الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ

LETTRE D'INFORMATION : BON A SAVOIR (N°31)

Logiciels malveillants et virus quelle est la différence ?

Le terme de « malware » (ou « logiciel malveillant ») est constitué par les deux mots anglais « malicious » (malicieux) et « software » (logiciel) ; il s'agit donc de «logiciels malicieux ».

Comme tout virus est, sans aucun doute, malicieux, il fait partie de la catégorie du malware ou des logiciels malveillants aussi bien que les chevaux de Troie, aussi nommés troyens, rootkits ou logiciels espion.

Tout logiciel malveillant n'est pas un virus, mais ils en sont plutôt une sous-catégorie.

Autrement dit, il n'y a plus que très peu de nouveaux virus, car la plupart des mêmes logiciels malveillants sont en fait d'autres parasites nocifs.

Anti-virus: un terme ambigu, de nos jours

Il est dommage que beaucoup de logiciels de protection utilisent les termes « anti-virus » et « anti-malware » de manière ambiguë.

Il y a des utilisateurs qui considèrent une solution anti-virus plus puissante que tout autre combattant les logiciels malveillants, mais le terme « logiciel malveillant » est le terme générique.

Veuillez toutefois vérifier contre quels programmes nocifs le logiciel vous protège, peu importe qu'il s'agisse d'anti-virus ou d'anti-malware. Ce qui compte, c'est le contenu, et non le nom ou l'emballage.

Quels genres de logiciels malveillants existent ?

Tout le monde connaît les virus, et beaucoup aussi bien les logiciels espion ou publiciels. Mais qu'en est-il des rootkits, rançongiciels et rogues ?

Brève introduction aux différents genres de logiciels malveillants.

- **Virus :** Un virus se propage de lui-même en infiltrant son code dans une application. Le nom vient de son archétype biologique. Le virus ne se limite généralement pas à sa propagation, ce qui rend inutilisable le logiciel hôte, mais lance en plus des routines malicieuses.
- **Cheval de Troie** : Un cheval de Troie est une forme de logiciel malveillant déguisé en logiciel utile. Son but : se faire exécuter par l'utilisateur, ce qui lui permet de contrôler l'ordinateur et de s'en servir pour ses propres fins, quelles qu'elles soient. Généralement d'autres logiciels malveillants seront installés sur votre ordinateur, tels que des portes dérobées ou des enregistreurs de frappe.
- **Ver** : Un ver est un logiciel nocif dont le but consiste à se propager au plus vite une fois lancé. Contrairement aux virus, ils ne se servent pas d'autres logiciels, mais plutôt de supports de données externes tels que les clés USB, des médias de communication tels que les mails ou des vulnérabilités de votre système d'exploitation. Leur propagation réduit les performances des ordinateurs et des réseaux, et parfois, des routines nocives y sont implémentées.

