***BlindElephant accÃ©lÃ¨re et affine lâidentification des applications Web***
**Mac et Linux**
PostÃ© par : JerryG
PubliÃ©e le : 29/7/2010 15:00:00

**Qualys, Inc**. le principal fournisseur de solutions Ã  la demande pour la gestion des risques de sÃ©curitÃ© informatique et de la conformitÃ©, annonce **BlindElephant, un moteur Open Source** rapide et prÃ©cis pour identifier les versions des applications Web et des plug-ins Ã  lâaide de fichiers statiques.

En marge de cette annonce, des travaux d'analyse seront dÃ©voilÃ©s Ã  l'occasion de Black Hat USA 2010 sur les rÃ©sultats de tests Ã  grande Ã©chelle de cet outil qui dÃ©montrent l'utilisation de logiciels non mis Ã  jour mettant en danger de nombreuses applications Web bien connues.

***De nombreuses applications Web classiques*** sont utilisÃ©es dans diffÃ©rents domaines, notamment pour gÃ©rer des blogs ou des forums, faire de l'e-commerce, gÃ©rer des bases de donnÃ©es ou envoyer ou recevoir du courriel. De par leur nature, ces applications prÃ©sentent des risques de sÃ©curitÃ© spÃ©cifiques. Et dans la mesure oÃ¹ toujours plus de vulnÃ©rabilitÃ©s sont dÃ©couvertes, il est important de pouvoir dÃ©tecter de maniÃ¨re fiable les applications et les plug-ins utilisÃ©s sur un site ainsi que l'utilisation de versions non actualisÃ©es. Contrairement Ã  d'autres outils destinÃ©s aux applications Web, BlindElephant utilise une nouvelle stratÃ©gie qui s'appuie sur le Â« hashage Â» de fichiers de ressources statiques au sein de l'application pour trouver un numÃ©ro de version.

Â« *Les applications Web standards sont rÃ©guliÃ¨rementÂ ciblÃ©es par les pirates puis corrompues pour distribuer des codes malveillants,* Â» dÃ©clare **Wolfgang Kandek**, CTO de Qualys. Â« *Nous diffusons l'outil BlindElephant en tant que projet Open Source qui permettra aux entreprises de se protÃ©ger et de superviser leurs applications Web. Il s'agit d'une premiÃ¨re collaboration avec la communautÃ© dans le but d'augmenter le nombre d'applications Web identifiÃ©es.* Â»

Â« *Avec BlindElephant, les professionnels de la sÃ©curitÃ© et les administrateurs systÃ¨me identifient tout ce qui tourne sur leurs serveurs, notamment toutes les applications Web que les utilisateurs ont pu tÃ©lÃ©charger,* Â» dÃ©clare **Patrick Thomas**, expert sÃ©curitÃ© chez Qualys et crÃ©ateur de BlindElephant. Â« *Cet outil ne vÃ©rifie pas les vulnÃ©rabilitÃ©s ni lâexposition des applications Ã  un exploit spÃ©cifique mais les versions de celles-ci exÃ©cutÃ©es sur un site.* Â»

**Quelques avantages de BlindElephant :**

- Intervention manuelle rÃ©duite pour la prise en compte et lâidentification de nouvelles versions/applications

- RÃ©sistance au durcissement (suppression de banniÃ¨res)

- DÃ©tection fine pour rÃ©duire les faux positifs et les faux nÃ©gatifs

- RÃ©utilisation du mÃªme code pour toutes les applications prises en charge

- Vitesse et gestion de la charge pour une utilisation sur le plus grand nombre dâapplications

- Faible utilisation des ressources

***Pour chaque application supportÃ©e par cet outil, BlindElephant*** conserve un grand nombre de versions de rÃ©pertoires. Tous les fichiers et les rÃ©pertoires sont traitÃ©s puis un Â« hash Â» est calculÃ© pour chaque fichier. Ce Â« hash Â» est stockÃ© dans une table temporaire avec le chemin et la version de l'application d'origine. La prÃ©cision de l'outil a Ã©tÃ© prouvÃ©e via une analyse Ã  grande Ã©chelle sur des sites visibles sur Internet. Les rÃ©sultats de l'analyse comprennent des informations sur les applications Web actuellement supportÃ©es qui sont les plus utilisÃ©es ainsi que la distribution de leurs versions.

**Lâanalyse sâest concentrÃ©e sur certaines applications Open Source parmi les plus populaires et notamment :**

- Drupal (systÃ¨me de gestion de contenu)

- Joomla! (systÃ¨me de gestion de contenu)

- Mediawiki (logiciel Wiki)

- Moodle (systÃ¨me de cours virtuels)

- MovableType (logiciel de blog)

- phpBB (logiciel de forum)

- phpMyAdmin (logiciel de gestion de bases de donnÃ©es)

- SPIP (systÃ¨me de gestion de contenu)

- Wordpress (logiciel de blog)

Et Patrick Thomas d'ajouter : Â« Le but de cet outil est de fournir un Â« Ã©tat des lieux Â» plutÃ´t que de signaler les vulnÃ©rabilitÃ©s spÃ©cifiques d'une application. Â»

**DisponibilitÃ©**

Patrick Thomas prÃ©sentera BlindElephant et ses travaux dâanalyse lors dâune session de 70 minutes le 28 juillet Ã  15h15 (heure dâÃ©tÃ© du Pacifique) pendant lâÃ©vÃ©nement Black Hat USA 2010.

**BlindElephant** est un outil Open Source immÃ©diatement disponible en tÃ©lÃ©chargement.

Pour tÃ©lÃ©charger les travaux de recherche sur BlindElephant ou obtenir plus de dÃ©tails, rendez-vous sur **le site de la communautÃ© Qualys**.

Cette technologie dâidentification est actuellement disponible dans QualysGuard Vulnerability Management.