cddb.ch/Bulletin Cybersécurité et Menaces Internet #008 – 25 avril 2012

Sommaire

1. En bref

Texas - Plainte déposée contre les propriétaires d'applications mobiles trop gourmandes
Une plainte contre 18 entreprises technologiques a été déposée auprès des Tribunaux de l'Etat du Texas en mars dernier. Le plaignant reproche aux entreprises d'avoir violé les principes de la proportionnalité et de la transparence en collectant ses données personnelles au travers de leurs applications mobiles.
-- http://www computerworld.com/s/article/9225219/18_firms_sued_for_ using_privacy_invading_mobile_apps
[ndlr: le respect de ces mêmes principes est également exigé au sens de la Loi fédérale sur la protection des données. Toutefois, seule la survenance d'un dommage sur la personne visée par les données, p.ex.: diffamation ou usurpation d'identité, peut généralement être porté devant les tribunaux.]

Authentification avec le téléphone portable: l'opérateur est-il le nouveau maillon faible?
Le cheval de Troie Gozi, actuellement en circulation sur plusieurs systèmes de téléphonie mobile, a pour fonction première d'extraire et remettre à des tiers les divers identifiants spécifiques au téléphone et à la carte SIM qui s'y trouve installée. Une fois les informations relayées, le programme bloque le téléphone. Les fraudeurs contactent ensuite directement l'opérateur, ou l'un de ses points de vente, pour obtenir un remplacement de carte SIM "abîmée." Cette démarche compromet ainsi la chaîne de confiance établie dans les récentes applications bancaires dont l'authentification repose sur un code envoyé par SMS.
-- http://www.americanbanker.com/issues/177_54/mobile-payments-sim-cards-1047644-1.html

Marché noir d'exploits informatiques: entre 50'000 et 100'000 dollars par exploit
La faille de sécurité corrigée par l'éditeur Microsoft dans le bulletin de sécurité de mars [cf. bulletin cddb #007] a été l'occasion pour la presse de s'intéresser de près au marché *underground* des exploits informatiques. Selon Nicholas Percoco, directeur au sein du cabinet SpiderLabs, ces petits bouts de code exécutable ayant généralement pour but d'automatiser l'exploitation d'une faille de sécurité, et ainsi de faciliter la tâche à tout personne qui le possède, s'échangent à travers des marchés parallèles pour des montants se situant entre 50'000 et 100'000 dollars.
-- http://securitywatch.pcmag.com/security/295488-rdp-exploit-confirmed-patch-windows-now?obref=obinsite

Récompenses pour des failles de sécurité: Google augmente sa prime à 20'000 dollars
L'éditeur du célèbre moteur de recherche a annoncé ce lundi avoir augmenté à 20'000 dollars le montant maximum de la récompense reversée à ceux qui trouveraient une faille de sécurité critique dans l'un de ses services majeurs. Lancé en novembre 2010, ce programme a déjà permis à Google d'identifier plus de 11'000 vulnérabilités. 780 d'entre elles étaient suffisamment importantes pour que l'auteur soit récompensé d'une prime allant de 300 à 3'133.70 dollars [ndlr: oui, ce montant a bel et bien une signification.].
-- http://news.yahoo.com/google-raises-bounty-software-bugs-193717387.html
[ndlr: l'on ne manquera pas ici d'identifier le lien potentiel avec la brève précédente dans laquelle il est fait mention d'un marché noir particulièrement bien rémunéré des vulnérabilités de sécurité.]

Chevaux de Troie persistants...ou pas?
Un cas intéressant que le cheval de Troie Lurk... Après avoir compromis un terminal client via un vecteur de type *drive-by-download* (aucun clic n'est nécessaire, l'infection du client est immédiate sur simple consultation d'un site web infecté), ce dernier s'installe exclusivement en mémoire vive. Le Cheval de Troie disparaît donc dès l'arrêt de la machine. Les pirates ont solutionné le problème de la persistance par une astuce pertinente: ils infectent en priorité des sites web d'actualité vulnérables. Les pirates sont ainsi assurés que les internautes y retourneront probablement au moins une fois par jour. La "disparition" du Cheval de Troie n'est ainsi que de faible durée tout en rendant la tâche bien plus complexe devant un Tribunal: le programme malveillant ne laisse aucune trace de son passage sur les disques des systèmes infectés.
-- http://securitywatch.pcmag.com/apps-and-websites/295571-java-based-malware-is-fileless

