Virus informatique : c'est quoi ? que faire ?

Pr Chérif DIALLO, CISSP
Professeur Assimilé (LAFMC CAMES)
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

"Dans un monde où l'information est une arme et où elle constitue même le code de la vie, la rumeur agit comme un virus, le pire de tous car il détruit les défenses immunitaires de sa victime." Jacques Attali, Europe(s).

Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui un problème crucial de cybersécurité. Il s'agit des virus informatiques qui s'apparentent aux virus biologiques compte tenu de leurs charges utiles, mais aussi et surtout des méthodes d'infection, de propagation et de reproduction inspirées de ces derniers. Après une brève définition, ce bulletin, donne quelques exemples de virus et de statistiques, les types de virus et les solutions face à ce fléau.

Mots clés : Virus, Vers, Cheval de Troie, logiciel malveillant.

---

1. Définition

Un virus informatique est un logiciel malveillant utilisé à des fins destructives sur un appareil ou un réseau et pourrait, par exemple, interrompre des services, endommager le système de fichiers, voler des données, télécharger d'autres logiciels malveillants supplémentaires ou toute autre action codée dans le programme par l'auteur du virus. De nombreux virus se font passer pour des programmes légitimes afin d'inciter les utilisateurs à les exécuter sur leur appareil, délivrant ainsi la charge utile du virus informatique.

Les virus informatiques sont donc des programmes standards. Mais au lieu d'offrir des ressources utiles, ces programmes ont pour but d'endommager votre appareil. Pour activer un virus sur votre machine, vous devez souvent initier l'exécution. Dans certains cas, un attaquant peut exécuter un code malveillant via votre navigateur ou à distance depuis un autre ordinateur du réseau. Les navigateurs modernes disposent de défenses contre l'exécution locale de code machine, mais les logiciels tiers installés sur le navigateur peuvent présenter des vulnérabilités permettant l'exécution locale de virus.

La diffusion d'un virus informatique peut se faire de plusieurs manières. L'une des méthodes les plus courantes est l'envoi d'un email de phishing. Une autre technique consiste à héberger un malware sur un serveur qui promet de fournir un programme légitime.

2. Quelques exemples de virus très répandus

Le web contient des millions de virus informatiques, mais seuls quelques-uns ont gagné en popularité et infectent un nombre record de machines. Voici quelques exemples de virus informatiques très répandus :

- ***Morris Worm :*** Le ver Morris était un programme informatique auto-répliquant (ver) écrit par Robert Tappan Morris, étudiant à l'Université Cornell, et sorti du MIT le 2 novembre 1988. Selon Morris, le but du ver était d'évaluer la taille du précurseur « Internet » de l'époque - ARPANET - bien qu'il ait provoqué involontairement un déni de service (DoS) pour environ 10 % des 60 000 machines connectées à ARPANET en 1988. Le ver s'est propagé en exploitant les vulnérabilités d'UNIX ainsi qu'en devinant des mots de passe faibles. Avant de se propager à une nouvelle machine, le Morris Worm a vérifié si la machine avait déjà été infectée et exécutait un processus Morris Worm. Si une machine cible avait déjà été infectée, le ver Morris la réinfecterait 1 fois sur 7. Cette pratique de « réinfection 1 sur 7 » garantissait qu'un utilisateur ne pouvait pas complètement éviter une infection par Morris Worm en créant un faux processus Morris Worm pour prétendre que sa machine était déjà infectée. Cela a également provoqué l'infection à plusieurs reprises des machines de certains utilisateurs - une fois que trop de processus Morris Worm s'exécutaient sur une machine cible, celle-ci manquait de ressources informatiques et commençait à mal fonctionner. L'affaire judiciaire États-Unis contre Morris (1991) a abouti à la première

condamnation en vertu de la loi de 1986 sur la fraude et les abus informatiques, Morris ayant été condamné à trois ans de prison, 400 heures de travaux d'intérêt général et une amende de 10 000 $.

