

**Bitdefender : La page d'accueil d'Opera expose ses utilisateurs à l'exploit BlackHole**

**Sécurité**

Posté par : JerryG

Publié le : 16/11/2012 14:00:00

Depuis quelques heures, les utilisateurs d'Opera sont exposés aux e-menaces du triste kit d'exploits BlackHole. Les systèmes d'analyse automatisée de Bitdefender nous ont signalé ce matin qu'un script malveillant obscurci chargé par l'adresse [redirigeait](#) les utilisateurs vers une page malveillante hébergeant le triste exploit BlackHole.

Le script a sans doute été chargé via une publicité publiée par un tiers, une pratique appelée « malvertising ».



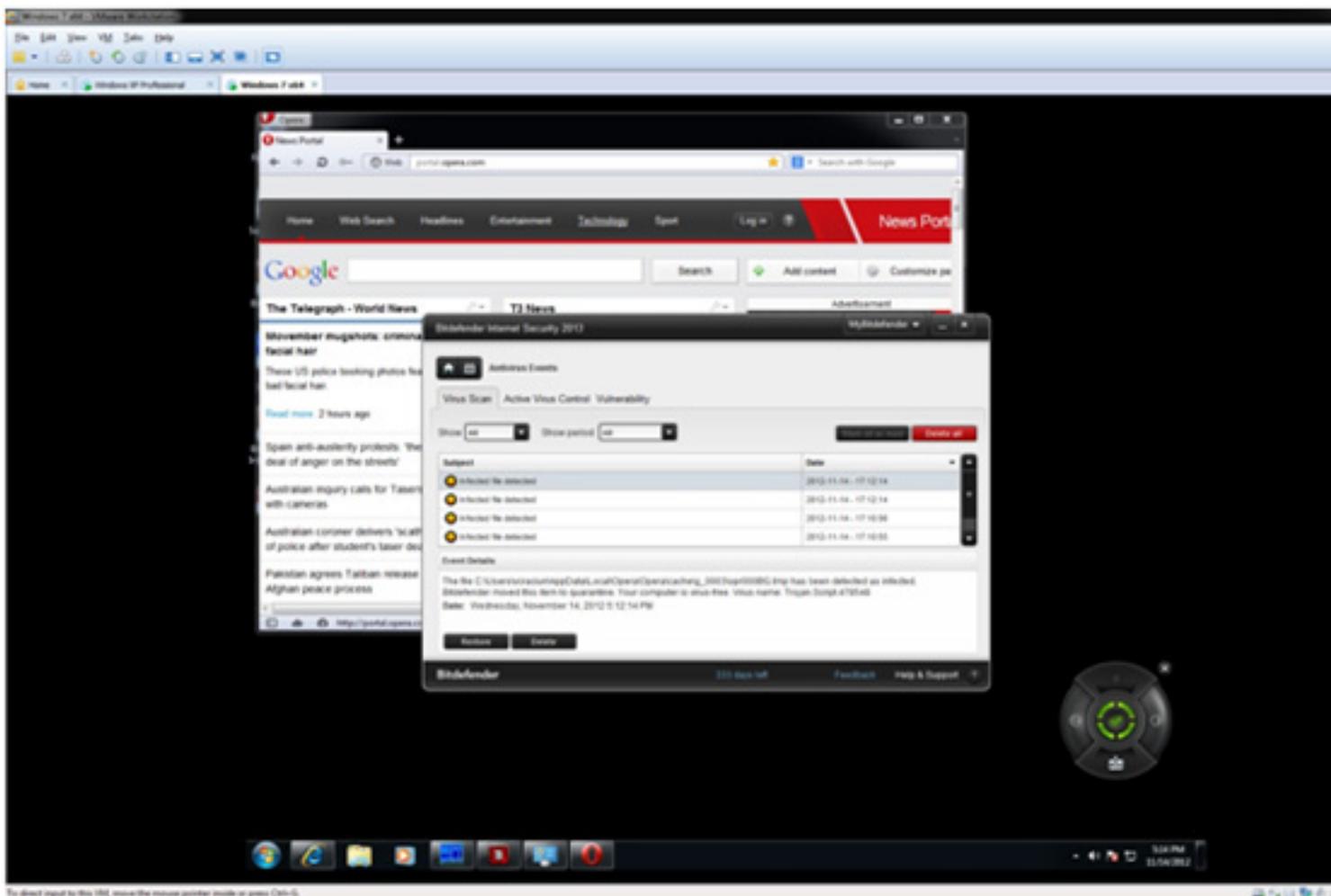
Ce code dissimulé dans la page d'accueil du portail d'Opera insère une iFrame qui charge du contenu malveillant à partir d'une source externe. Si l'utilisateur d'Opera n'a pas changé sa page d'accueil par défaut, il chargera involontairement du contenu actif malveillant à partir d'un site Web tiers ((g[supprimé]750.com/in.cgi) lorsqu'il ouvre son navigateur.

**Bitdefender détecte un malware lorsque la page d'accueil du portail d'Opera est chargée**



Cette page malveillante héberge le kit d'exploits BlackHole (nous avons reçu l'échantillon par un fichier PDF contenant l'exploit CVE-2010-0188) qui infecte l'utilisateur malchanceux avec une variante de ZBot récemment compilée, indiquée par Bitdefender sous le nom de « Trojan.Zbot.HXT ». Le malware ZBot se trouve sur un serveur en Russie, qui a probablement été victime lui aussi d'une attaque, permettant un accès non autorisé via FTP.

**Bitdefender détecte le script sous le nom de « Trojan.Script.478548 »** ; la page incriminée est chargée par le Portail d'Opera à également bloquée dès le début de l'attaque par le bloqueur d'URL dans le cloud.



Si vous craignez d'avoir été infecté, exécutez une analyse rapide en 60 secondes sur le site Web de Bitdefender Quickscan.

[Pour retrouver Bitdefender](#)