- **Enregistreur de frappe :** Les enregistreurs de frappe enregistrent tout ce que vous saisissez au travers du clavier, ce qui permet d'espionner vos mots de passe et d'autres données importantes telles que celles de votre service bancaire en ligne.
- **Dialer** : Les dialers (en français « numéroteurs ») sont un relicte des temps où l'on se connectait sur Internet avec des modems ou le numéris. Ils composaient des numéros surtaxés et vous causaient des factures de téléphone d'un montant astronomique, ce qui représentait des dommages financiers considérables pour la pauvre victime. Avec les connexions ADSL ou par câble, les dialers ne marchent plus, on les considère quasiment disparus, de nos jours.
- **Porte dérobée / Bot :** Une porte dérobée est une partie programmée par l'auteur du logiciel lui-même qui permet d'entrer dans l'ordinateur ou s'emparer d'une fonctionnalité normalement protégée d'un logiciel. Les portes dérobées sont effectuées par les chevaux de Troie une fois lancés pour ouvrir toutes grandes les portes de l'ordinateur attaqué. L'ordinateur infecté (également appelé « bot ») devient partie d'un réseau nommé bot net.
- **Exploit :** « To exploit » veut dire « exploiter » en français ; il s'agit donc d'un point faible d'un logiciel exploité à des différentes fins. Celui-ci permet au pirate de s'emparer de votre ordinateur ou de le contrôler en partie.
- **Logiciel espion :** Un logiciel espion fait ce que dit son nom : il est un espion qui collecte diverses données sur l'utilisateur sans que celui-ci ne s'en rende compte.
- **Publiciel :** « Publiciel » ou « adware » en anglais vient de « publicité » ou «advertisement », l'équivalent du mot en anglais. A part les fonctions mêmes du logiciel, il présente des pubs à l'utilisateur. Les publiciels, en soi, ne sont pas dangereux, mais des tonnes de pubs affichées sont quand même considérées comme gênantes et donc détectées par une bonne solution anti-malware.
- **Rootkit :** Un rootkit est souvent constitué par plusieurs composants qui ouvrent toutes grandes les portes de votre ordinateur aux pirates. En outre, ces logiciels cachent leurs processus et utilisent des routines d'autres logiciels. L'installation se fait, par exemple, à travers un exploit ou un cheval de Troie.
- **Rogues :** Ils sont également connus sous le nom de « Rogue Anti-Spyware » ou « Rogue Anti-Virus » et se présentent à la victime comme logiciel de sécurité. Ils se servent souvent d'avis falsifiés censés vous mener à acheter le logiciel de sécurité, ce qui fait gagner de l'argent aux pirates.
- **Rançongiciels :** « Rançon » est bien ce que vous pensez être. Les rançongiciels cryptent généralement vos données personnelles ou bloquent tout accès à votre ordinateur. Ils vous demandent de payer une rançon à travers un service anonyme afin de débloquer votre ordinateur.

https://www.pcsansvirus.com/pages/emsisoft-anti-malware/logiciels-malveillants-et-virus.html

Comment fonctionne une infection par des logiciels malveillants ?

La plupart des logiciels malveillants sont les chevaux de Troie et les Bots.

Comment fonctionne une infection par des logiciels malveillants ?

Premièrement pour pouvoir répondre à cette question, il faut tout d'abord analyser différents types individuels de logiciels malveillants :

- **Virus**

Les virus ont la propriété d'utiliser une application comme hôte, afin d'être fonctionnels. Un virus s'accroche toujours à un programme légitime, en installant son code malicieux dans le fichier exécutable (ex. : .exe). Aussitôt que le programme légitime est chargé, le virus peut commencer sa routine de dévastation, et se reproduire sur d'autres applications. Aujourd'hui, les virus ne jouent qu'un petit rôle négligeable sur le secteur des logiciels malveillants.

- **Chevaux de Troie, Porte dérobée, Agent logiciel (Bot), Vers**

Aujourd'hui, la plupart des nouveaux logiciels malveillants sont de loin les chevaux de Troie et les Bots. Ils n'ont pas besoin d'un hôte pour fonctionner, car ils sont eux-mêmes des programmes indépendants. Les Bots essayent, si possible, d'être discret et se cachent le plus souvent enfin bien camouflé dans les profondeurs du système d'exploitation. Parmi ses tâches figurent tout d'abord l'ouverture d'un port du PC pour que désormais l'attaquant puisse prendre le plein contrôle du PC, pour le trafic d'envoi en masse de pourriels ou de la coordination de surcharge de différents sites Web en passant par de nombreuses demandes manipulées (DoS). Un ordinateur ne peut être considéré comme infecté que si un tel logiciel malveillant est actif. Des fichiers non démarrés ne constituent aucun danger. Cheval de Troie et Bots disposent toutefois d'un grand nombre de fonctions qui s'assurent qu'à chaque initialisation du système que le programme démarre automatiquement.

Espions, Adware, faux logiciels de sécurité

Une nouvelle tendance pour les logiciels malveillants est la manipulation des composants importants du système, pour que les fichiers malveillants ne soient dorénavant plus simplement supprimés. Ainsi, certains logiciels espions lancent en parallèle plusieurs processus actifs (instances de programmes), qui se surveillent mutuellement. À chaque fois qu'un processus sera terminé, l'autre se lancera immédiatement de nouveau derrière, etc… Faux logiciels de sécurité, les soi-disant outils Rogue antivirus et antispywares s'injectent essentiellement dans les processus du système. Lorsque l'on essaye de se débarrasser des logiciels malveillants, en essayant de terminer le processus hôte pour ensuite supprimer le fichier nuisible, l'action se termine avec un écran bleu (Blue screen) redouté et le système reste sans réaction.

