Communiqué de presse

LES SPAMMEURS METTENT À PROFIT LE BATTAGE MÉDIATIQUE AUTOUR DE LA SORTIE DE L'iPHONE 5 POUR LANCER DES ATTAQUES DE MALWARE

Le rapport Cyberoam sur les menaces Internet pour le deuxième trimestre 2011, fruit des travaux de recherche menés par son auteur sur la sécurité des applications mobiles et les réseaux sociaux, identifie des attaques de malware d'un nouveau genre visant l'iPhone 5.

FRANCE, 27 juillet 2011 - Cyberoam, division d'Elitecore Technologies et initiateur de solutions de gestion unifiée des menaces (UTM, *Unified Threat Management*) basées sur l'identité, annonce la publication de son rapport sur les tendances des menaces Internet (édition de juillet 2011), préparé en collaboration avec son partenaire Commtouch. Durant ce trimestre, les spammeurs ont redoublé d'ingéniosité, profitant du battage médiatique autour de la sortie de l'iPhone 5 pour alimenter les rumeurs sur ce nouveau modèle (terminal plus plat et plus véloce, doté d'un écran plus confortable, à l'intégration cloud optimisée, etc.) en usant de texte et d'images factices pour appâter des utilisateurs naïfs.

La totalité des images et liens inclus dans le courrier électronique en question renvoyaient à un fichier iPhone.gif qui n'était en réalité rien d'autre qu'un programme malveillant baptisé iPhone.gif.exe. Le simple fait de cliquer sur un lien téléchargeait ce fichier de malware dissimulé dans un site légitime.

« La popularité mondiale croissante de l'iPhone et d'autres terminaux mobiles sous Android attire aussi bien l'attention des développeurs d'applications que celle des cyberdélinquants. En l'état actuel des études menées par Cyberoam sur les smartphones s'agissant des failles de sécurité et de la divulgation d'informations personnelles, nous sommes convaincus que les actuelles attaques de malware sur le web ne sont que les prémices d'un phénomène qui donnera lieu à un nombre illimité d'attaques ciblées sur le terminal lui-même. À l'avenir, il faut s'attendre à ce que les applications de médias sociaux opèrent des attaques ciblées sur les téléphones mobiles en raison du chevauchement accru entre univers physique et virtuel, dès lors que l'anonymat des utilisateurs en ligne n'existera plus », souligne Abhilash Sonwane, vice-président senior de la gestion de produits chez Cyberoam.

Autre épisode marquant : des spammeurs ont pris Facebook et ses 500 millions d'utilisateurs actifs pour cibles, avec des messages de type « visionner la vidéo sur Oussama Ben Laden ». Le lien en question, renvoyant prétendument à la vidéo de l'exécution du chef d'Al Qaïda, s'est ensuite propagé viralement sur

Facebook, aiguillant les utilisateurs vers des sites malveillants. Le code malveillant transmettait des messages nominatifs censés émaner d'un « ami » du destinataire, intégrant un lien hypertexte.

« La diffusion massive et non sollicitée sur Facebook de la vidéo consacrée à Oussama Ben Laden dans les heures qui ont suivi son exécution met en exergue l'empressement et l'agilité dont font preuve les cyberdélinquants pour tirer parti de l'actualité. Ils mettent à profit ces informations, en particulier les derniers gros titres du jour, et tentent de comprendre et d'analyser la psychologie des utilisateurs pour définir de redoutables codes permettant de leur soutirer des informations confidentielles », poursuit Abhilash Sonwane.

Autres faits marquants évoqués dans le rapport de juillet 2011 : la prolifération de programmes malveillants basés sur l'empoisonnement par SEO, les courriers électroniques factices de « rejet de paiement » en provenance de l'administration fiscale américaine (IRS) et les scripts malveillants incorporés à des fichiers Adobe PDF. La Journée mondiale de l'IPv6, le 8 juin dernier, a confirmé le probable remplacement du protocole IPv4 mais a également mis en avant les menaces potentielles qui accompagneront son introduction.

Cliquez ici pour télécharger le rapport sur les menaces pour le deuxième trimestre 2011

À propos de Cyberoam

Axés sur l'identité des utilisateurs, les boîtiers UTM de Cyberoam offrent un bouclier de protection complet contre les menaces existantes et émergentes en provenance d'Internet, notamment les virus, les vers, les chevaux de Troie, les logiciels espions (spywares), ou encore les usurpations de type phishing et pharming. Pare-feu avec filtrage dynamique des paquets (stateful inspection), VPN, systèmes anti-virus, anti-logiciels malveillants et anti-spam au niveau des passerelles, système de détection et de prévention des intrusions, système de filtrage de contenu… Autant d'éléments qui constituent la panoplie complète des fonctions de sécurité proposées par Cyberoam. Il convient d'y ajouter son système de gestion de la bande passante et son système de gestion des liens multiples basé sur une plate-forme unique. Suite au lancement récent de la Version X, de nouvelles fonctionnalités ont été intégrées aux appliances Cyberoam UTM. Parmi ces nouveautés, on peut notamment citer une fonction permettant d'accroître la visibilité sur la couche applicative 7, une fonction de commande et de gestion de la messagerie instantanée, un dispositif de connectivité 3G/WWAN, une architecture de sécurité extensible, une interface utilisateur nouvelle génération et le logo Or « IPv6 Ready ». Le portefeuille de solutions Cyberoam comporte également la solution Cyberoam iView, une appliance de journalisation et de reporting, les appliances Cyberoam SSL VPN et la gamme Cyberoam Endpoint Data Protection qui permettent de protéger les données et de gérer les actifs au niveau des différents postes clients d'un réseau d'entreprise. Cyberoam a obtenu les certifications ICSA Labs et CheckMark (UTM Level 5). Membre du consortium *Virtual Private Network Consortium*, Cyberoam se positionne également parmi les « visionnaires » du *Magic Quadrant* de Gartner des pare-feux multifonctions pour PME. Cyberoam est établie à Woburn (Massachussets, États-Unis) et en Inde. Pour plus d'informations, rendez-vous sur : www.cyberoam.com/fr