

BitDefender : Le Top 5 des e-menaces pour les utilisateurs de Mac

S curit 

Post  par : JerryG

Publi e le : 25/1/2011 13:30:00

Les menaces sur Mac n'ont jamais  t  aussi r pandues que sur Windows et ont, pour le moment, eu des effets moins d vastateurs.

Pourtant, en passant la barre des 9% de parts de march , le syst me Mac OS X est devenu **une cible   fort potentiel pour les auteurs de malwares** : escroqueries, vols d'identit , fraudes bancaires, utilisation de l'ordinateur   l'insu des utilisateurs par des pirates, etc. ne sont plus l'apanage des utilisateurs de Windows.

Plusieurs centaines de e-menaces sp cialement con sues pour la plateforme Mac OS X sont r pertori es   ce jour. Certaines sont de simples applications adwares pr tes   profiter de notre n vet  humaine, alors que d'autres sont de dangereux outils capables d'exploiter des failles logicielles et de d tourner des identifiants bancaires ou d'exposer l'ensemble des donn es d'un ordinateur   un attaquant.

Voici le Top 5 de ces e-menaces :



1. Trojan.OSX.Jahlav.A & Trojan.OSX.Jahlav.A

La famille OSX.Jahlav a  t  d couverte en novembre 2008, lorsqu'elle a commenc     tre diffus e sous la forme d'un faux codec. Afin de convaincre les utilisateurs de t l charger et d'installer le fichier DMG (image disque) malveillant, une page a  t  cr  e, cens e contenir une vid o ne pouvant  tre lue sans le fameux codec. Si l'utilisateur l'installe, la charge utile malveillante du malware t l charge automatiquement d'autres chevaux de Troie   partir d'un serveur web distant.

2. Trojan.OSX.RSPlug.A

Il s'agit de l'une des plus dangereuses familles de malwares fonctionnant sous Mac OS X. Le cheval de Troie RSPlug joue  galement la carte du codec manquant afin de convaincre les utilisateurs de t l charger et d'installer son fichier DMG infect . Il est particuli rement pr sent sur les sites web pornographiques. Une fois install , ce cheval de Troie modifie les entr es du serveur DNS afin de rediriger le trafic vers des imitations de domaines, cr  es par des phisheurs leur permettant de recueillir des informations confidentielles concernant des comptes

bancaires, e-mails, etc.

Ce type d'attaque est extrêmement difficile à remarquer, puisque l'utilisateur est redirigé vers une copie quasi-parfaite d'un site web, même s'il tape correctement l'URL ou accède à un marque-page qui fonctionnait auparavant. Le seul indice pourrait être l'absence de certificat SSL.

3. Trojan.OSX.HellRTS.A

Trojan.OSX.HellRTS.A est plus qu'une simple e-menace, il s'agit d'un kit de développement de malwares. Le pack contient une application client-serveur, le serveur étant un service backdoor s'exécutant sur la machine infectée et l'application cliente étant utilisée par l'attaquant pour envoyer des commandes. Outre le client et le serveur, le pack contient une application de configuration, Configurator, qui « ajuste » en permanence les paramètres essentiels du cheval de Troie tels que le port d'écoute ou le mot de passe de la connexion, ainsi qu'un moteur SMTP, utilisé pour transmettre à l'attaquant TOUS les messages reçus par la victime.



Si le système est infecté, un attaquant peut effectuer de nombreuses opérations à distance sur l'ordinateur infecté, allant de simples plaisanteries agaçantes (lancement de la messagerie

instantané, lancement d'applications et de pages web, arrêt du système) – des actes extrêmement rapides (notamment l'obtention de toutes les données disponibles sur le disque dur ou la redirection des e-mails entrants vers l'adresse de l'attaquant). L'attaquant peut également voir l'utilisateur travailler à son insu via le module « Desktop View ».

4. Trojan.OSX.OpinionSpy.A

La famille de spywares OpinionSpy est généralement installée par certaines applications distribuées gratuitement telles que des écrans de veille et des convertisseurs audio/vidéo. L'utilitaire d'installation de ces applications récupère le package de spywares, l'installe et l'exécute avec des privilèges root. Trojan.OSX.OpinionSpy.A se présente comme étant un outil de recherche marketing, mais il ne s'intéresse pas uniquement aux habitudes et préférences de navigation des utilisateurs : il ouvre également des backdoors et des accès vers de nombreux documents d'ectés – la fois sur les disques locaux et distants.

5. Trojan.OSX.Boonana.A

Trojan.OSX.Boonana.A est une e-menace multiplateforme exécutant – la fois sous Windows, Mac OS X et Linux. Ce malware Java télécharge des fichiers malveillants dans le dossier de départ de l'utilisateur, dans un dossier invisible nommé « .jnana », puis installe un serveur IRC local, et un serveur Web, entre autres. Le malware Boonana tente également de modifier les paramètres du serveur DNS afin de détourner les requêtes de sites légitimes vers des sites web « spoofés », dans le cadre d'une tentative de phishing extrêmement efficace.

« Les utilisateurs de Mac sont concernés par un nombre plus restreint de e-menaces que les adeptes de Windows, mais nous leur recommandons d'adopter des mesures préventives pour assurer de profiter d'Internet sans mauvaises surprises. » déclare **Fabrice Le Page**, Chef de Produit BitDefender chez Editions Profil. « La sécurité est pour nous une priorité depuis 15 ans, et ce, quelle que soit la plateforme ciblée : Mac OS, Windows ou Linux. Se protéger c'est aussi protéger les personnes avec qui nous communiquons et contribuer à bloquer l'expansion des malwares qui polluent nos usages numériques. Même si la surenchère n'est pas notre objectif, il n'en reste pas moins qu'il suffit d'un seul virus pour être infecté ».