Les malwares

Cet article vous conduira dans le monde des programmes malveillants. Vous y apprendrez comment fonctionne un malware, ainsi que les principaux modes d'infection et comportements malveillants adoptés par ces programmes. Au fur et à mesure, vous découvrirez comment vous protéger efficacement à l'aide de nos « 5 étapes pour votre sécurité numérique ».

Principales informations à connaître :

- Les malwares sont des programmes informatiques qui exécutent des fonctions indésirables et souvent malveillantes.
- Ils se manifestent par des comportements divers et variés et nécessitent l'adoption d'une série de mesures de prévention.
- Au cours de ces dernières années, nous avons assisté à une multiplication des risques liés aux malwares.
- Nos « 5 règles pour votre sécurité numérique (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) » permettent de réduire de manière efficace les risques liés aux malwares.

Malware – un programme informatique indésirable

Le mot « malware » est un terme générique qui désigne des programmes informatiques généralement créés dans l'intention de faire du tort aux utilisateurs.

À l'instar des logiciels traditionnels, le développement et la diffusion des malwares ont évolué. Leur création intervient de plus en plus à un niveau professionnel, ce qui contribue à augmenter la volatilité du développement des logiciels malveillants. Leur diffusion est quant à elle de plus en plus ciblée : particuliers et PME sont en effet systématiquement attaqués.

Infection

Comme tous les programmes informatiques, les malwares ne sont rien de plus qu'une série de commandes destinées à être exécutées par l'ordinateur.

Pour déployer son potentiel nuisible, un malware doit être exécuté par le système. Cela peut se produire sur indication de l'utilisateur ou d'une application déjà en cours d'exécution.

Dans le premier cas, il s'agit bien entendu de tromper l'utilisateur en lui faisant croire qu'il peut en tirer quelque avantage ou éviter quelque déboire. On regroupe généralement ce type de malwares sous le terme générique de cheval de Troie ou trojan. Camouflé sous la forme d'une application utile, il est généralement démarré par la victime elle-même. C'est lorsqu'il est exécuté qu'il commence à déployer tout son potentiel nuisible.

Mais il ne s'agit pas nécessairement de fichiers de programmes exécutables classiques. Des documents Office et des fichiers .pdf peuvent en effet contenir des macros qui s'exécutent directement au sein des différents programmes.

Notre « Règle n°5 – Faire attention et être vigilant (https://www.ebas.ch/fr/5-faire-attention-et-etre-vigilant/) » suffit sou-

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

vent à déjouer ce type de feinte.

Lorsque le malware est exécuté par un programme en cours, donc sans l'intervention de personne, c'est qu'il exploite ce que l'on appelle une faille de sécurité. Les failles de sécurité sont des erreurs de programmation dans une application pouvant avoir des répercussions sur le plan de la sécurité.

Les failles de sécurité présentes dans les navigateurs (https://www.ebas.ch/fr/les-navigateurs-web/) permettent de réaliser des infections par « drive-by download (https://www.ebas.ch/fr/infection-par-drive-by-download/) ». Les failles de sécurité dans le système d'exploitation sont aussi couramment exploitées, notamment pour introduire des logiciels malveillants via le réseau ou des supports de données externes tels que les clés USB. Les malwares capables d'exploiter de telles failles pour se diffuser de manière autonome sont aussi connus sous le nom de « vers ».

Les fabricants de logiciels publient régulièrement des mises à jour qui permettent de corriger ces failles de sécurité. D'où l'importance d'appliquer la « Règle n°3 – Prévenir avec les mises à jour logicielles (https://www.ebas.ch/fr/3-prevenir-avec-les-mises-a-jour-logicielles/) » afin de se prémunir contre les malwares.

Une fois exécutées, les différentes variantes de malwares sont la plupart du temps capables de faire en sorte que leur code malveillant soit d'une manière ou d'une autre continuellement relancé. C'est précisément dans ce but que les virus écrivent leur propre code malveillant dans d'autres programmes. Les « rootkits » se nichent quant à eux directement dans le code du système d'exploitation.

Effet néfaste

Dans la mesure où il est impossible d'éliminer complètement le risque d'infection par un malware, il est vivement recommandé de savoir quoi faire dans le cas où une tentative d'infection réussirait.

Voici donc quelques scénarios des effets néfastes pouvant dériver d'une infection par malware. Dans chaque cas, nous vous expliquerons comment limiter les dégâts en appliquant nos « 5 règles pour votre sécurité numérique (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) ».

