Livre blanc | Mai 2006

McAfee®
Proven Security™

Le nouveau fruit défendu du malware : Mac OS X est-il le prochain Windows ?

Table des matières

Principales conclusions

1. De 2003 à 2005, le taux annuel de découverte de vulnérabilités a augmenté de 228 % pour la plate-forme Mac OS d'Apple (figure 2). Comparativement, les produits Microsoft ont connu une augmentation de 73 % sur la même période.

2. Le patch distribué par Apple en mars 2006 pour corriger quelque vingt vulnérabilités démontre que la plate-forme Mac OS est tout aussi vulnérable que les autres systèmes d'exploitation aux attaques ciblées de logiciels malveillants (page 6).

3. De plus en plus, Mac OS et les autres produits Apple, tels que l'iPod ou le service iTunes, vont susciter l'intérêt des chercheurs en sécurité et des pirates (page 6).

Introduction

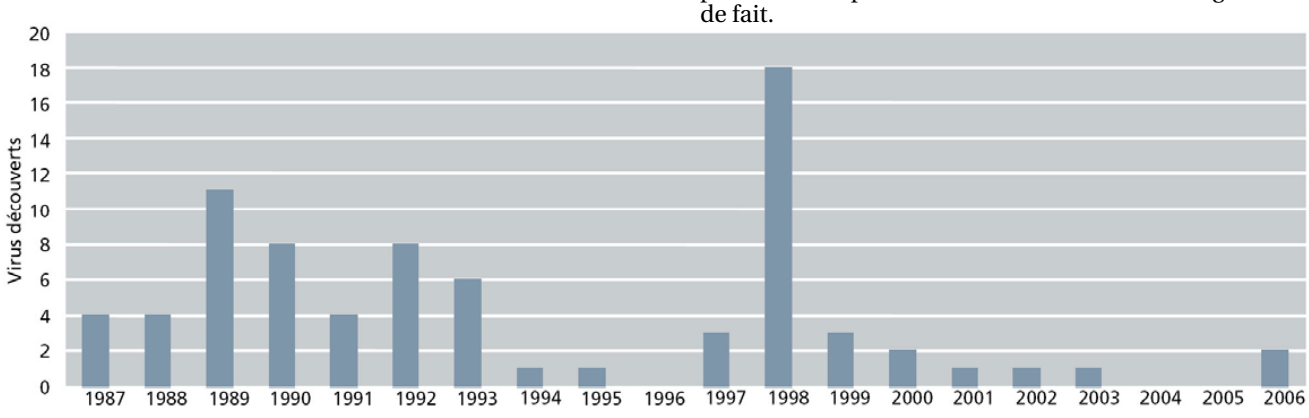
Pendant plus de 26 ans, Apple est parvenu à tirer son épingle du jeu en matière de sécurité informatique. Cette bonne fortune s'explique notamment par la présence relativement discrète d'Apple sur le marché de l'ordinateur personnel, où Microsoft se taille la part du lion. De fait, la plate-forme et les technologies d'Apple ont longtemps joui d'une réputation d'immunité face aux virus et d'infaillibilité en matière de sécurité — profitant favorablement de la comparaison au vu des failles découvertes dans les systèmes Microsoft au cours des vingt dernières années. Toutefois, la progression sur le marché du système d'exploitation Macintosh OS X (Mac OS) et la forte popularité des technologies grand public d'Apple (iPod et iTunes) ont éveillé les convoitises des pirates et l'intérêt des chercheurs en sécurité, exposant davantage Mac OS et les autres produits Apple aux attaques perpétrées par logiciels malveillants.

Visibilité croissante d'Apple

Jusqu'il y a peu, la part très limitée d'Apple sur le marché mondial de l'ordinateur personnel (2,2 % à 2,3 %)[1] était la raison principale qui valait à l'entreprise d'être épargnée par les auteurs de logiciels malveillants. Depuis 1987, les laboratoires McAfee AVERT ont recensé 76 virus ciblant le système d'exploitation Mac OS (voir la figure 1 pour la répartition annuelle). Des chiffres qui tranchent nettement avec les 168 000 menaces, dont environ 100 000 virus, qui ont visé les équipements Windows de 1986 à fin 2005.

La figure 2, cependant, n'augure pas des lendemains qui chantent pour les utilisateurs Apple. La *National Vulnerability Database* (base de données officielle du gouvernement américain sur les vulnérabilités informatiques) indique une envolée de 228 % du taux annuel de découverte de vulnérabilités pour les produits Apple entre 2003 (45 vulnérabilités) et 2005 (143 vulnérabilités). En comparaison, pour les produits Microsoft, ce taux a seulement augmenté de 73 % sur la même période.[2] L'émergence, en 2006, de logiciels malveillants exploitant des vulnérabilités connues ou encore inconnues (attaques dites « émergentes ») confirme qu'Apple est bel et bien dans le collimateur des auteurs de logiciels malveillants.

Apple subit actuellement les premiers stades d'évolution des logiciels malveillants, les exploits écrits et diffusés uniquement en tant que preuve de concept, afin de mettre en évidence les talents ou d'établir la notoriété de leurs auteurs. Les coups d'éclat de ce genre, s'ils existent toujours au sein de la communauté Windows, sont désormais largement éclipsés par des agissements plus professionnels, motivés par l'appât du gain. A l'heure actuelle, la clientèle d'Apple ne constitue pas une cible suffisamment rémunératrice pour éveiller l'intérêt de ce contingent. Mais le succès commercial grandissant d'Apple et la popularité croissante de ses produits auprès du grand public vont rapidement et inévitablement changer cet état de fait.

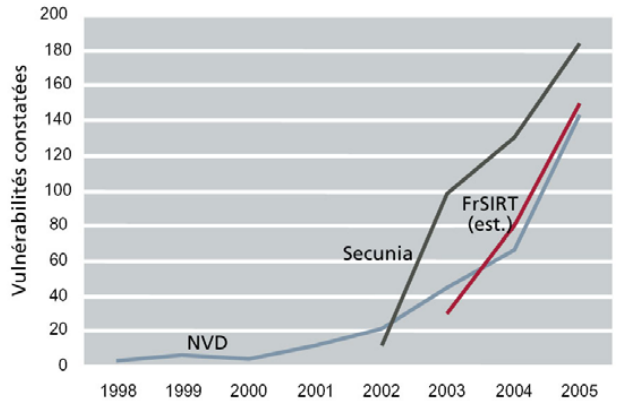


Source : McAfee AVERT Labs

Figure 1 – Virus ciblant Mac OS, 1987-2006

[1] Mike Langberg : « Low Market Share is Badge of Honor, as far as Mac Faithful Are Concerned », Mercury News, 26 mars 2006, http://www.siliconvalley.com/mld/siliconvalley/business/columnists/mike_langberg/14191452.htm?source=rss&channel=siliconvalley_mike_langberg

[2] La *National Vulnerability Database* fait état de la découverte de 92 vulnérabilités Microsoft en 2003 et de 159 en 2005, ce qui correspond à une augmentation de 73 %.



Sources : National Vulnerability Database, French Security Incident Response Team et Secunia

Figure 2 – Vulnérabilités Apple, 1997-2006[3]

OSX/Leap : un saut dans l'inconnu pour Macintosh

Conçu pour se propager via le système de messagerie instantanée AIM/iChat, *OSX/Leap*[4] est le premier virus à s'attaquer à la plate-forme Mac OS X. Le virus tire parti de la technologie Spotlight d'Apple, de sorte que seuls les systèmes Mac OS X version 10.4 à 10.4.4 sont concernés. Après quelques distributions confidentielles, *OSX/Leap* a été publié sur le forum *MacRumors*[5] le 13 février 2006. Le virus amène les utilisateurs à le télécharger en se présentant comme une série de captures d'écrans de Mac OS X version 10.5 (Leopard), toujours en développement.

Distribué sous la forme d'un fichier joint d'une taille de 40 893 octets, *OSX/Leap* permet à l'utilisateur d'accepter ou de refuser le fichier. Si ce dernier marque son accord, le fichier est enregistré sous le nom *latestpics.tgz* (voir la figure 3). L'extension *.tgz* indique qu'il s'agit d'un fichier compressé (fichier tar compressé à l'aide de GZIP). Ce fichier décompressé, on trouve un dossier comprenant deux fichiers HFS (Hierarchical File System) Apple standard : *._latestpics* (43 694 octets) et *latestpics* (39 596 octets).

