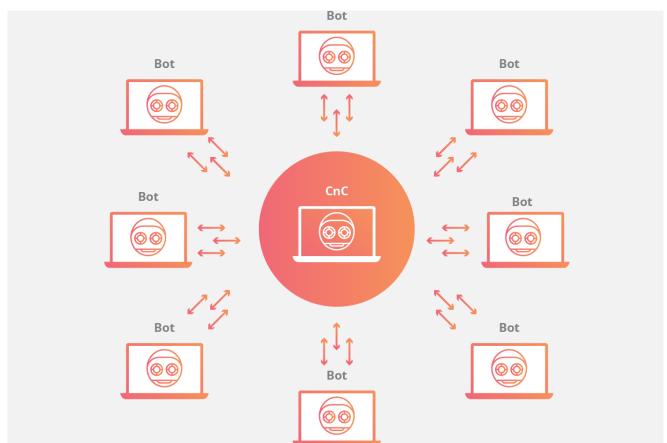
Fonctionnement

Si le ver n'a pas besoin de profiter du manque d'attention d'un utilisateur pour proliférer, il peut comme tout autre malware se répandre de manière plus commune : via un email trompeur par exemple ([malspams](#)). Le ver peut exploiter les failles des services de messagerie et, si l'appareil infecté en a une, le ver s'en servira pour envoyer aux contacts de l'utilisateur une copie de lui-même en pièce-jointe ou un lien redirigeant vers un site infecté par le ver.



Risques

Une fois implanté, un ver peut transmettre les informations saisies par l'utilisateur au pirate ou le laisser contrôler l'ordinateur à distance. Les ordinateurs alors "zombies" peuvent servir par exemple à effectuer des attaques DDOS contre un serveur dans le but de le rendre inopérant. Un réseau d'ordinateurs contrôlés à distance est appelé [botnet](#).

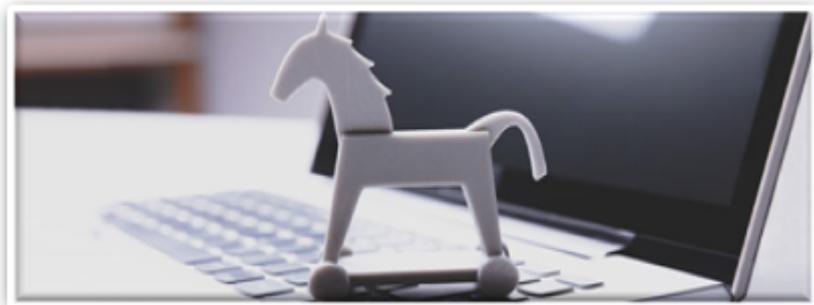


Les Chevaux de Troie

Définition du Cheval de Troie

Le Cheval de Troie, aussi connu sous le nom de Trojan, est un malware. Sa technique de pénétration au sein des systèmes d'utilisateurs consiste à se présenter comme un logiciel bienveillant et authentique auquel l'utilisateur adhère, tandis que son réel objectif est de véhiculer un parasite, qui est donc l'entité malveillante et qui s'instaure sur la machine.

Ces programmes sont d'une polyvalence remarquable, il en existe plusieurs types en fonction de l'intention criminelle du créateur.



Le terme "Cheval de Troie" a été utilisé pour la première fois dans le domaine informatique en 1970 par Daniel J. Edwards, chercheur à la **National Security Agency**. Cette appellation provient de la légende grecque de l'Odyssée d'Ulysse où le personnage éponyme et son armée envahissent la cité de Troie en se cachant dans un gigantesque cheval de bois.

Impact des Chevaux de Troie

Comme cité plus haut, on connaît à ce jour une dizaine de Chevaux de Troie dont le fonctionnement diverge selon les actions que le malware peut effectuer sur la machine. Parmi les plus répandus, on citera les suivants :

