

## SourceFire : Les menaces les plus fréquentes, Bitdefender répond

### Sécurité

Posté par : JerryG

Publié le : 31/1/2012 15:00:00

La technologie **FireCLOUD de Sourcefire**, qui constitue la solution de protection contre les malwares perfectionnés FireAMP, est une plateforme puissante pour analyser la sécurité des données. Ce court rapport fait état des données collectées sur les postes de travail en France. Plusieurs tendances se dégagent de l'analyse effectuée sur ces données.

### Méthodologie

Tout d'abord, nous avons identifié tous les fichiers malicieux provenant d'un poste utilisateur en France. Ensuite, pour chaque malware détecté, nous avons identifié l'application logicielle qui a permis de laisser entrer ce malware sur le poste de travail. Dans certains cas, ces malwares proviennent d'applications malicieuses dont le seul but est d'installer un malware.

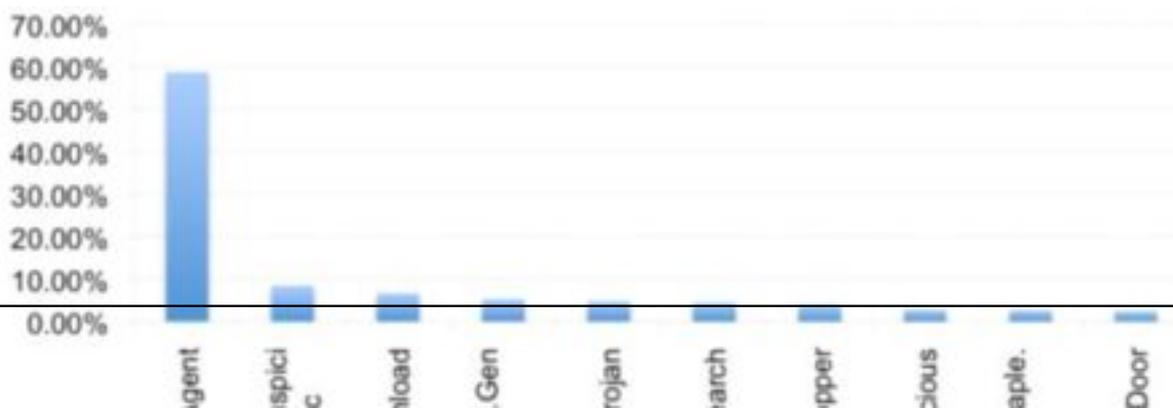


Dans d'autres cas, il s'agit d'applications légitimes tels que des navigateurs web dont la sécurité a été compromise à un instant T ou il s'agit de l'installation d'un programme malveillant par un utilisateur à son insu.

Nous avons segmenté l'analyse en deux phases. Pour l'une d'entre elles, nous avons ignoré la version de l'application (ex., nous n'avons pas fait de distinction entre Internet Explorer 8.0.6001.18702 et la version 9.0.8112.16421). Le but était de faire ressortir les tendances des applications au plus haut niveau. Dans la seconde phase, nous avons tenu compte de la version de l'application.

### Résultats

- Le malware le plus répandu en France est W32.Agent.
- Les 10 principaux malwares les plus détectés en France représentent 35,5% de l'ensemble des détections. (Le tableau ci-après fournit la répartition en pourcentage de ces 10 malwares).



- Les 4eme et 9eme malwares les plus frÃ©quents en France ont Ã©tÃ© dÃ©tectÃ©s grÃ¢ce Ã la technologie Spero Machine Learning, spÃ©cifique Ã Sourcefire et conÃ§ue pour dÃ©tecter de faÃ§on proactive les menaces inconnues.