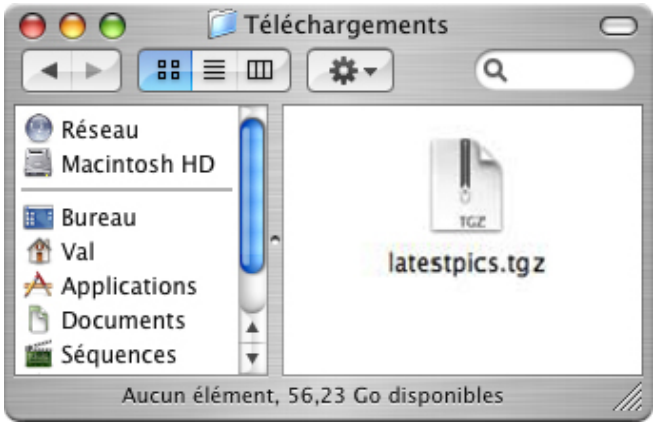


Figure 3 – Fichier d'archive OSX/Leap après téléchargement initial

Prenant l'aspect d'une icône JPEG (voir la figure 4), le fichier *._latestpics* est en réalité un fichier exécutable compilé pour le PowerPC. L'utilisateur qui souhaite voir l'image est tenté de double-cliquer sur l'icône. Il lance ainsi l'exécution du virus, qui affiche un message et se copie vers le dossier temporaire (/tmp) en manipulant ce fichier (*branche de ressource*) à l'aide d'un code exécutable contenu dans le fichier *latestpics* (*branche de données*).

Figure 4 – .latestpics apparaissant comme une icône JPEG

Le fichier se réplique sous la forme d'une image compressée, qu'il envoie dans des messages. Il crée ensuite ses propres entrées système et se dépose soit dans le dossier racine InputManagers (/Library/InputManagers/), si les autorisations le lui permettent, ou dans le dossier d'accueil de l'utilisateur actuel (/Users/[utilisateur actuel]/Library/InputManagers/). La présence du virus dans le dossier InputManagers implique qu'il sera exécuté dès qu'une autre application le sera. Il est possible que l'utilisateur soit invité à entrer le mot de passe d'administrateur pour que le processus décrit ci-dessus se déroule. En effet, le virus doit pouvoir écrire d'autres fichiers dans le dossier Applications (/Applications).

Lorsqu'il est exécuté, le virus utilise l'outil de recherche *Spotlight* pour identifier les quatre dernières applications utilisées qui ne dépendent pas des droits d'administrateur (*root*). Quand il les trouve, le virus modifie leur processus de lancement pour qu'il soit exécuté au préalable. Le virus

[3] National Vulnerability Database : http://nvd.nist.gov/statistics.cfm, French Security Incident Response Team : http://www.frsirt.com/search.php, Secunia : http://secunia.com/vendor/
[4] http://vil.nai.com/vil/content/v_138578.htm
[5] http://forums.macrumors.com/

place également les marqueurs *oompa* et *loompa*[6] dans les fichiers qu'il a infectés pour éviter toute réinfection. Lorsque l'application est lancée et que le virus est en place, l'utilisateur est averti de l'infection par le message « *Welcome to Darwin!* » (Bienvenue à Darwin !), comme illustré à la figure 5.

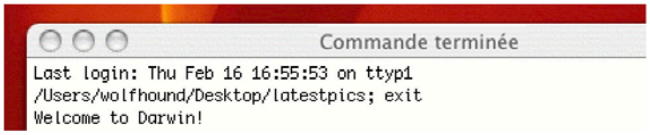


Figure 5 – Exécution du virus contenu dans .latestpics confirmée par le message « Welcome to Darwin! »

A cause d'un bogue dans ce processus, les applications infectées ne s'exécutent plus correctement par la suite. Bien qu'il semble que l'auteur ait prévu une propagation du virus via la messagerie électronique (*mail.app)*, OSX/Leap se diffuse uniquement par la messagerie instantanée, s'envoyant à tous les contacts de la liste d'amis (*AIM/iChat buddy list)* de l'utilisateur à chaque démarrage de l'application. On peut en conclure que le code viral n'a pas été optimisé pour être mis en circulation, mais qu'il a plutôt été programmé à des fins de test.