- ***Nimda :*** Nimda est un virus complexe avec un composant de ver de publipostage de masse qui se propage dans les pièces jointes des e-mails nommé README.EXE. Il affecte les utilisateurs de Windows 95, Windows 98, Windows Me, Windows NT 4 et Windows 2000. La première variante de la famille Net-Worm:W32/Nimda a été découverte le 18 septembre 2001 et s'est rapidement propagée dans le monde entier. Nimda est le premier ver à modifier des sites Web existants pour commencer à proposer des fichiers infectés en téléchargement. Il s'agit également du premier ver à utiliser les machines normales des utilisateurs finaux pour rechercher des sites Web vulnérables. Comme techniques de propagation :
  - Nimda recherche les adresses e-mail dans tous les fichiers '.htm' et '.html' du dossier Temporary Internet Files. Il lit la boîte de réception de l'utilisateur et collecte les adresses des expéditeurs. Lorsque la liste d'adresses est prête, elle utilise son propre moteur SMTP pour envoyer les messages infectés.
  - Nimda utilise des portes dérobées sur les serveurs IIS tels que celui installé par CodeRed II. Il scanne les adresses IP aléatoires pour ces portes dérobées. Lorsqu'un hôte en possède un, le ver ordonne à la machine de télécharger le code du ver (Admin.dll) à partir de l'hôte utilisé pour l'analyse. Après cela, il exécute le ver sur la machine cible, l'infectant ainsi.
- ***ILOVEYOU :*** Le 4 mai 2000, le virus « I Love You » s'est propagé de façon fulgurante en touchant les systèmes informatiques du Pentagone, de la CIA, et de grandes entreprises comme L'Oréal, Siemens et Nestlé. Ce petit morceau de code a infecté des dizaines de millions d'ordinateurs, ce qui en fait l'un des virus les plus virulents de l'histoire. Son auteur est identifié quelques jours plus tard : c'est un Philippin de 24 ans, nommé Onel de Guzman. Il ne sera pas inquiété car à cette époque, la loi de son pays ne prévoit pas ce type de délit. La pièce jointe dans le virus ILOVEYOU est un programme VBScript que les destinataires à l'époque confondaient avec un simple fichier texte car l'extension .vbs était masquée sur les machines Windows. Lorsque le fichier est ouvert, il trouve le carnet d'adresses Outlook du destinataire et renvoie la note à tous ceux qu'il contient. ILOVEYOU a fait détruire toutes sortes de fichiers, y compris des photographies, des fichiers audio et des documents. Les utilisateurs concernés qui n'avaient pas de copies de sauvegarde perdaient donc définitivement leurs données.
- ***Tinba :*** Le virus Tinba, ou virus Tiny Banker, est un cheval de Troie malveillant. Il est conçu pour infecter les appareils des utilisateurs finaux afin de compromettre les comptes des sites Web financiers et de voler les données envoyées vers et depuis les sites bancaires. Cela permettrait au pirate d'accéder à des informations financières et de voler de l'argent à ses victimes. Alors que les logiciels malveillants de cheval de Troie et les codes malveillants similaires ne sont pas uniques, Tiny Banker l'est. Il est le plus petit cheval de Troie connu existant à seulement 20 Ko. Cela le rend particulièrement difficile à détecter et incroyablement efficace. Il a été découvert pour la première fois en 2012 sur des milliers d'ordinateurs infectés en Turquie. Dans une tournure malheureuse des événements, son code source a été divulgué en ligne, ce qui a conduit à une série de révisions individuelles par des pirates du monde entier. Chaque nouvelle révision le rendait encore plus difficile à détecter et à supprimer. L'aspect de l'attaque silencieuse n'est pas tout ce dont le virus Tinba est capable. Même s'il ne fait que 20 Ko, il a une charge utile efficace et dangereuse. Il peut également s'injecter dans d'autres processus système. Plus particulièrement, il peut s'insérer dans explorer.exe, firefox.exe et svchost.exe, ce qui pose un grave problème de cybersécurité. Le virus Tinba fonctionne en utilisant un exploit connu sous le nom de « kit Rig Exploit » pour exploiter les vulnérabilités de Silverlight et Flash. L'exploit permet à un code malveillant de télécharger et d'exécuter une charge utile de logiciel malveillant. Après l'infection, le code malveillant injecte des formulaires qui semblent authentiques pour que l'utilisateur remplisse ses informations de compte. Le code malveillant qui fabrique le virus Tinba ne dépend pas de la méthode d'infection. Le virus reste inactif jusqu'à ce qu'il détecte que l'utilisateur tente d'accéder à un site Web bancaire. Les effets ne sont donc pas souvent visibles tant que vos comptes bancaires n'ont pas subi de modifications importantes, car le créateur du cheval de Troie avait pour objectif que le virus vole vos informations plutôt que d'anéantir votre ordinateur.
- ***Shlayer :*** Shlayer est un virus cheval de Troie spécifiquement ciblé sur les systèmes Mac. Sa fonction principale est de télécharger du code malveillant via de fausses applications et des mises à jour flash. Une fois que le virus Shlayer est installé sur un système, il commence à télécharger et à installer des logiciels malveillants axés sur la prolifération des publicités, autrement appelés logiciels publicitaires. Le logiciel publicitaire téléchargé puis installé par Shlayer force la publicité dans le navigateur de Mac et peut même intercepter les recherches du navigateur pour modifier les résultats afin de promouvoir davantage de publicités. En 2019, le virus Shlayer représentait 29 % de toutes les attaques d'appareils macOS par code malveillant. Avec un taux d'infection aussi élevé, Shlayer était la menace numéro un des logiciels malveillants pour les appareils Mac. Shlayer n'est pas un ver qui se propage aux systèmes. Il s'agit plutôt d'un ancien type de code malveillant auquel on accède en incitant les utilisateurs de Mac à l'installer par des moyens néfastes. Le virus Shlayer utilise l'une des techniques les plus anciennes et préférées des