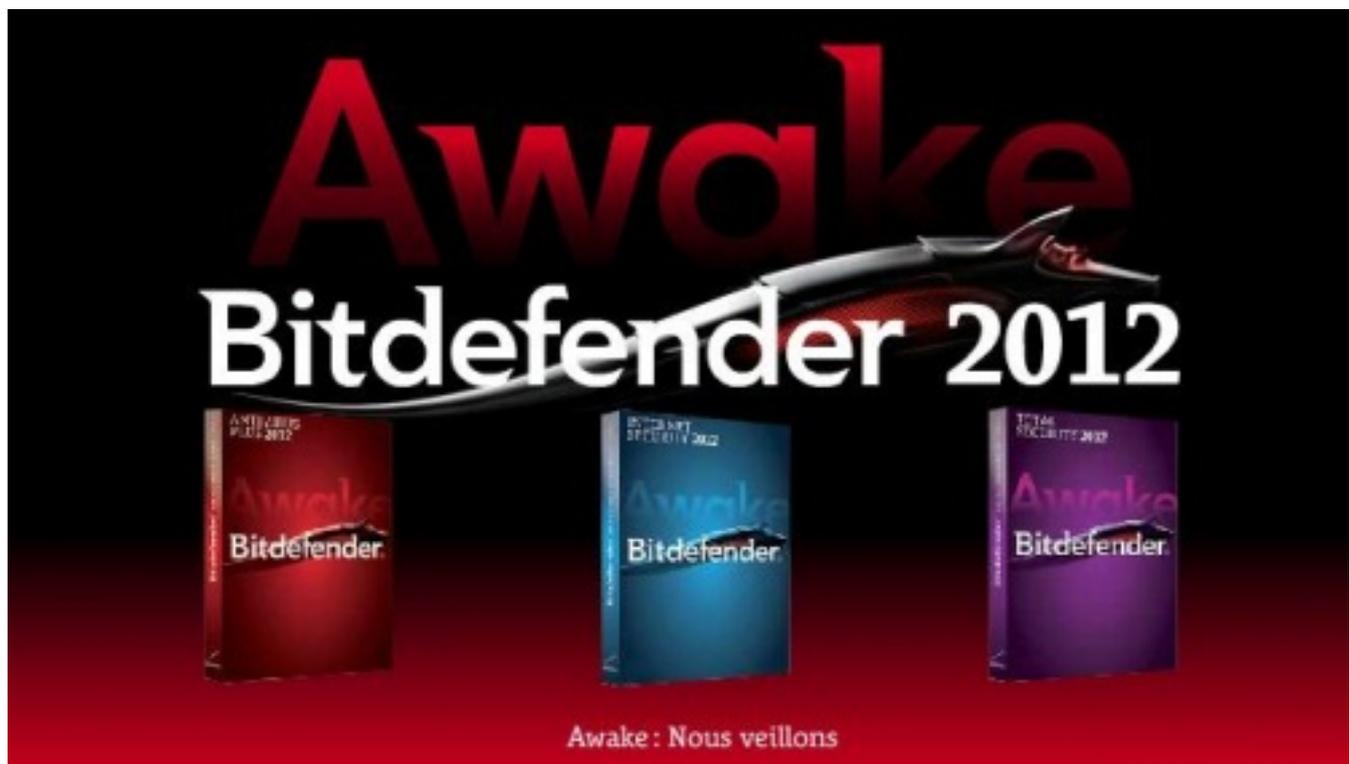
- Actuellement, le malware le plus rÃ©pandu en France est contenu dans le programme "service.exe", certainement une tentative de la part des hackers de tromper l'utilisateur qui souhaite installer l'application Windows "services.exe" ( avec un Ã« s Ã» Ã services). Le prochain malware Ã se rÃ©pandre massivement sera sans doute contenu dans l'application "EmangEloh.exe", un nom dÃ©jÃ associÃ© Ã d'autres logiciels malveillants connus.

En France, parmi les principaux navigateurs, Chrome apporte la plupart des malwares, suivi de Firefox, et d'Internet Explorer.

**Oliver Friedrichs**, Senior Vice PrÃ©sident Cloud Technology Group de Sourcefire, nous confiait rÃ©cemment :

Ã« L'adoption rapide d'Immunet atteste et dÃ©montre que les utilisateurs recherchent aussi bien une couche supplÃ©mentaire de protection pour renforcer leurs dÃ©fenses, et une approche plus adaptative pour bloquer les menaces persistantesÃ»

Ã« Cette adaptabilitÃ© est possible grÃ¢ce Ã une [approche Big Data](#), devenue incontournable dans le paysage des menaces et des attaques d'aujourd'hui. Les solutions anti-malware traditionnelles ne peuvent tout simplement pas atteindre le niveau de protection et de contrÃ´le que les clients souhaitent Ã».



**Christophe Delorme**, Directeur Marketing et Communication chez Editions Profil, rÃ©pond Ã

cette affirmation.

« La forte croissance du nombre de codes malveillants ainsi que lvolution de leur forme et de leurs objectifs ont depuis des annes, rendu les technologies traditionnelles insuffisantes, en particulier celles bases sur les seules analyses par signature. Les diteurs ont ds adapter pour faire face  cela mais ont parfois eu le tort de penser quune nouvelle technologie ou approche pourrait se substituer  une autre. Cela a t par exemple le cas de ceux qui ont mis sur des technologies 100% proactives ou dautres sur le 100% cloud.

Tous ont t obligs de revenir en arrire ou ont disparu. Chez Bitdefender, nous avons toujours pens que ctait lajout et la bonne coordination de differentes couches de protection qui pouvaient offrir le niveau de scurit que lutilisateur est en droit dattendre de sa solution. Cest ainsi que nous mixons dtection par signatures, analyse comportementale et analyse in-the-cloud de faon totalement transparente pour lutilisateur, apportant ainsi  ce dernier les avantages de chaque technologie et en supprimant les limites et contraintes de chacune. Cette approche a t conforte ces derniers mois par les rultats obtenus dans des tests de rfrence comme AV Test qui ont dmontr un taux de protection de 100% contre les attaques zro-day et les menaces rellement en circulation.»