Apple a vivement réagi face à l'annonce de la découverte d'OSX/Leap, refusant d'accorder à ce dernier le statut de virus. « [OSX/Leap] n'est pas un virus, c'est un logiciel malveillant que l'utilisateur doit lui-même télécharger et ensuite exécuter », a commenté la société. « Apple recommande toujours aux utilisateurs Macintosh de n'accepter que des fichiers provenant de fournisseurs et de sites web connus et fiables[7]. »

S'il est exact que l'utilisateur doit exécuter des actions spécifiques pour activer la fonction d'autoréplication du logiciel malveillant, la position adoptée par Apple rappelle la première réaction de Microsoft en 1995 face au premier virus de macro, *WM/Concept*, alors qualifié de « macro farce » plutôt que de virus. De fait, de nombreux virus Windows exigent également de l'utilisateur qu'il décompresse volontairement un fichier joint puis double-clique dessus pour démarrer un exécutable. Selon ces critères, *OSX/Leap* est donc bel et bien un virus.

Pour supprimer le virus, l'utilisateur doit d'abord supprimer le fichier *latestpics*, qui contient le virus même. Si l'utilisateur intervient avant l'exécution du fichier, la suppression est complète. Sinon, tous les fichiers présents dans le dossier temporaire doivent également être supprimés, de même que le fichier */Users/[UTILISATEUR ACTUEL*[8]*]/Library/InputManagers/apphook.bundle*.

L'ordinateur doit ensuite être redémarré pour terminer la suppression du virus. En outre, les applications infectées doivent être réinstallées à partir d'une sauvegarde précédente.

Rien ne va plus pour Mac OS X

Quarante-huit heures à peine après l'annonce de la diffusion d'*OSX/Leap, OSX/Inqtana.a*[9] et ses variantes surgissent. Coiffés au poteau, les auteurs de cette seconde vague n'ont probablement pas obtenu la publicité qu'ils recherchaient. Contrairement à *OSX/Leap*, *OSX/Inqtana.a* exploite une vulnérabilité Mac OS X de type traversée de répertoires (« directory traversal ») par le biais des services d'échange de fichiers *Bluetooth*, portant la référence CVE-2005-1333.[10] Le virus s'installe dans une zone normalement interdite, ce qui lui permet de s'exécuter au redémarrage suivant. Une fois exécuté, le virus recherche les périphériques *Bluetooth* acceptant des transferts de fichiers via le service OBEX (OBject EXchange) (requêtes de type *push*). Si l'utilisateur accepte la requête sur l'ordinateur cible, le virus exploite la vulnérabilité et se copie en dehors du dossier d'échange. Apple a développé un patch corrigeant la vulnérabilité exploitée par *OSX/Inqtana.a.*[11], disponible sur son site web.

En février 2006, deux nouvelles vulnérabilités Mac sont mises au jour, exploitées par *OSX/Exploit-ZipShell*[12] et *OSX/Exploit-ScriptEx*[13]. La première concerne les navigateurs *Safari* et la seconde, l'application de messagerie *Apple Mail*. Ces deux applications, parce qu'elles sont à même d'exécuter certains scripts avec des autorisations avancées, peuvent être détournées de sorte qu'elles exécutent un script de shell sans que l'utilisateur en soit informé. Visant à ouvrir des fichiers multimédias, des images de disque et des archives, ces vulnérabilités concernent les fichiers d'archive ZIP dans le cas de *Safari* et les fichiers au format MIME AppleDouble pour ce qui est d'*Apple Mail*. Un pirate peut donc exploiter ces vulnérabilités pour exécuter une application et, en principe, prendre le contrôle d'un ordinateur à distance.

Notez que le client de messagerie *Thunderbird* de Mozilla Foundation ne souffre pas de telles vulnérabilités pour la simple raison qu'il ne prend pas en compte les sous-types MIME /appledouble et /applefile. Apple a distribué

[6] L'auteur du logiciel malveillant semble s'être inspiré des Oompa-Loompas, les minuscules ouvriers du livre Charlie et la chocolaterie, pour nommer les marqueurs.
[7] Peter Cohen, « Reports Emerge of Mac OS X Trojan Horse or Worm », *Macworld*, 16 février 2006, *http://www.macworld.com/news/2006/02/16/oompa/index.php*
[8] [UTILISATEUR ACTUEL] correspond au nom de la session utilisateur en cours au moment où l'ordinateur a été infecté.