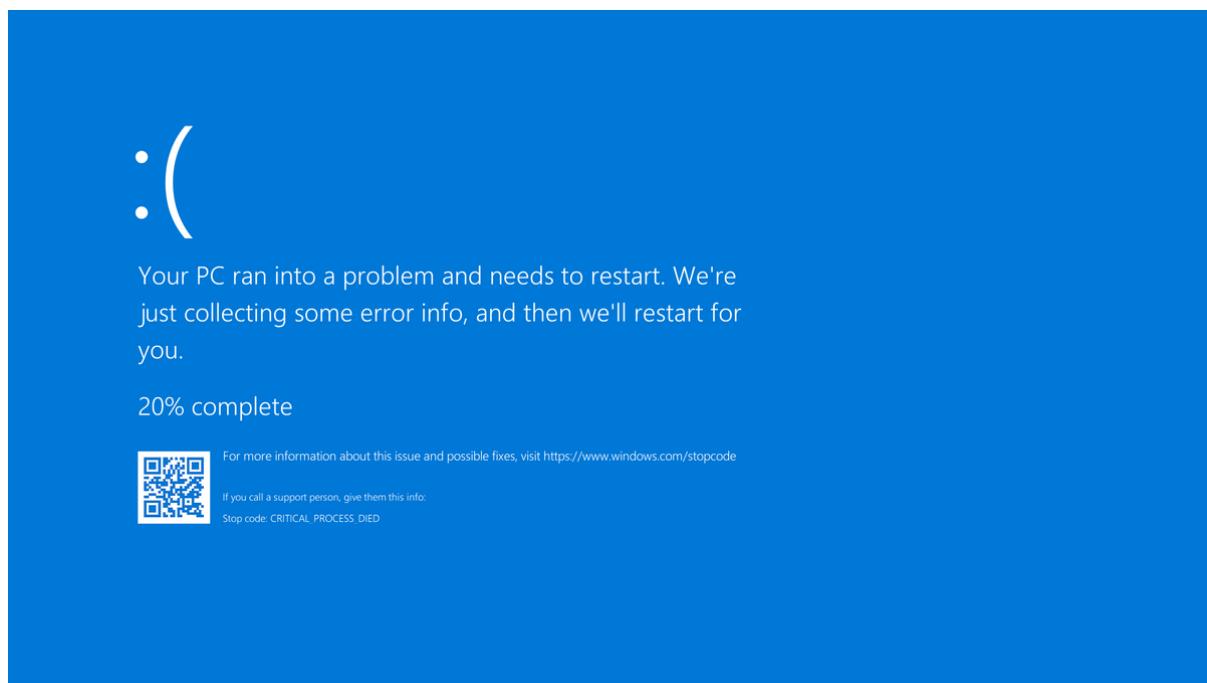
- * Backdoor : permet à un utilisateur mal intentionné le contrôle de l'ordinateur infecté à distance. L'auteur peut donc exécuter ce que bon lui semble et peut-être même instaurer d'autres malwares.
- * Cheval de Troie téléchargeur : Ces programmes seront autorisés à télécharger et installer divers autres logiciels plus malicieux que les autres.
- * Cheval de Troie bancaire : dérobent les données bancaires de l'utilisateur.
- * Rootkits : aussi appelés dissimulateurs, ils sont conçus dans le but de dissimuler certains objets ou activités de l'ordinateur. Ils ne sont pas à sous-estimer étant donné leur efficacité à prolonger l'invisibilité des malwares.
- * Cheval de Troie rançonneur : bloquent vos données et exigent une somme d'argent en échange pour vous y redonner l'accès.
- * Cheval de Troie messagerie instantanée : s'approprient vos identifiants et mots de passes de messageries instantanées.
- * Cheval de Troie DDoS : Ces malwares opèrent des attaques **Denial of Service** contre un serveur ou une adresse web en envoyant une multitude de requêtes et forcer un déni de service.
- * 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.

Détection des Chevaux de Troie

La présence de ces malwares occasionne des réactions improbables sur les systèmes infectés, ce qui pourrait mettre la puce à l'oreille pour l'utilisateur.

Les conséquences les plus communes sont les suivantes :

- * Ouverture et fermeture de programmes sans raisons apparentes.
- * **Blue Screen Of Death.***
- * Installation de programmes nocifs.
- * Vol de données personnelles.
- * Générer des notifications de sources inconnues aléatoirement.
- * Réactions inhabituelles de la souris.
- * Accès à des sites web non voulu.
- * La machine plante souvent.



Illustration

ANIMAL :

Considéré comme la première attaque mondiale de cheval de Troie, ce malware se dissimulait en 1975 en un quizz de plusieurs questions avant de se propager via les répertoires partagés à divers utilisateurs. Même si le programme en question n'était en aucun cas offensif, il aurait servi à démontrer la viralité des Trojans.