Ralentissement du système

Une mauvaise utilisation des ressources du système et du réseau peut ralentir considérablement voire empêcher complètement le travail d'un appareil infecté. Ainsi, les malwares conçus pour miner de la cryptomonnaie (Crypto Miner) par exemple, ou hacker des mots de passe ou exécuter des attaques sur d'autre systèmes (p. ex. les attaques par déni de service ou DDoS) ont une incidence majeure sur les performances d'un système.

Ce type de malware déploie tout son potentiel en infectant le plus grand nombre possible de systèmes qui se trouvent regroupés en « botnet ».

Conçu pour une action à long-terme sur les systèmes, il devrait finir tôt ou tard par être détecté par le programme antivirus. Mais pour que cela advienne, ce dernier doit être mis à jour régulièrement et procéder à des scans complets réguliers de l'ensemble du système. Pour tout complément d'information, consulter la « Règle n°2 – Surveiller avec l'antivirus et le pare-feu (https://www.ebas.ch/fr/2-surveiller-avec-lantivirus-et-le-pare-feu/) ».

Affichage de publicités

Généralement perçus comme fastidieux par les utilisateurs qui en sont victimes, les programmes connus sous le vocable anglais de adware ou publiciel en français ont pour fonction d'afficher des publicités.

Ainsi l'affichage subit de nombreuses publicités est un signal qui doit alerter l'utilisateur sur une infection possible.

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

Dans ce cas, il convient de procéder sans plus attendre à un bon nettoyage du système.

Si les publicités se limitent à des pages de sites Internet et restent confinées sur votre navigateur, il peut être intéressant de suivre nos conseils pour améliorer la protection de vos données personnelles (https://www.ebas.ch/fr/respect-de-la-vie-privee-et-protection-des-donnees-personnelles-sur-internet/) et de votre vie privée sur le web, ou d'utiliser des bloqueurs de publicité (https://www.ebas.ch/fr/les-bloqueurs-de-publicite-et-les-anti-traceurs/) .

Collecte d'informations
Les malwares espions ou spywares sont de véritables mouchards qui collectent et transfèrent des informations ciblées sur leurs victimes. Ils peuvent par exemple s'intéresser au comportement des internautes sur le web, enregistrer les frappes effectuées sur le clavier (keylogger) ou voler des données sensibles.

Pour réduire les risques liés aux spywares, il est recommandé de segmenter ses activités numériques et d'observer une certaine réserve vis-à-vis de de ses données personnelles. La « Règle n°4 – Protéger les accès Internet (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) » vous permet de réduire efficacement l'ampleur des dégâts dans le cas d'une attaque réussie par un logiciel espion. Ainsi, si vous utilisez une méthode d'authentification à deux facteurs en e-banking, le vol d'un mot de passe ne compromettra pas irrémédiablement votre compte bancaire.

Cryptage ou destruction de données
Les ransomwares (ou rançongiciels en français) utilisent principalement le chiffrement des données afin d'exercer une pression pour le paiement d'une rançon.

Dans le cas d'une attaque rançongicielle, la seule parade consiste à nettoyer le système puis à récupérer les données à partir d'une sauvegarde effectuée précédemment. Bien entendu, la réussite de l'opération passe par le respect absolu de la « Règle n°1 – Sauvegarder les données (https://www.ebas.ch/fr/1-sauvegarder-les-donnees/) ».

Attaques combinées
Il faut savoir que les malwares peuvent adopter de nombreux comportements autres que ceux décrits plus haut. Il s'agit en effet souvent d'une combinaison des scénarios évoqués précédemment ou de nouvelles formes d'attaque.

Les attaques combinées sont l'œuvre d'un injecteur qui télécharge automatiquement, ou sur demande, d'autres malware sur le système-cible.

Les arnaques au chantage constituent un parfait exemple de ce cas de figure, où le système-cible est dans un premier temps espionné avant d'être verrouillé par chiffrement des données. Cette méthode permet aux escrocs d'exercer une pression plus forte sur leurs victimes dont ils menacent par exemple de publier les données volées ou de les transférer à la concurrence.

Identification et nettoyage

En respectant nos « 5 règles pour votre sécurité numérique (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) », vous pourrez réduire efficacement l'éventualité d'une infection par malware et par conséquent les probabilités que se réalise un des scénarios mentionnés plus haut.

Il faut toutefois être conscient du fait que le risque ne peut être totalement exclu. Consultez notre article « Infection par malware (https://www.ebas.ch/fr/les-infections-par-malware/) » pour savoir comment détecter et remédier à une infection.

Le terme malware (programme malveillant ou maliciel) désigne des programmes informatiques conçus pour exécuter

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

des fonctions indésirables et même parfois nuisibles du point de vue de la victime. Il s'agit d'un mot-valise composé des mots malicious « malveillant » et software.

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique