***BitDefender : Le Top 5 des e-menaces pour les utilisateurs de Mac***
**SÃ©curitÃ©**
PostÃ© par : JerryG
PubliÃ©e le : 25/1/2011 13:30:00

**Les menaces sur Mac nâ□□ont jamais Ã©tÃ© aussi rÃ©pandues** que sur Windows et ont, pour le moment, eu des effets moins dÃ©vastateurs.

Pourtant, en passant la barre des 9% de parts de marchÃ©, le systÃ¨me Mac OS X est devenu **une cible Ã  fort potentiel pour les auteurs de malwares** : escroqueries, vols dâ□□identitÃ©, fraudes bancaires, utilisation de lâ□□ordinateur Ã  lâ□□insu des utilisateurs par des pirates, etc. ne sont plus lâ□□apanage des utilisateurs de Windows.

Plusieurs centaines de e-menaces spÃ©cialement conÃ§ues pour la plateforme Mac OS X sont rÃ©pertoriÃ©es Ã  ce jour. Certaines sont de simples applications adwares prÃªtes Ã  profiter de notre naÃ¯vetÃ© humaine, alors que dâ□□autres sont de dangereux outils capables dâ□□exploiter des failles logicielles et de dÃ©tourner des identifiants bancaires ou dâ□□exposer lâ□□ensemble des donnÃ©es dâ□□un ordinateur Ã  un attaquant.

**Voici le Top 5 de ces e-menaces :**

### *1. Trojan.OSX.Jahlav.A & Trojan.OSX.Jahlav.A*

La famille OSX.Jahlav a Ã©tÃ© dÃ©couverte en novembre 2008, lorsquâ□□elle a commencÃ© Ã  Ãªtre diffusÃ©e sous la forme dâ□□un faux codec. Afin de convaincre les utilisateurs de tÃ©lÃ©charger et dâ□□installer le fichier DMG (image disque) malveillant, une page a Ã©tÃ© crÃ©Ã©e, censÃ©e contenir une vidÃ©o ne pouvant Ãªtre lue sans le fameux codec. Si lâ□□utilisateur lâ□□installe, la charge utile malveillante du malware tÃ©lÃ©charge automatiquement dâ□□autres chevaux de Troie Ã  partir dâ□□un serveur web distant.

### *2. Trojan.OSX.RSPlug.A*

Il sâ□□agit de lâ□□une des plus dangereuses familles de malwares fonctionnant sous Mac OS X. Le cheval de Troie RSPlug joue Ã©galement la carte du codec manquant afin de convaincre les utilisateurs de tÃ©lÃ©charger et dâ□□installer son fichier DMG infectÃ©. Il est particuliÃ¨rement prÃ©sent sur les sites web pornographiques. Une fois installÃ©, ce cheval de Troie modifie les entrÃ©es du serveur DNS afin de rediriger le trafic vers des imitations de domaines, crÃ©Ã©es par des phisheurs leur permettant de recueillir des informations confidentielles concernant des comptes

bancaires, e-mails, etc.

Ce type dâ□□attaque est extrÃªmement difficile Ã  remarquer, puisque lâ□□utilisateur est redirigÃ© vers une copie quasi-parfaite dâ□□un site web, mÃªme sâ□□il tape correctement lâ□□URL ou accÃ¨de Ã  un marque-page qui fonctionnait auparavant. Le seul indice pourrait Ãªtre lâ□□absence de certificat SSL.

### *3. Trojan.OSX.HellRTS.A*

Trojan.OSX.HellRTS.A est plus quâ□□une simple e-menace, il sâ□□agit dâ□□un kit Ã©laborÃ© de dÃ©veloppement de malwares. Le pack contient une application client-serveur, le serveur Ã©tant un service backdoor sâ□□exÃ©cutant sur la machine infectÃ©e et lâ□□application cliente Ã©tant utilisÃ©e par lâ□□attaquant pour Ã©mettre des commandes. Outre le client et le serveur, le pack contient une application de configuration, Configurator, qui Â« rÃ©ajuste Â» en permanence les Ã©lÃ©ments essentiels du cheval de Troie tels que le port dâ□□Ã©coute ou le mot de passe de la connexion, ainsi quâ□□un moteur SMTP, utilisÃ© pour transmettre Ã  lâ□□attaquant TOUS les messages reÃ§us par la victime.


Si le systÃ¨me est infectÃ©, un attaquant peut effectuer de nombreuses opÃ©rations Ã  distance sur lâ□□ordinateur infectÃ©, allant de simples plaisanteries agaÃ§antes (lancement de la messagerie

instantanÃ©e, lancement dâ□□applications et de pages web, arrÃªt du systÃ¨me) Ã  des actes extrÃªmement nÃ©fastes (notamment lâ□□obtention de toutes les donnÃ©es disponibles sur le disque dur ou la redirection des e-mails entrants vers lâ□□adresse de lâ□□attaquant). Lâ□□attaquant peut Ã©galement voir lâ□□utilisateur travailler Ã  son insu via le module Â« Desktop View Â».

### *4. Trojan.OSX.OpinionSpy.A*

La famille de spywares OpinionSpy est gÃ©nÃ©ralement installÃ©e par certaines applications distribuÃ©es gratuitement telles que des Ã©crans de veille et des convertisseurs audio/vidÃ©o. Lâ□□utilitaire dâ□□installation de ces applications rÃ©cupÃ¨re le package de spywares, lâ□□installe et lâ□□exÃ©cute avec des privilÃ¨ges root. Trojan.OSX.OpinionSpy.A se prÃ©sente comme Ã©tant un outil de recherche marketing, mais il ne sâ□□intÃ©resse pas uniquement aux habitudes et prÃ©fÃ©rences de navigation des utilisateurs : il ouvre Ã©galement des backdoors et des accÃ¨s vers de nombreux documents dÃ©tectÃ©s Ã  la fois sur les disques locaux et distants.

### *5. Trojan.OSX.Boonana.A*

Trojan.OSX.Boonana.A est une e-menace multiplateforme sâ□□exÃ©cutant Ã  la fois sous Windows, Mac OS X et Linux. Ce malware Java tÃ©lÃ©charge des fichiers malveillants dans le dossier de dÃ©part de lâ□□utilisateur, dans un dossier invisible nommÃ© Â« .jnana Â», puis installe un serveur IRC local, et un serveur Web, entre autres. Le malware Boonana tente Ã©galement de modifier les paramÃ¨tres du serveur DNS afin de dÃ©tourner les requÃªtes de sites lÃ©gitimes vers des sites web Â« spoofÃ©s Â», dans le cadre dâ□□une tentative de phishing extrÃªmement efficace.

Â« *Les utilisateurs de Mac sont concernÃ©s par un nombre plus restreint de e-menaces que les adeptes de Windows, mais nous leur recommandons dâ□□adopter des mesures prÃ©ventives pour sâ□□assurer de profiter dâ□□Internet sans mauvaises surprises.* Â» dÃ©clare **Fabrice Le Page**, Chef de Produit BitDefender chez Editions Profil. Â« *La sÃ©curitÃ© est pour nous une prioritÃ© depuis 15 ans, et ce, quâ□□elle que soit la plateforme ciblÃ©e : Mac OS, Windows ou Linux. Se protÃ©ger câ□□est aussi protÃ©ger les personnes avec qui nous communiquons et contribuer Ã  bloquer lâ□□expansion des malwares qui polluent nos usages numÃ©riques. MÃªme si la surenchÃ¨re nâ□□est pas notre objectif, il nâ□□en reste pas moins quâ□□il suffit dâ□□un seul virus pour Ãªtre infectÃ©* Â».