ILOVEYOU :

En 2000, le globe terrestre a connu la cyberattaque la plus dévastatrice de son époque avec un total de 8.7 milliards de dollars de dommages, et ce simplement en ouvrant un fichier texte nommé "ILOVEYOU" contenu dans un e-mail. Le programme se glissait dans les e-mails envoyés.



Wack-A-Mole :

Dans les années 1990, un autre cheval de Troie tristement célèbre apparut déguisé sous la forme d'un simple jeu de la taupe. Le programme cachait une version de NetBus, un programme qui permet de contrôler le système informatique Microsoft Windows à distance sur un réseau. Grâce à l'accès à distance, le cybercriminel pouvait effectuer de nombreuses actions sur l'ordinateur, y compris ouvrir son lecteur CD.



RANSOMWARE



Un **ransomware** est la contraction de ransom et de ware (l'abréviation de software). En français cela se traduirait par **rançongiciel**, soit la compression de rançon et de logiciel.

Définition

Le **ransomware** est un type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels en les chiffrant, et exige le paiement d'une rançon en échange du rétablissement de l'accès avec la clé de déchiffrement.

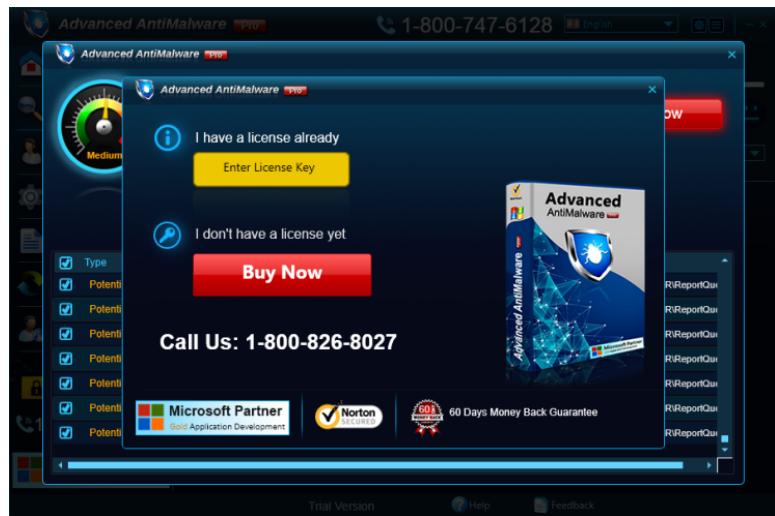
Les différents types

Il existe 3 grands types de ransomwares, lesquels sont :

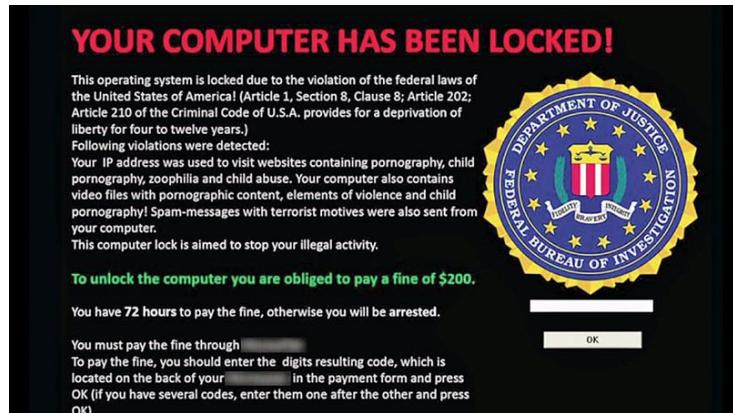
Scareware/Faux antivirus : fait croire aux utilisateurs que leur système est défaillant.

Ils doivent ensuite **acheter** un autre logiciel pour nettoyer le système. Bien évidemment, rien ne cloche avec l'ordinateur et la plupart du temps, le logiciel nécessaire au nettoyage infecte davantage l'ordinateur.

La plupart du temps, vous recevez une popup avec un message vous annonçant des problèmes comme un nouveau virus, un ralentissement du système ou des problèmes de registre, avec un gros texte en gras en plein milieu de l'écran.



Verrouilleurs d'écran : Cette catégorie de ransomware vous empêche d'utiliser votre ordinateur tant que vous n'avez pas payé de rançon. La plupart du temps, la fenêtre prend tout l'écran et affiche un message d'avertissement.