- **Rootkits**

Les Rootkits manipulent le système d'exploitation afin que les fichiers du rootkit ne soient simplement plus affichés et par conséquent de ne plus être trouvés par les logiciels antivirus. De même, les entrées dans le registre, les ports ouverts et les processus actifs se font invisibles afin de ne pas laisser de traces qui révèleraient la présence d'un rootkit.

Une fois le PC infecté - Nouvelle installion !

Plus le logiciel malveillant est complexe, plus la suppression sera difficile. Le vrai problème est que l'on ne peut jamais partir du principe, que le nettoyage complet soit réussi. Dans de nombreux cas, des fonctions de nettoyage de produits de sécurité, qui

ne feront que masquer la vérité : La conclusion logique est que l'ordinateur n'est plus digne de confiance, dès qu'il a été une fois infecté par des logiciels malveillants.

Pourquoi ?

- Il se pourrait qu'après un nettoyage un Rookit soit encore caché sur votre ordinateur, qui n'a pas encore été détecté par la technologie d'Anti-Rootkit.
- En voyant encore un peu plus vaste la probabilité, qui par l'infection de composants importants du système d'exploitation ait été manipulée. Par exemple, les droits ont pu être activés, qui donnent à l'attaquant le droit d'ouvrir un port sur l'ordinateur, ou des logiciels qui ont été manipulés de façon à ce que les routines nuisibles créées soient incorporées dans des fichiers.

Le Seul moyen est par conséquent de rendre de nouveau l'ordinateur utilisable, de formater le disque dur et de recréer le système d'exploitation !

Le mieux : Éviter les infections

Ne faites jamais confiance au nettoyage seul. Protéger l'ordinateur à l'avance contre les infections des logiciels malveillants est toujours mieux que par la suite d'éliminer le chaos considérable laissé. L'important est donc un système de protection existant à plusieurs niveaux :

- **Tenir ses logiciels à jour**

Une partie considérable de tous les logiciels malveillants arrivent sur l'ordinateur par des failles de sécurité. Gardez toujours votre système d'exploitation à jour. La mise à jour automatique de Windows doit être toujours activée, car de plus en plus souvent seuls quelques jours séparent la connaissance d'une faille et de la première exploitation en masse par les vers. De même, il est nécessaire que tous les logiciels avec des données qui hantent l'Internet soient également tenus d'être à jour. Il s'agit notamment du navigateur, lecteur PDF, lecteur MP3, visualisateur d'images, etc., parce que ces fichiers doivent être traités, car ils peuvent contenir des codes malveillants.

- **Protection de navigation Internet**

Évitez si possible de naviguer sur des sites douteux, où vous pouvez vous attraper un logiciel malveillant. Ceci peut-être réalisé avec l'aide du bloqueur d'hôtes ou pare-feu avec les fonctions adéquates.

- **Premier grand obstacle : Scanneur de définitions de signatures**

Si par malheur, il vous arrivait une fois de télécharger et d'exécuter un fichier dangereux, il y aurait une probabilité de plus de 99 % qu'un gardien d'arrière-plan de scanneur de signatures de logiciels malveillants détecte et l'empêcherait de démarrer.

- **Deuxième grand obstacle : Analyse comportementale (ou proactive)**

Si vous deviez cependant une fois un fichier dangereux d'un nouveau logiciel malveillant ou autre qui est créé pour des attaques particulières, ils ne peuvent dans ce cas être détectés seulement par des bloqueurs de logiciels malveillants basés sur la surveillance comportementale et qui empêcheront leur démarrage.

https://www.undernews.fr/malwares-virus-antivirus/goznym-le-trojan-bancaire-qui-fait-des-ravages-en-amerique.html

Pièges par mail actuels
Exemples de hameçonnage et comment les détecter

Vous vous êtes déjà étonné de recevoir, de temps en temps, des mails émis par des entreprises telles que DHL, Amazon ou de certaines banques ?
Vous devriez en être étonné si vous n'avez pas encore eu de relations commerciales avec ces expéditeurs. Car, souvent, ces mails n'ont pas été envoyés par ce groupe international, mais par des escrocs. Cet article vous donnera quelques exemples actuels et vous renseignera comment reconnaître ces fraudes et comment vous en protéger.