pirates. Au lieu d'un processus automatisé qui se reproduit de lui-même, il nécessite que les utilisateurs téléchargent le virus de leur plein gré. Les pirates incitent les utilisateurs à le faire en déguisant le téléchargement en fonction nécessaire ou en logiciel souhaité. La méthode la plus courante consiste à effectuer une mise à jour déguisée de Flash Player. D'autres méthodes d'infection incluent l'ouverture de liens ou de publicités infectés, le téléchargement de fichiers ou de logiciels non fiables et le clic sur l'un des nombreux liens masqués poussés par un réseau lâche de distributeurs de virus. Les créateurs du cheval de Troie Shlayer ont augmenté leur portée en offrant aux YouTubers, aux propriétaires de sites Web et aux éditeurs de Wikipédia un pourcentage des gains créés par des publicités malveillantes pour pousser leurs téléspectateurs à installer le cheval de Troie par tous les moyens qu'ils jugent nécessaires. Dans certains cas, les domaines complices peuvent même inciter les Mac à télécharger Shlayer en tant que fausse mise à jour ou installation Flash. Kaspersky rapporte que plus de 1 000 sites partenaires distribuent Shlayer avec une instance d'un individu qui possède 700 domaines qui redirigent vers les pages de téléchargement de Shlayer. Une fois que Shlayer a été installé, il devient un véhicule pour diffuser d'autres logiciels malveillants. L'une des charges utiles les plus connues est Cimpli qui est un logiciel publicitaire généralement déguisé en une extension de navigateur Safari telle que Any Search. Shlayer est un code malveillant si simple qu'il n'y a aucun symptôme d'infection visible. Les utilisateurs de Mac soucieux de la sécurité devront utiliser un logiciel antivirus pour analyser, détecter et supprimer le cheval de Troie. Bien que Shlayer lui-même ne présente aucun symptôme visible, les utilisateurs de Mac peuvent rechercher les symptômes des charges utiles qu'il installe. Comme cette menace de cybersécurité est principalement utilisée pour installer des logiciels publicitaires, le signe évident que votre appareil a été infecté est un nombre inhabituel de publicités.

3. Quelques statistiques sur les virus

Ces statistiques sur les virus aident à mieux appréhender la dimension du problème viral.