[9] *http://vil.nai.com/vil/content/v_138608.htm*
[10] « Directory traversal vulnerability in the Bluetooth file and object exchange services in Mac OS X 10.3.9 allows remote attackers to read arbitrary files » (La vulnérabilité de type traversée de répertoires au niveau des services d'échange d'objets et de fichiers Bluetooth dans Mac OS X version 10.3.9 permet à des attaquants distants de lire des fichiers arbitraires) : *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1333*
[11] Mise à jour de sécurité *Security Update 2005-005* (Client) : *http://www.apple.com/support/downloads/securityupdate2005005client.html*
Mise à jour de sécurité *Security Update 2005-005* (Server) : *http://www.apple.com/support/downloads/securityupdate2005005server.html*
[12] *http://vil.nai.com/vil/content/v_138661.htm*
[13] *http://vil.nai.com/vil/content/v_138663.htm*

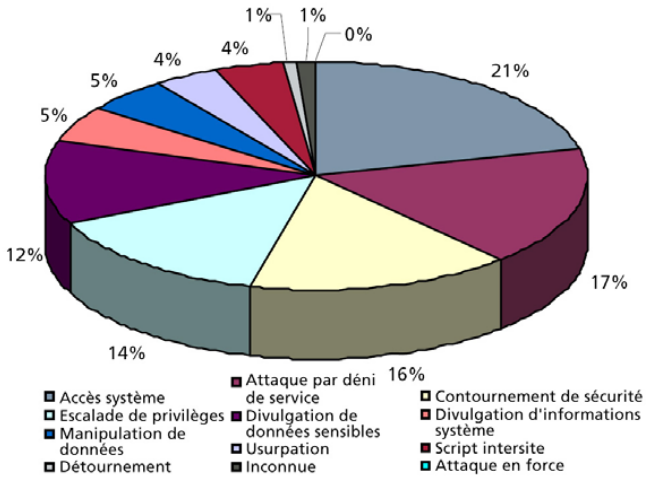
récemment des patchs[14] corrigeant ces vulnérabilités. Toutefois, les utilisateurs doivent veiller à désactiver dans leur navigateur l'option d'ouverture automatique des fichiers « fiables » après téléchargement.

Mac OS X : quel avenir ?

Parmi les attaques récentes, aucune n'a semble-t-il connu de propagation à grande échelle, du fait peut-être de la présence de bogues dans le code et de la faible empreinte de Mac OS sur le marché. Toutefois, étant donné la facilité avec laquelle il est possible d'accéder au code source des logiciels malveillants sur Internet, il faut s'attendre à ce que d'autres attaques soient lancées. Même si le nombre total de virus ciblant Mac OS X reste relativement faible depuis janvier 2004, la découverte d'un nombre croissant de vulnérabilités Macintosh risque d'attirer des pirates plus doués. Ainsi, le 21 février 2006, Apple a essuyé la première attaque émergente[15] ciblant Mac OS, avec la distribution des exploits *OSX/Exploit-ZipShell* et *OSX/Exploit-ScriptEx* tirant parti de vulnérabilités inconnues jusqu'alors. Huit jours se sont écoulés avant qu'Apple ne distribue un patch de sécurité pour ces vulnérabilités (le 1er mars 2006).[14]

Si de nombreux utilisateurs Macintosh restent convaincus que leurs systèmes sont à l'abri d'attaques, il leur faudra pourtant renoncer rapidement à leur politique de l'autruche. En outre, la décision récente d'Apple d'équiper tous les nouveaux Macintosh de microprocesseurs Intel pourrait marquer le début d'une nouvelle ère pour les logiciels malveillants ciblant ces ordinateurs. Si aucune menace au niveau des puces n'a été observée à ce jour, l'architecture commune ne passera pas inaperçue auprès des cyberpirates. Pour ne rien arranger, les technologies de virtualisation telles que Q, QEMU, WinTel 2.1 et Parallels Workstation, de même que la nouvelle technologie Boot Camp d'Apple, en offrant aux utilisateurs Mac des performances élevées avec une installation parallèle des systèmes d'exploitation Windows et Mac OS X, les exposent en fait aux menaces propres à ces deux plates-formes.

Le patch distribué par Apple en mars 2006 pour colmater la brèche exploitée par *OSX/Inqtana.a* corrige également vingt autres vulnérabilités[16] dont auraient pu tirer parti des attaquants locaux ou distants à des fins d'escalade de privilèges, de détournement d'ordinateur ou d'attaques par déni de service. Les derniers patchs d'Apple corrigent plus d'une quinzaine de vulnérabilités supplémentaires. La vulnérabilité de la plate-forme Mac OS X ne fait aucun doute, et les utilisateurs Macintosh — à l'instar de leurs homologues Windows — doivent rester vigilants face aux menaces, nouvelles ou en évolution.