Ransomwares chiffreurs : le plus dangereux des 3 types de ransomware, il inclut les programmes qui cryptent tous vos fichiers et les rendent inutilisables à moins de payer une rançon. En général, ils pénètrent dans le système de la victime et crypte tous ses fichiers, les rendant complètement inaccessibles, puis exigent une rançon pour les déchiffrer.



Ce type de malware est très efficace, pour preuve, on entend beaucoup parler des ransomwares lorsqu'une entreprise ou une autre institution se fait pirater (cf Baltimore).

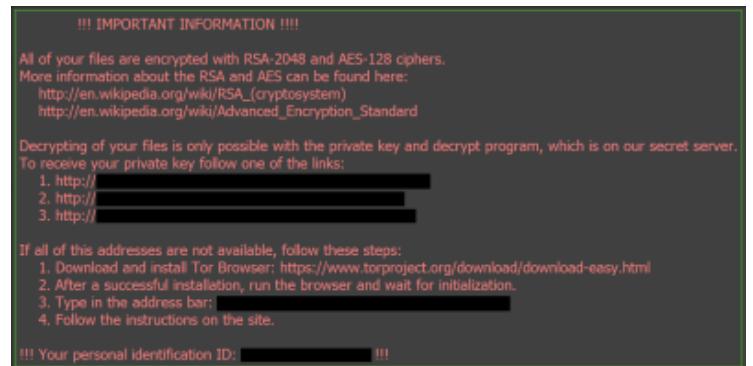
Divers ransomwares sont connus mondialement pour leur impact considérable, dû aux pertes directes (l'argent de la rançon, pertes de données, ...) et aux pertes indirectes (interruption de l'activité de travail, pertes de réputation, ...)

Les plus connues

Wannacry : (230.000 postes infectés dans 150 pays différents, les pertes financières sont incalculables)



Locky



CryptoLocker

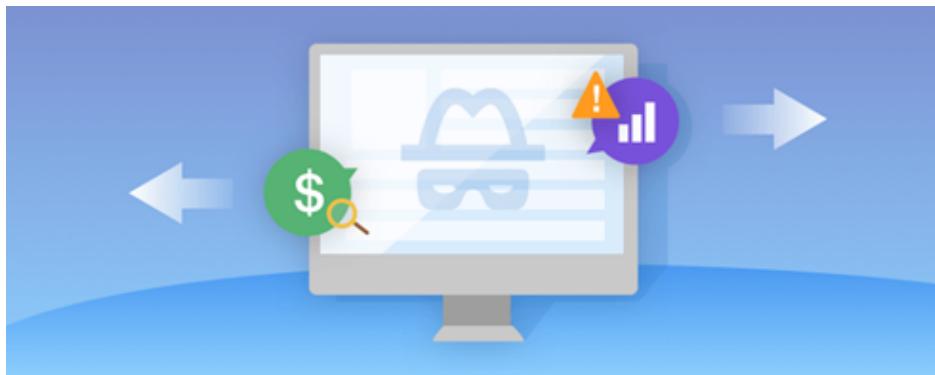
Les pirates utilisent des failles dans les systèmes pour arriver à leur fin. Mais la meilleur porte d'entrée pour eux reste vous-même. Vous êtes le maillon faible, et ils en ont bien conscience. C'est pour cela qu'il est plus simple pour un pirate de vous piéger plutôt que de trouver une faille.

Illustration

Comme fait célèbre, on peut citer le cas de la ville de Baltimore aux Etats-Unis en Mai 2019, qui en a fait les frais. Les pirates ont utilisé le ransomware RobinHood, infectant au moins 10 000 ordinateurs appartenant à la municipalité, pour une rançon de 13 bitcoins (100 000\$ ou 89 000€ au moment des faits).

L'attaque aura duré quelques semaines, nécessitant l'intervention du FBI, une équipe d'informaticiens travaillant jour et nuit, occasionnant des pertes totales estimées à 18 millions de dollars (soit 16 millions d'euros)

Les Spywares



Qu'est-ce qu'un Spyware :

Les spywares sont des logiciels espions ou des mouchards qui s'installent sur votre ordinateur et sur tous les appareils connectés à internet dans l'objectif de collecter et de transférer de nombreuses informations sur l'environnement de lequel il s'est installé sans que l'utilisateur soit averti de sa présence. L'essor des spywares est lié à celui d'internet qui lui sert de moyen de transmission pour les données qu'il collecte.

