cddb.ch/Bulletin Cybersécurité et Menaces Internet #009 – 2 mai 2012

Ce qu'il faut savoir, en bref.

Des systèmes du constructeur automobile Nissan ont été compromis. Seuls des identifiants et des condensés de mots de passe auraient été volés[1]. **Les prochaines versions du navigateur Firefox (version 12 et suivantes) seront dotées d'un mécanisme de mise à jour silencieuse**, n'affichant pas d'avertissement à l'utilisateur.[2][a] **Les Etats faisant usage de solutions de surveillance des télécommunications afin de commettre des violences sur leurs citoyens seront désormais soumis à des sanctions financières par les Etats-Unis**, ainsi que les éditeurs ou intermédiaires qui leur auraient fourni le produit[3].

Un correctif majeur de sécurité pour la plateforme gratuite de blogs WordPress est disponible depuis le 20 avril. L'éditeur a souhaiter conserver le silence sur le détail des failles de sécurité corrigées, mais confirme que ce nombre est composé de deux chiffres[4][b]. **Le système de vote électronique Sequoia a retourné un scrutin erroné** lors des récentes élections municipales de Palm Beach (Floride). Une erreur de configuration du vote en serait la cause, le système est actuellement utilisé dans plus de 300 municipalités[5]. **Une nouvelle variante du cheval de Troie FlashBack est en circulation**. Le programme vise les systèmes Mac OS[6]. Selon les experts, il rapporterait chaque jour plus de 10'000 dollars à ses créateurs en insérant son code à la place du dispositif publicitaire du moteur de recherche Google[7].

Les nouvelles versions Android du navigateur Chrome et le réseau social Twitter sont désormais équipées d'une option de proxy, les rendant compatibles avec des dispositifs d'anonymisation du trafic tels que Tor. De son côté, **Twitter pour appareils iPhone est désormais doté du *certificate pining***. Une mesure visant à inscrire en dur les certificats de sécurité du réseau social afin de protéger le logiciel contre certaines techniques d'interception. **Avec 54% de parts de marché, Amazon possède désormais plus de contrôle que Google** sur l'écosystème américain des tablettes numériques Android[8][c]. A Sydney, le constructeur de téléphones mobiles **Samsung aurait engagé des acteurs afin de simuler un mouvement de mobilisation sociale contre la firme concurrente, Apple**. Les manifestants invitaient les badauds à "se réveiller"[9].

75% des 200'000 plus importants sites web accessibles en *https* ont une configuration vulnérable à l'attaque BEAST. Cette attaque facilite le travail de l'attaquant souhaitant casser le chiffrement des jetons de session dans un échange SSL/TLS. Une simple modification de la configuration de ces serveurs empêcherait l'attaque[10]. **L'Iran est suspecté [ndlr: par les Etats-Unis] d'investir plus d'un milliard de dollars dans sa cyberdéfense**, entre autres, à travers des opérations de recrutement, d'équipement et de commandement informel de *cybermiliciens*[11]. **Les entreprises allemandes n'auront pas à dédommager des clients victimes d'une attaque informatique exploitant leur crédulité (tel que *le phishing*)**. C'est le jugement prononcé la semaine dernière par la Haute Cour en Allemagne[12].

1: http:// computerworld.com/s/article/9226596
2: http:// computerworld.com/s/article/9226463?taxonomyId=17
3: http://www.bbc.co.uk/news/world-us-canada-17817520
4: http://www.zdnet.com/blog/security/wordpress-332-is-out/11678
5: http://www.pcadvisor.co.uk/news/software/3349041/e-voting-system-awards-election-wrong-candidates-in-florida-village/
6: http://securitywatch.pcmag.com/none/296979-new-flashback-variant-spotted-in-the-wild
7: http://www.zdnet.com/blog/security/mac-botnet-generated-10000-a-day-for-flashback-gang/11727
8: http://www.readwriteweb.com/archives/its-official-google-has-lost-control-of-the-android-tablet-market.php
9: http://huffingtonpost.com/2012/04/26/samsung-reportedly-behind_n_1457375.html
10: http://www.csoonline.com/article/705158
11: http://www.washingtontimes.com/news/2012/apr/25/us-seen-as-iran-cyberarmy-target/
12: http://www.thelocal.de/money/20120425-42161.html

a: (ndlr) Une approche que de nombreuses entreprises n'apprécient guère, le risque d'incompatibilité avec des applications développées sans processus durable étant dès lors accru.
b: (ndlr) La recherche de vulnérabilités dans le logiciel WordPress est de haute valeur pour les pirates: le logiciel est actuellement déployé sur plus de 60 millions de serveurs dans le monde et constitue un excellent vecteur d'infection par chevaux de Troie.
c: (ndlr) Amazon n'est pas le premier constructeur à s'affranchir des services de Google en exploitant les possibilités offertes par la licence du système Android, plusieurs fabricants de téléphones portables évaluent cette stratégie. Il sera intéressant de voir si Google déploiera des efforts pour contourner cette tendance. Le risque étant bien évidemment la mise en place d'un nouvel écosystème applicatif, qui aurait pour effet de couper Google de tout revenu réalisé par la vente d'applications.

VOTRE AVIS EST LE BIENVENU! --> écrivez à mailing@cddb.ch
> Format de ce bulletin: préférez-vous le format précédent? l'actuel? une alternance?
> Souhaitez-vous plus d'analyses? Moins (juste des brèves)?
> A quelle fréquence préféreriez-vous que le bulletin soit émis?
FIN/#009.

Conditions et tarifs:
- Inscription : envoyer un email avec sujet "inscription texte" ou "inscription PDF" à cddb-mailing@nxtg.net
- Désinscription: envoyer un email avec sujet "désinscription" à cddb-unmailing@nxtg.net
- Le bulletin est publié sur http://cddb.ch deux semaines après sa diffusion par email
- Tarif: gratuit
Données sur les abonnements et abonnés:
- Mesures de confidentialité: best effort, liste d'abonnés stockée sur conteneur chiffré, envois en copie carbone
- Eléments conservés: uniquement adresse email et date d'inscription/désinscription
- Diffusion: aucune (sauf cas de force majeure ou distraction exceptionnelle)
- Suppression: sur demande, par email à cddb-mailing@nxtg.net
- Tiers identifiés: fournisseurs d'accès (envoi des bulletins en clair, par courrier électronique)