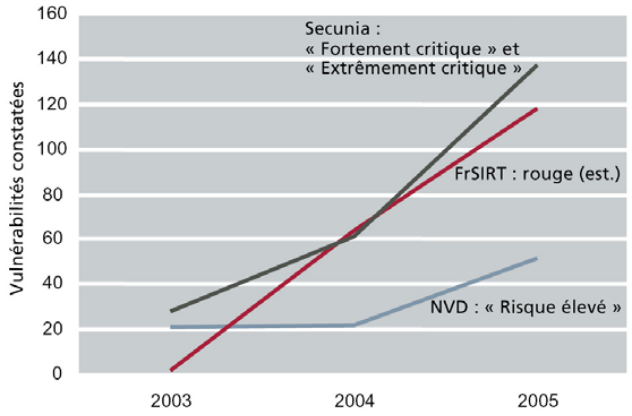
Source : Secunia, http://www.secunia.com/product/96/

Figure 6 – Répartition des attaques Mac OS X en fonction de leur impact, 2003-2006

La figure 6 montre l'impact des attaques lancées sur Mac OS X, tel qu'observé par Secunia. Dans la figure 7, la distribution annuelle des failles de sécurité critiques découvertes pour la plate-forme Mac OS X est représentée pour les années 2003, 2004 et 2005. La croissance rapide observée par les centres de recherche NIST et FrSIRT démontre l'intérêt grandissant des auteurs de logiciels malveillants pour ce système d'exploitation[17,18].

Le 19 avril 2006, un chercheur spécialisé dans la sécurité informatique a révélé l'existence de six autres vulnérabilités potentiellement exposées à des menaces émergentes. Exploitées par un individu malveillant, ces vulnérabilités auparavant inconnues peuvent mener au détournement ou au blocage d'un ordinateur. Elles sont donc considérées comme extrêmement dangereuses et classées « hautement critiques », même si elles nécessitent une certaine interaction de la part de l'utilisateur (p. ex. l'ouverture d'un fichier ZIP ou la consultation d'une page web contenant des graphismes) [19].

[14] Mise à jour de sécurité *Security Update 2006-001* : http://docs.info.apple.com/article.html?artnum=303382
[15] Un exploit dit « émergent » (en anglais, *zero-day*) utilise une vulnérabilité qui n'a pas encore été corrigée, c.-à-d. pour laquelle aucun patch ou correctif n'est disponible.
[16] http://www.frsirt.com/bulletins/1155
[17] http://www.frsirt.com/searchengine.php
[18] http://secunia.com/vendor/17/
[19] http://secunia.com/advisories/19686/



Sources : National Vulnerability Database, French Security Incident Response Team et Secunia

Figure 7 – Vulnérabilités Mac OS X, 2003-2005

Par le passé, la faible proportion d'utilisateurs Mac a limité l'intérêt des auteurs de logiciels malveillants pour cette plate-forme. Aujourd'hui, la donne a changé. La forte popularité des produits grand public d'Apple (notamment le périphérique iPod et le service iTunes) éveille l'appétit des pirates et crée de nouvelles cibles pour les activités malveillantes. En 2005, quatre vulnérabilités, qui auraient pu donner lieu à des escalades de privilèges ou à l'exécution de code arbitraire, ont été découvertes dans iTunes[20]. Février 2006 a vu l'apparition de *Slurp*, le premier logiciel malveillant véhiculé par iPod. *Slurp* est conçu pour parcourir les fichiers de données et dérober les informations stratégiques d'un ordinateur connecté à un iPod infecté[21].

Le nouveau penchant des auteurs de logiciels malveillants pour des attaques de précision, à petite échelle, dans le but de réaliser en toute discrétion des gains financiers ciblés et, d'autre part, l'accès aisé au code des exploits Mac sur Internet risquent d'exposer la plate-forme Mac OS aux menaces qui frappent actuellement la communauté Windows (réseaux de robots, logiciels espions, logiciels publicitaires, spam, attaques par déni de service distribué, etc.). A l'heure où les vulnérabilités et les attaques de Mac OS se multiplient, un conseil s'impose aux utilisateurs Mac : ne vous croyez pas à l'abri et soyez vigilants.

[20] National Vulnerability Database : *http://nvd.nist.gov/*
[21] *http://vil.nai.com/vil/content/v_138662.htm*