- Le tristement célèbre virus ILOVEYOU a causé 10 milliards de dollars de dégâts en 2009.
- 560 000 nouveaux malwares sont détectés chaque jour.
- Il existe aujourd'hui plus d'un milliard de programmes malveillants.
- Chaque minute, quatre entreprises sont victimes d'attaques de ransomwares.
- Les chevaux de Troie représentent 58 % de tous les logiciels malveillants informatiques.
- SonicWall a enregistré plus de 3,2 milliards d'attaques de logiciels malveillants au premier semestre 2020.
- En 2020, le nombre de variantes de logiciels malveillants détectées a augmenté de 62 %.
- 20 millions d'attaques de logiciels malveillants IoT ont été détectées au premier semestre 2020.
- 46 % des pirates diffusant des logiciels malveillants les diffusent presque exclusivement par e-mail.
- Le nombre total d'attaques de logiciels malveillants mobiles a dépassé 28 millions au cours du premier semestre 2020.
- Il y a 50 fois plus d'infections sur les appareils Android que sur les appareils iOS.
- 47 % des programmes antivirus Android gratuits ne peuvent pas détecter correctement les logiciels malveillants.

4. Quelques types de virus

De nombreux virus n'affectent qu'un appareil local, mais d'autres se propagent dans un environnement réseau pour trouver d'autres hôtes vulnérables. Un ver informatique est un logiciel malveillant, tout comme un virus, mais un ver prend une copie de lui-même et la propage à d'autres utilisateurs. Les virus polymorphes rendent l'élimination difficile car ils modifient constamment leur empreinte. La charge utile peut être le vol de données, la destruction de données ou l'interruption de services sur le réseau ou le périphérique local. Un cheval de Troie (ou Trojan Horse) est un type de logiciel malveillant qui est souvent masqué comme un logiciel authentique. On note en outre plusieurs types de virus :

- ***Virus à action directe.*** Ils délivrent immédiatement une charge utile. Ces virus peuvent également rester inactifs jusqu'à ce qu'une action spécifique soit effectuée ou qu'un délai soit écoulé.
- ***Virus infecteur de fichiers.*** Pour persister sur un système, un acteur de la menace utilise des virus infecteurs de fichiers pour injecter du code malveillant dans des fichiers critiques qui exécutent le système d'exploitation ou des programmes importants. Lorsque le système démarre ou que le programme s'exécute, le virus est activé.
- ***Virus multipartite.*** Ces programmes malveillants se propagent sur un réseau ou d'autres systèmes en se copiant ou en injectant du code dans des ressources informatiques critiques.
- ***Virus résident.*** Un virus qui peut accéder à la mémoire de l'ordinateur et rester inactif jusqu'à ce qu'une charge utile soit délivrée est considéré comme un virus résident. Ce malware peut rester en sommeil jusqu'à une date ou une heure spécifique, ou jusqu'à ce qu'un utilisateur effectue une action.
- ***Virus visant le secteur de démarrage.*** Le disque dur de votre ordinateur possède un secteur uniquement chargé de pointer vers le système d'exploitation afin qu'il puisse démarrer dans l'interface. Un virus visant le secteur de démarrage endommage ou contrôle le secteur d'amorçage du lecteur, rendant la machine

inutilisable. Les attaquants diffusent généralement ce type de virus à l'aide d'un périphérique USB malveillant. Le virus est activé lorsque les utilisateurs branchent le périphérique USB et démarrent leur machine.

- ***Virus macro.*** Les fichiers Microsoft Office peuvent exécuter des macros, et ces macros peuvent être utilisées pour télécharger des logiciels malveillants supplémentaires ou exécuter du code malveillant. Les virus de macro délivrent une charge utile lorsque le fichier est ouvert et que la macro est exécutée.
- ***Virus des scripts Web.*** La plupart des navigateurs disposent de défenses contre les scripts Web malveillants, mais les navigateurs plus anciens et non pris en charge présentent des vulnérabilités qui permettent à un attaquant d'exécuter du code sur le périphérique local.
- ***Détourneur de navigateur (browser hijacker).*** Un virus qui peut modifier les paramètres de votre navigateur détourne les favoris du navigateur, l'URL de la page d'accueil, vos préférences de recherche et vous redirige vers un site malveillant. Le site peut être un site de phishing ou une page de logiciel publicitaire utilisée pour voler des données ou gagner de l'argent pour l'attaquant.

