Communiqué de Presse

www.pandasecurity.com/france

Des faux sites web annoncent la démission de Barack Obama pour convertir les ordinateurs des internautes en PC zombies

- **Plus de 40 sites web relaient l'annonce de la prétendue démission du président des États-Unis**

- **Sur ces sites, les utilisateurs sont invités à télécharger un fichier pour découvrir toute l'histoire. Ce faisant, ils installent sur leur ordinateur plusieurs codes malveillants.**

- **Ceux-ci transforment leur ordinateur en PC zombie, contrôlé à distance par des pirates.**

Paris, le 20 janvier 2009

PandaLabs, le laboratoire d'analyse et détection des malwares de Panda Security, a détecté plus de quarante sites web qui exploitent l'élection de Barack Obama pour propager des codes malveillants. Ces pages ont pour titre : "Barack Obama has refused to be a President" *(Barack Obama renonce à la présidence).*

Lorsque les internautes cliquent sur l'article, une fenêtre s'ouvre leur proposant de télécharger un fichier pour en savoir plus cette prétendue nouvelle. Il s'agit en réalité de fichiers malveillants qui seront installés sur l'ordinateur. Ces fichiers muent l'ordinateur des victimes en PC zombie contrôlé à distance par des pirates. Une capture d'écran est disponible à l'adresse : http://www.flickr.com/photos/panda_security/3209435502/.

« Les ordinateurs zombies sont organisés en réseaux, les "botnets", que les cybercriminels contrôlent à distance au moyen de codes malveillants appelés les "bots". Ces botnets sont loués par les pirates à des tiers qui les utilisent, par exemple, pour envoyer du spam ou lancer des attaques par déni de service. », explique Luis Corrons, le directeur technique de PandaLabs.

Selon PandaLabs, cette attaque semble avoir été lancée depuis la Chine car tous les domaines impliqués ont été achetés auprès d'une entreprise chinoise déjà connue pour son implication par le passé dans des cyber-attaques.

Ce n'est pas la première fois que la notoriété de Barack Obama est utilisée par les pirates. Lors de la campagne présidentielle et des jours qui ont suivi l'élection, les cybercriminels ont propagé de nombreuses fausses nouvelles visant à infecter les ordinateurs avec des codes malveillants.

Pour plus d'informations sur cette attaque, consultez le blog de PandaLabs à l'adresse http://pandalabs.pandasecurity.com/archive/Malware-Campaign-Impersonates-Barack-Obama_2700_s-Website.aspx.

A propos de PandaLabs

Depuis 1990, la mission de PandaLabs est d'analyser les nouvelles menaces le plus rapidement possible pour assurer une totale sécurité à nos clients. Pour cela, PandaLabs a développé un système automatisé et innovant qui analyse et traite les milliers de nouveaux échantillons reçus chaque jour et renvoie automatiquement un verdict (logiciel malveillant ou

inoffensif). Ce système repose sur l'Intelligence Collective Antimalware, le nouveau modèle de sécurité de Panda Security, qui détecte même les codes malveillants capables de passer au travers des autres solutions de sécurité.

Actuellement, 94 % des malwares détectés par PandaLabs sont analysés par l'Intelligence Collective Antimalware. Cette analyse automatique est complétée par le travail de plusieurs équipes spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, rootkits, etc.) qui travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Grâce à ce système, Panda peut offrir à ses clients des solutions plus sûres, plus simples et consommant moins de ressources.

Pour plus d'informations, visitez le blog de PandaLabs : http://www.pandalabs.com

	ATTACHEE DE PRESSE : ÉMILIE SACKSICK **SACKSICK@ELIOTROPE.FR** ➲ LIGNE DIRECTE : **01 53 17 16 43**	**ELIOTROPE** 151, rue du Faubourg Saint Antoine 75011 Paris France **www.eliotrope.fr** TEL : + 33 (0)1 53 17 16 40 FAX : + 33 (0)1 53 17 16 41