

**Objet :** Suite à l'apparition d'un premier ver pour la plate-forme **Mac OS X** baptisé **OSX/Leap-A** qui se propage automatiquement sur les réseaux de messagerie instantanée AIM , un second ver appelé **OSX/Inqtana.A**, exploitant une vulnérabilité de type "traversée de répertoire" dans le service d'échange de fichiers par connexions "Bluetooth" , vient d'être mis au point pour but de preuve de concept ( "Proof-of-Concept") sur les systèmes **MacOS X versions 10.4.1 et antérieures** (serveur et client). **OSX/Inqtana.A** devrait **s'arrêter de se propager le 24 Février** si pas de nouvelles versions apparues.

## 1- OSX/Leap-A

**Systèmes concernés :** Systèmes Mac OS X

<b>Effets</b>	<p>Une fois OSX.Leap.A est exécuté il réalise les actions suivantes :</p> <ol style="list-style-type: none"> <li><b>Affiche le message suivant :</b> <code>/Users/apple/mac/Desktop/Latestpics; exit</code>  <i>Welcome to Darwin!</i>  <i>APPLE-MACs-Computer:~apple/mac\$ /Users/apple/mac/Desktop/Latestpics; exit logout [Process completed]</i></li> <li><b>Crée les fichiers suivants :</b> <code>/tmp/latestpics , /tmp/latestpics.tgz, /tmp/latestpics.tar.gz , /tmp/hook , /tmp/apphook , /tmp/pic.gz , /tmp/apphook.tar, /tmp/pic</code></li> <li><b>Détruit tous les fichiers du répertoire</b> <code>~/Library/InputManagers</code></li> <li><b>Copie</b> <code>/tmp/apphook</code> dans <code>~/Library/InputManagers/apphook/apphook.bundle/Contents/MacOS,</code> afin d'être lancé à chaque boot du système.</li> <li><b>Se duplique par différents moyens :</b> Recherche pour l'extended attribut oompa. et s'il ne le trouve pas il infecte les fichiers des exécutables récemment utilisés en copiant le contenu du data fork vers la ressource fork du fichier sélectionné, puis en se copiant dans la data fork du fichier sélectionné et Crée l'extended attribut oompa et le positionne en loompa.</li> <li><b>Supervise les applications lancées ;</b> à chaque fois qu'une application iChat est lancée, le ver envoie le fichier <b>latestpics.tgz</b> à tous les contacts</li> </ol>
<b>Signes visibles d'infection</b>	<p>- Parfois, observation de dysfonctionnement de certaines applications dû à un bug dans le processus de duplication du ver</p> <p>- OSX.Leap.A arrive à la machine victime au message instantané <b>iChat</b> vous invitant de télécharger le fichier latestpics.tgz</p> <p style="padding-left: 20px;"><i>Name: latestpics.tgz</i>  <i>Kind: gzip compressed archive</i>  <i>Size: 2314.7 MB</i></p> <p>- Si l'utilisateur accepte de sauvegarder, le fichier archive est enregistré sous le nom <b>latestpics.tgz</b>, une fois ouvert le fichier <b>latestpics</b> est créée.</p>
<b>Degré d'infection à l'échelle Internationale</b>	Limité (Niveau 1)
<b>Degré d'infection à l'échelle nationale</b>	Limité
<b>Propagation</b>	<p>Ce ver se répand par le biais de programmes de messagerie instantanée, entre autres <b>iChat d'Apple</b>.</p> <p>Le ver se fait passer au travers son message « <b>attrape nigaud</b> » comme étant des images de la prochaine version de l'OS d'AppleMac OS X Leopard. En acceptant de télécharger le fichier, l'utilisateur reçoit le code malveillant compressé en attachement nommé "latestpics.tgz"</p>
<b>Pour plus de détails</b>	<ul style="list-style-type: none"> <li>- <a href="http://cme.mitre.org/data/list.html#4">http://cme.mitre.org/data/list.html#4</a></li> <li>- <a href="http://www.f-secure.com/v-descs/leap_a.shtml">http://www.f-secure.com/v-descs/leap_a.shtml</a></li> <li>- <a href="http://www.symantec.com/avcenter/venc/data/osx.leap.a.html">http://www.symantec.com/avcenter/venc/data/osx.leap.a.html</a></li> <li>- <a href="http://www.sophos.com/virusinfo/analyses/osxleapa.html">http://www.sophos.com/virusinfo/analyses/osxleapa.html</a></li> <li>- <a href="http://vil.nai.com/vil/content/v_138578.htm">http://vil.nai.com/vil/content/v_138578.htm</a></li> <li>- <a href="http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=51355">http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=51355</a></li> <li>- <a href="http://www.viruslist.com/en/weblog?weblogid=180198992">http://www.viruslist.com/en/weblog?weblogid=180198992</a></li> </ul>

## MESURES PREVENTIVES

Il est conseillé de faire preuve de vigilance, et de prendre des précautions similaires à celles prises sur les systèmes Microsoft Windows.