Comment procèdent les escrocs ?

Ils aiment bien prendre les noms d'entreprises connues. Car, d'un côté ces noms inspirent confiance et de l'autre, le destinataire fait probablement partie de leurs clients.
Les buts que les escrocs poursuivent par ces mails falsifiés sont divers : soit ils ne visent qu'à ramasser des données, à infecter votre PC avec des logiciels malveillants ou vous délester de votre argent d'une manière ou d'une autre.
Un essai de hameçonnage conventionnel, heureusement un essai très maladroit.
Ce qui frappe avant tout, c'est la grammaire et l'absence d'une entreprise expéditrice.
Si d'une part, il n'est pas clair pour quelle entreprise ce Mr X travaille, et que d'autre part, l'adresse e-mail paraît douteuse, cela devrait vous laisser sceptique
Vous vous rendrez compte que l'on ne s'adresse pas personnellement à vous. Si vous cliquez quand même sur le lien contenu dans ce mail apparemment falsifié, on vous demandera de saisir les coordonnées de votre carte de crédit sur une page web douteuse. Une fois cela fait, il ne faut pas s'étonner de voir des transactions bizarres sur votre prochaine facture de carte de crédit. La capture d'écran montre avec beaucoup de clarté l'adresse cachée derrière le texte du lien est cryptée. Afin d'afficher l'adresse, il ne faut rien faire d'autre que de passer la souris sur le lien.

Comment me protéger ?

Tous ces exemples sont réels et échappent aux filtres de courriel indésirable de logiciels de mail tels que Microsoft Outlook ou Thunderbird.
Il s'agit d'un risque très élevé, car ce que l'on menace, c'est très souvent, soit votre porte-monnaie, soit la sécurité de votre ordinateur et ainsi de vos données.
Il faut donc toujours analyser tout mail que vous recevez avant d'ouvrir des fichiers ou liens joints. Veuillez tenir compte des points suivants :

- Dans quelle langue le mail a-t-il été rédigé ? Si vous n'utilisez que des fournisseurs français, vous n'allez d'habitude recevoir que des mails rédigés en français.
- Quelle est l'adresse e-mail que l'expéditeur a mis dans le champ "A: " ? Si le mail ne s'adresse pas à votre adresse e-mail exacte, il est très probable qu'il s'agisse d'une tentative de fraude.
- L'adresse e-mail de l'expéditeur, elle aussi, devrait être logique. La plupart des entreprises emploient des formats tels que Nom@entreprise.fr ou du moins des adresses générales telles que service@entreprise.fr ou support@entreprise.fr.
- S'adresse-t-on à vous par votre nom ? Les entreprises de vente par correspondance, vos amis et membres de votre famille connaissent votre nom et vont donc vous envoyer des mails personnalisés.

- Comment la mise en page a-t-elle été réalisée, est-elle professionnelle ou reflète-t-elle l'identité de l'entreprise ? Les expéditeurs sérieux veillent au style et à la présentation, tandis que les escrocs s'en passent souvent. Tout mail ayant de nombreuses fautes d'orthographe est très probablement une tentative de hameçonnage.
- Les liens contenus vous mènent-ils sur la page de l'entreprise ? En passant la souris sur le lien, vous pourrez voir vers quel site il vous mène. Si l'adresse semble cryptée : Ne touchez pas à ça !
- De quel type de fichier s'agit-il pour le fichier joint ? Normalement, vous recevez des fichiers PDF ou DOC, car il n'est pas nécessaire de les comprimer dans un fichier ZIP. N'exécutez jamais des fichiers exécutables de sources douteuses ! Veuillez toujours faire attention à l'extension du fichier.
- Il est d'autant plus probable qu'il s'agisse d'une tentative de fraude, dans la mesure où le mail correspond aux critères de cette liste. Il est aussi possible de se protéger activement en tenant compte des trois points suivants :
  - Afficher les mails texte seul ("Plain Text") au lieu de HTML. Ceci rendra quelques mails un peu bizarres en les regardant, mais vous permet de reconnaître un lien falsifié immédiatement.
  - On vous demande de vous connecter sur votre compte ou de prendre contact avec une certaine entreprise ? Ne jamais cliquer sur des liens ni ouvrir des fichiers joints, mais plutôt saisir manuellement l'adresse de l'entreprise correspondante dans votre navigateur. En cas de doute, veuillez simplement prendre contact avec votre personne responsable ou le service clientèle qui vous diront si un mail est authentique ou pas.
  - Veiller à utiliser un logiciel anti-virus muni d'une protection en temps réel.