5. Solutions

Voici quelques bonnes pratiques pour éviter les virus informatiques ou limiter leurs conséquences :

- ***Installez un logiciel antivirus.*** Un antivirus devrait être exécuté sur tout appareil connecté au réseau. C'est votre première défense contre les virus. Un logiciel antivirus empêche les exécutables de logiciels malveillants de s'exécuter sur votre appareil local.
- ***N'ouvrez pas les pièces jointes exécutables des emails.*** De nombreuses attaques de logiciels malveillants, y compris les ransomwares, commencent par une pièce jointe malveillante. Les pièces jointes exécutables ne doivent jamais être ouvertes, et les utilisateurs doivent éviter d'exécuter des macros programmées dans des fichiers Microsoft Word ou Excel.
- ***Maintenez votre système d'exploitation à jour.*** Les développeurs de tous les principaux systèmes d'exploitation publient des correctifs pour remédier aux bugs courants et aux failles de sécurité. Maintenez toujours votre système d'exploitation à jour et cessez d'utiliser les versions en fin de vie (par exemple, Windows 7 ou Windows XP).
- ***Évitez les sites web douteux.*** Les anciens navigateurs sont vulnérables aux exploits utilisés lors de la simple navigation sur un site web. Vous devez toujours maintenir votre navigateur à jour avec les derniers correctifs, mais en évitant ces sites, vous éviterez les téléchargements par drive-by ou les redirections vers des sites hébergeant des logiciels malveillants.
- ***N'utilisez pas de logiciels piratés.*** Les logiciels piratés gratuits peuvent être tentants, mais ils contiennent souvent des logiciels malveillants. Téléchargez les logiciels des fournisseurs uniquement à partir de la source officielle et évitez d'utiliser des logiciels piratés et partagés.
- ***En cas d'infection, déconnectez l'équipement infecté d'Internet ou du réseau pour éviter que le virus ne se propage à d'autres appareils.*** Pour cela, débranchez le câble réseau (Ethernet) de votre ordinateur ou de votre serveur ou désactivez la connexion Wi-Fi et/ou Bluetooth de votre appareil ou les connexions de données s'il s'agit d'un appareil mobile (téléphone, tablette).
- ***Changez vos mots de passe au moindre doute.*** Utilisez des mots de passe différents et complexes pour chaque site et application utilisés.
- ***Restaurez votre système si les symptômes de l'infection continuent de se manifester.*** En effet, les systèmes d'exploitation actuels intègrent des fonctionnalités qui permettent de restaurer le système de votre ordinateur à une date antérieure, ce qui permettra d'annuler les modifications qui ont été apportées à votre appareil sans affecter vos fichiers personnels.
- ***Réinitialisez ou réinstallez complètement votre appareil en dernier recours si le virus persiste toujours.*** Cette action permettra de le remettre dans ses paramètres d'usine. N'oubliez pas d'effectuer une sauvegarde de vos fichiers personnels avant cette opération car autrement vous perdrez vos données.

6. En conclusion

"Ne sous-estimez pas les petits adversaires : un lion se voit, pas un virus."

Un virus est donc un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire. Il existe différents types de virus qui peuvent s'infiltrer dans un système informatique par l'ouverture d'un message (mail, MMS, chat), d'une pièce jointe ou d'un clic sur un lien frauduleux, par exemple. Les symptômes d'une infection par un virus peuvent rester silencieux ou se manifester par une alerte de l'antivirus, un ralentissement ou un blocage anormal de l'appareil, des fenêtres ou des messages d'erreur qui s'affichent. Enfin, pour faire face aux virus il faut combiner plusieurs solutions en utilisant nécessairement un logiciel antivirus.