- Mettre à jour automatiquement votre Anti-virus.
- Ne pas ouvrir des fichiers joints de messages aux quels vous ne vous attendez pas.
- Isoler immédiatement les machines infectées pour empêcher une plus ample propagation au sein de votre réseau.
- Configurer votre serveur mail de sorte à bloquer ou de supprimer tout email ayant des fichiers joints communément utilisés pour la propagation de virus  
Nettoyage manuel :
- Si le fichier latestpics n'a pas été exécuté, il suffit de le détruire, ainsi que les fichiers associés (fichiers d'attributs oompa ou loompa) et de redémarrer l'ordinateur
- Sinon il faudra détruire le fichier suivant /Users/[CURRENT USER]/Library/InputManagers/apphook.bundle et redémarrer l'ordinateur.

## 2- OSX/Inqtana.A

**Systèmes concernés :** Systèmes Mac OS X versions **10.4.1** et antérieures (serveur et client)

<b>Effets</b>	Une fois installé sur le système, "Inqtana" tente de - créer des fichiers sur la machine victime en exploitant la vulnérabilité " <b>Directory Traversal</b> " de Apple Mac OS X BlueTooth : - chercher les systèmes Bluetooth qui acceptent des fichiers via le service "OBEX Push", afin de se propager sur ces systèmes.
<b>Signes visibles d'infection</b>	- Le ver crée les fichiers suivants /Users/wOrm-support.tgz /Users/InqTest.class /Users/com.openbundle.plist /Users/com.pwned.plist /Users/libavetanaBT.jnilib  -Les répertoires suivants sont également créés avec des fichiers sains utilisés pour l'exécution du ver : /Users/javax /Users/de  - Pour s'exécuter à chaque démarrage de Mac OS X, le ver crée les deux fichiers suivants : /Users/[USER NAME]/Library/LaunchAgents/com.pwned.plist /Users/[USER NAME]/Library/LaunchAgents/com.openbundle.plist
<b>Degré d'infection à l'échelle Internationale</b>	Limité (Niveau 2)
<b>Degré d'infection à l'échelle nationale</b>	Limité
<b>Propagation</b>	Le ver se propage en se copiant sur d'autres ordinateurs via une connexion bluetooth.
<b>Pour plus de détails</b>	<a href="http://www.f-secure.com/v-descs/inqtana_a.shtml">http://www.f-secure.com/v-descs/inqtana_a.shtml</a> <a href="http://www.viruslist.com/en/viruses/encyclopedia?virusid=112525">http://www.viruslist.com/en/viruses/encyclopedia?virusid=112525</a> <a href="http://vil.nai.com/vil/content/v_138608.htm">http://vil.nai.com/vil/content/v_138608.htm</a> <a href="http://www.sophos.com/virusinfo/analyses/osxinqtanaa.html">http://www.sophos.com/virusinfo/analyses/osxinqtanaa.html</a> <a href="http://www.symantec.com/avcenter/venc/data/osx.inqtana.a.html">http://www.symantec.com/avcenter/venc/data/osx.inqtana.a.html</a> <a href="http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=OSX_INQTANA.A">http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=OSX_INQTANA.A</a>

## Solution

- Mettre à jour automatiquement votre Anti-virus afin de prendre en compte le ver décrit .

- ou mettez à jour manuellement :

- **Mise à jour Symantec**
  - <http://securityresponse.symantec.com/avcenter/defs.download.html>
- **F-Secure**
  - <ftp://ftp.f-secure.com/anti-virus/updates/fsupdate.exe>
  - <http://f-secure.com/download-purchase/latest.zip>
- **NAI**
  - [http://download.nai.com/products/mcafee-avert/daily\\_dats/DAILYDAT.ZIP](http://download.nai.com/products/mcafee-avert/daily_dats/DAILYDAT.ZIP)
  - [http://download.nai.com/products/mcafee-avert/daily\\_dats/SDATDAILY.EXE](http://download.nai.com/products/mcafee-avert/daily_dats/SDATDAILY.EXE)
- **Sophos**
  - <http://www.sophos.com/downloads/ide/inqtan-a.ide>
- **TrendMicro**
  - <http://www.trendmicro.com/ftp/products/pattern/lpt221.zip>
  - <http://www.trendmicro.com/ftp/products/pattern/lpt221.tar>
- **Kaspersky (AVP)**
  - [http://downloads1.kaspersky-labs.com/updates\\_zip/daily.zip](http://downloads1.kaspersky-labs.com/updates_zip/daily.zip)

Il est toujours conseillé de faire preuve de vigilance et de prendre les mesures préventives suivantes :

- Ne pas ouvrir des fichiers joints de messages aux quels vous ne vous attendez pas.

- Isoler immédiatement les machines infectées pour empêcher une plus ample propagation au sein de votre réseau.

- Configurer votre serveur mail de sorte à bloquer ou de supprimer tout e-mail ayant des fichiers joints communément utilisés pour la propagation de virus