https://www.pcsansvirus.com/pages/emsisoft-anti-malware/pieges-par-mail-actuels-exemples-de-hameconnage-et-comment-les-detecter.html

Attention aux attaques DNS…

Certes les problématiques liées à la sécurité et à la protection de l'information ne manquent pas aujourd'hui : sécurité des applications Web, des bases de données, nombreux projets de mobilité, menaces APT, phishing e-mail, etc., au risque d'en oublier les attaques plus « traditionnelles ».

Depuis la création du DNS, ces services ont régulièrement fait l'objet de toutes les convoitises des hackers du monde entier. Pourquoi ? Ce système nous permet de nous soustraire à l'ennuyeuse et difficile tâche de mémoriser les adresses IP des serveurs Internet !

Le DNS : pierre angulaire d'Internet.

Le Domain Name Service (DNS) est l'annuaire d'Internet, transformant un nom en IP. Tel le « Roi » aux échecs, les DNS sont les parties d'Internet les plus fragiles et vulnérables. Contrôler le DNS revient à contrôler Internet, et de nos jours peut signifier contrôler notre monde interconnecté.

Intérêt pour les pirates

Un attaquant peut porter un intérêt au DNS dans le cadre de plusieurs types d'attaques

- ***Déni de Service par saturation*** : le déni de service peut être opéré directement sur le serveur DNS ayant autorité sur un domaine. Une fois saturé, il n'est plus en mesures de répondre aux requêtes légitimes, et donc les internautes se

retrouvent sans annuaire, dans l'incapacité de trouver les services auxquels ils souhaitent accéder.

- ***Déni de Service par modification des entrées DNS*** : la modification des entrées DNS pour un domaine ciblé peut aisément rendre le service associé injoignable (en pointant sur une adresse IP qui n'existe pas par exemple).
- ***Atteinte à l'image de marque*** : au lieu de dévier les internautes sur une IP qui n'existe pas, le pirate peut rediriger les requêtes sur des serveurs offrant des contenus pornographiques ou autres, pouvant sérieusement porter préjudice au nom et à l'image de marque de l'entreprise attaquée.
- ***Fraude, escroquerie*** : imaginez que vous vous connectiez sur un site marchand pour un paiement en ligne. Comme à votre habitude, vous entrez le nom du site dans votre navigateur Internet et procédez au paiement. Si un pirate parvient à rediriger votre connexion vers son site en modifiant l'enregistrement DNS sur le serveur DNS du site marchand, il peut facilement récupérer vos informations de paiement, comme par exemple le numéro de carte bancaire utilisé, et s'offrir ses prochaines vacances au soleil.

Focus sur le « DNS Spoofing » et « DNS Cache Poisonning »

L'attaque par « DNS Poisoning » (empoisonnement DNS) est celle qui offre le plus de possibilités pour un pirate, et en particulier celle de faire croire à un internaute qu'il navigue sur un site légitime alors qu'il se fait dérober ses informations sur un site pirate.

Se protéger

Combler les lacunes listées ci-dessus est une première étape. A savoir :

- ***Patcher ses serveur DNS à la version la plus récente***. Les problèmes de prédictabilité des ID et le numéro de port source statique pour les requêtes DNS sont des problèmes connus de longue date, et les dernières versions des serveurs DNS y remédient le plus souvent.
- ***Limiter l'accès à ses serveurs DNS***. Si vous êtes une entreprise, rares sont les cas où votre serveur DNS récursif doit être accessible sur Internet, l'accès doit généralement être limité à vos employés. Si vous êtes un fournisseur d'accès Internet, à vos clients.