Les vecteurs d'infection :

Les logiciels espions fonctionnent de manière à ce que nous ne les remarquons pas, ils accèdent à nos ordinateurs et s'installent sur notre système d'exploitation pour rester présent sur nos ordinateurs. L'un des principaux vecteurs d'intrusions de logiciels espions est :

Le marketing trompeur, car la plupart des créateurs de spywares présentent leurs programmes comme des outils utiles. Ils les présentent comme des accélérateurs Internet, de nouveaux gestionnaires de téléchargements, de nettoyeur de disque dur ou de services de recherche Web alternatif. Lors de l'installation de ce logiciel un spyware est installé en même temps. Et même si par la suite vous désinstallez le logiciel à l'origine de l'infection, le spyware restera sur votre ordinateur et continuera à fonctionner.

Ensuite après avoir infecté nos ordinateurs les logiciels espions s'exécutent discrètement en arrière-plan et commencent à collecter des informations ou alors ils surveillent nos activités sur nos ordinateurs. Il existe différents types de Spywares :

Il y a pour commencer **les voleurs de mots de passe** se sont des applications faites pour récupérer les mots de passe sur les ordinateurs infectés. Parmi ces mots de passe on retrouve des identifiants enregistrés sur des navigateurs Web, des identifiants de connexion au système et des mots de passe divers. Ces mots de passe peuvent être stockés à un emplacement que le pirate informatique à choisi sur l'appareil infecté ou alors ces mots de passe sont transmis à un serveur à distance pour être récupérés par la suite.

Les chevaux de Troie bancaires sont des applications conçues pour voler des identifiants en lien avec les institutions financières. Ces virus se servent des failles de sécurité des navigateurs pour modifier les pages Web, le contenu des transactions ou insérer des transactions supplémentaires sans que l'utilisateur et l'application Web en aient connaissance. Ils peuvent cibler différentes institutions financières, comme les banques, les sociétés de courtage, les portails financiers en ligne ou les porte-monnaie électroniques. Pour récupérer les informations collectées, ils peuvent les transmettre à des serveurs à distance.

Les voleurs d'informations sont des spywares qui analysent les ordinateurs infectés et recherchent de nombreuses informations, comme les noms d'utilisateur, les mots de passe, les adresses e-mail, l'historique du navigateur, des informations système ou d'autres fichiers divers. Comme les chevaux de Troie bancaires, ces spywares se servent des failles de sécurité des navigateurs pour récupérer des informations personnelles, puis les transmettent à des serveurs à distance ou ils les stockent localement sur votre PC pour les récupérer.

Les enregistreurs de frappe, que l'on nomme aussi dispositifs de surveillance du système, sont des spywares conçus pour capturer l'activité de l'ordinateur, principalement les frappes, les sites Web visités, l'historique de recherche, les discussions par e-mail, les conversations par chat et les identifiants système. La plupart du temps, ils prennent

des captures d'écran de la fenêtre en cours, à des intervalles prévus. Ils peuvent également récupérer des fonctionnalités pouvant leurs permettre la capture et la transmission de manière discrète d'images et de fichiers audio/vidéo depuis n'importe quel appareil connecté. Ils peuvent même collecter des documents imprimés sur des imprimantes connectées, ensuite ils peuvent transmettre toutes ces captures d'écran à un serveur à distance ou stockés localement pour être récupérés plus tard.

Conclusion

Pour conclure, l'avènement d'internet a permis de moderniser les communications, l'information, mais aussi les pratiques frauduleuses. Plus internet se démocratise, plus les malwares sont sophistiqués. Nous devons alors redoubler de vigilance dans notre utilisation, particulièrement quand internet prend une place majeure dans notre vie quotidienne.

Quelques rappel pour se protéger des malwares :

Pour diminuer les risques de se faire infecter, il faut être prudent vis-à-vis des liens et des fichiers téléchargeables. Si un site, un mail, le nom ou l'extension d'un fichier paraît suspect, il vaut mieux s'abstenir d'y accéder, même si la source semble connue.

Il est recommandé de toujours posséder la dernière version des logiciels installés sur un appareil ainsi qu'un antivirus tels que MalwareBytes, Kaspersky, McAfee. Au cas où un malware serait téléchargé, il pourrait alors être bloqué avant exécution par l'antivirus ou ne pas fonctionner à la suite d'une mise à jour du logiciel cible. Un pare-feu empêche également les intrusions en provenance des réseaux.

En prévention d'une infection réussie, il est conseillé d'effectuer des sauvegardes régulières de ses données sur un support de stockage externe à la machine (cloud, disque dur externe...).

En cas d'infection il existe différentes manières d'éliminer le malware dépendamment de son type. Si le virus se répand sur un réseau, déconnecter les appareils et/ou de les éteindre peut limiter la propagation. Il est possible d'éliminer un malware en exécutant en antivirus ou en téléchargeant un programme spécifique (tel Wannakiwi en réponse au ransomware WannaCry de 2017). Dans le pire des cas, un formatage du disque dur est une solution envisageable pour refaire fonctionner un appareil infecté.

Les autorités recommandent de ne pas payer les rançons demandées par certains malwares car il n'est pas garanti qu'une clé de décryptage sera vraiment donnée. Il faut noter cependant que le piratage est un vrai business et que les pirates ont intérêt à ce que le décryptage soit possible pour que les victimes achètent. Certains gangs mettent même à disposition un service client et acceptent de faire des réductions ou d'étendre le temps de paiement.

Sources

Introduction / Adware

<https://www.speedcheck.org/fr/wiki/hote/#:~:text=ou%20moins%20capable.-,Histoire,et%20ayant%20moins%20de%20capacit%C3%A9>.

<https://www.kaspersky.fr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>

https://fr.wikipedia.org/wiki/Virus_informatique#Diff%C3%A9rents_types_de_virus

<https://fr.norton.com/internetsecurity-malware-what-is-a-computer-virus.html#:~:text=Tout%20commence%20le%20virus%20de,un%20fichier%20ou%20un%20document>.

<https://www.kaspersky.fr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>

https://fr.wikipedia.org/wiki/Virus_informatique#Terminologie

<https://geniorama.com/top-10-des-virus-informatiques-les-plus-dangereux-en-2019/>

<https://fr.norton.com/internetsecurity-malware-what-is-a-computer-virus.html#:~:text=Tout%20comme%20le%20virus%20de,un%20fichier%20ou%20un%20document>.

<https://www.buzzwebzine.fr/virus-informatique/>

Vers informatiques

Cheval de Troie

<https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203489-cheval-de-troie-trojan-definition-traduction-et-acteurs/>

<https://www.kaspersky.fr/resource-center/threats/trojans>

<https://fr.malwarebytes.com/trojan/>

Ransomware

<https://fr.malwarebytes.com/ransomware/#:~:text=Le%20malware%20de%20ransomware%20ou,la%20fin%20des%20années%201980.>

<https://www.kaspersky.fr/resource-center/threats/ransomware-examples>

<https://sciencepost.fr/la-ville-de-baltimore-prise-en-otage-par-des-hackers/>

<https://www.kaspersky.fr/resource-center/definitions/scareware>

<https://fr.vpnmentor.com/blog/les-attaques-ransomware-et-les-facons-de-les-gerer/#:~:text=Les%20ransomwares%20verrouillent%20d%C3%A9finitivement%20les%20fichiers.%C3%A9tant%20difficiles%20%C3%A0%20d%C3%A9crypter.>

<https://www.silicon.fr/hub/malwarebytes-hub/wannacry-et-les-degats-economiques-des-ransomwares>

<https://www.journaldunet.com/solutions/dsi/1490333-quels-sont-les-couts-reels-d-un-ransomware/>

<https://www.leparisien.fr/economie/la-cyberattaque-de-baltimore-a-coute-plus-de-18-millions-de-dollars-a-la-ville-20-07-2019-8120535.php>

<https://www.ictjournal.ch/news/2019-05-27/baltimore-est-paralyse-par-un-ransomware-depuis-trois-semaines>

Spyware

https://fr.wikipedia.org/wiki/Logiciel_espion

<https://fr.malwarebytes.com/spyware/>

RÉPARTITION

Introduction : Justin.B + surtout Justin.S

Plan : tout le monde

Adware : Justin.S

Vers Informatique : Dylan.T

Cheval de Troie: Nasser.A

Ransomware : Justin.B

Spyware : Florian.R

Conclusion : Justin.S + Justin.B + Dylan.T