DNSSEC est l'étape suivante pour vraiment résoudre les problèmes de Spoofing et Poisonning. L'ajout de mécanismes de cryptographie asymétrique pour authentifier les échanges permet une validation plus stricte des interactions entre les différents composants de l'architecture DNS. En effet, les enregistrements DNS sont signés.

Pour forger un enregistrement, un pirate devrait alors également récupérer la clé privée de signature. Et la complexité n'est pas la même.

Certains pays ont déjà adopté cette extension pour leur TLDs (Top Level Domain), et l'implémentation sur les DNS ROOT a eu lieu en Juillet 2010.

https://blog.e-xpertsolutions.com/attention-aux-attaques-dns/

Les Keyloggers : des enregisteurs de touches

Qu'est ce que c'est ?

Les keyloggers sont des enregistreurs de touches et par extension des enregistreurs d'activités informatiques permettant d'enregistrer les touches utilisées par un utilisateur sur son clavier et tous les évènements déclenchés.

Objectif :

L'objectif des keyloggers est d'enregistrer et de restituer tout le travail qui a été réalisé par un utilisateur. Les touches enregistrées permettent effectivement de retracer non seulement le travail courant, mais aussi de récupérer tous les identifiants et mots de passe.

Mode d'action :

Le mode opératoire des keyloggers est identique, même s'il existe une multitude de keyloggers différents. Ils sont installés directement par le pirate sur la machine visée, si l'ordinateur n'a pas de connexion internet permettant une installation à distance via un cheval de Troie.

En général, les keyloggers se lancent directement au démarrage de la machine hôte.

Une fois le keyloggers lancé, il enregistre au fur et à mesure tout ce qui est frappé sur le clavier. Dans la plupart des cas, si la machine cible est pourvue d'une connexion internet, le keylogger enverra discrètement, à une adresse mail ou à un serveur internet, un fichier, généralement crypté, contenant tous les renseignements collectés.

Ainsi le pirate aura tout le temps nécessaire pour retracer votre activité et sélectionner les éléments qui lui semblent utiles. En fonction du keylogger sélectionné différents types d'écran de configuration existent.

Selon le keylogger choisi, il est possible de paramétrer l'option "auto-destruction".

Dès lors impossible à l'utilisateur ou à l'administrateur du parc informatique de remonter au programme et à l'espion qui se cache derrière. Il suffit de déterminer la plage en nombre de jours pendant laquelle le keylogger doit rester actif sur la machine cible pour qu'automatiquement le logiciel se détruise une fois le délai passé.

Contre-mesures :

Les keyloggers ne sont pas toujours identifiés par les anti-virus. Il n'est donc pas évident de les remarquer. En outre, dans la plupart des cas des options permettant l'invisibilité du programme exécuté existent.

Par contre, les keyloggers s'exécutent au démarrage de la machine. Tout ralentissement du système au lancement doit sembler suspect. Cependant, avec les nouvelles générations d'ordinateurs il est de moins en moins simple de noter ces ralentissements machines.

Dans le cas ou vous trouveriez un fichier suspect le plus simple est de commencer par faire travailler votre machine uniquement en local. Déconnectez-vous de votre réseau et stoppez toute connexion internet. Cela empêchera aux fichiers de parvenir à l'espion. Prévenez votre administrateur qui recherchera via le serveur les échanges de mail et tentera de retrouver l'adresse du destinataire.

Une inspection des tâches qui sont en train d'être exécutées par votre ordinateur s'impose. Dans le pire des cas, il sera peut être nécessaire que vous sauvegardiez tous vos fichiers de données pour ensuite formater votre disque dur.

Conclusion

Les keyloggers permettent aux pirates de récupérer comme nous l'avons dit les mots de passe et les logins des utilisateurs.

Sur un poste non connecté à internet, l'installation d'un tel outil implique le passage du pirate sur la machine cible.

Le meilleur moyen de prévention reste donc la vigilance, ne pas quitter son poste sans avoir au minimum verrouillé son écran, et bien ne pas diffuser son mot de passe de session à quiconque. Il faut aussi que le mot de passe soit robuste.

https://www.securiteinfo.com/attaques/divers/keylogger.shtml