Canada: 10'000 zombies pour un déni de service sur une plateforme de vote
Le système de vote électronique, déployé fin mars dernier pour l'élection du nouveau leader du parti politique NDP au Canada, a été sévèrement ralenti par un déni de service distribué. Selon les détails de l'investigation communiqués à la presse, un *botnet* composé de plus de 10'000 systèmes aurait été sollicité pour réaliser l'attaque. Les *zombies* ont ainsi dirigé des requêtes à répétition sur le réseau de la plateforme de vote, l'empêchant ainsi de recevoir correctement les requêtes provenant des internautes votants et des bornes de vote installées lors du rassemblement du parti. Selon un expert de l'université de Queen University (Kingston, Canada), la location d'un tel réseau de zombies pour une journée aurait coûté un peu moins de 100 (cent) dollars.
--
http://www.thestarphoenix.com/technology/Company+computers+behind+malicious+cyber+attack/6366386/story.html

Quelques chiffres sur les dénis de service... (source: Kaspersky, DDoS attacks Q2-2011)
Les États-Unis, l'Indonésie, la Pologne, l'Egypte et la Serbie constituent les 5 pays majeurs depuis lesquels des attaques coordonnées de déni de service sont lancées. 69% des attaques visent en priorité: des commerces en ligne, des plateformes de jeux en ligne, des banques et des plateformes de trading. 7% des attaques visent des sites d'actualité. 89% des attaques pointent sur le service web (HTTP), dont 72% sur une adresse IP spécifique (par opposition à une URL). Les attaques ont principalement lieu les jours de semaine, surtout le mardi et le mercredi.

2. Apple conserverait une copie des clés de chiffrement des données hébergées sur iCloud

Bien qu'il soit clairement communiqué dans les termes d'utilisation que les données des utilisateurs sont chiffrées et protégées de tout accès par un tiers lorsqu'elles sont synchronisées sur la plateforme iCloud, elles ne seraient en revanche pas du tout protégées d'un accès par Apple. Selon les clauses d'utilisation, ces données seraient même analysées.

Des journalistes du magazine technologique ArsTechnica ont examiné les éléments relatifs au chiffrement des données synchronisées sur la plateforme iCloud, le service de stockage de données en ligne proposé par Apple et destiné aux utilisateurs de ses systèmes.

L'analyse a révélé la mise d'un chiffrement de données réalisé en deux étapes. La première opération de chiffrement a lieu lors du transport des données vers iCloud (*in-transit data encryption*), réduisant ainsi le risque d'un vol de données dans le cas où un pirate intercepterait le flux établi entre l'appareil de l'utilisateur et les serveurs de Apple. La seconde opération de chiffrement a lieu côté service, dans la plateforme iCloud (*server-side data encryption*), réduisant à ce stade le risque d'un vol de données dans le cas d'une intrusion physique, ou logique, dans ses systèmes. Toutefois, le service n'opère aucun chiffrement des données avant leur envoi (*client-side data encryption*) sur iCloud.

Le modèle choisi présente deux opportunités intéressantes pour Apple. Premièrement, il permet à la firme de rassurer ses utilisateurs en leur garantissant que leurs données sont protégées par de la cryptographie et dès lors, les choses étant bien faites, protégées de tout accès par des tiers. Deuxièmement, ce modèle lui permet d'analyser l'intégralité des contenus placés en ligne par ses utilisateurs. Cette pratique est d'ailleurs clairement stipulée dans les conditions d'utilisation que l'utilisateur a probablement pris le temps de lire à tête reposée avant de les accepter: Apple se réserve le droit de dénoncer à l'organisme compétent toute suspicion d'infraction au droit d'auteur et/ou à la propriété intellectuelle, ainsi que les cas de contenus à caractère explicitement illicite. Cette clause leur permet ainsi la mise en œuvre d'un moyen de lutte active contre certaines formes de cybercriminalité exploitant les environnements *cloud* à haute dose (partage et revente de données volées, contenus à caractère pédopornographique, fichiers multimédia piratés). Bien entendu, le message s'adresse également à tous ceux et celles qui activeraient le service de synchronisation sur leurs équipements alors qu'ils contiennent des vidéos, musiques ou images pour lesquelles les droits nécessaires n'auraient pas été acquis. Sur ce point, l'intérêt économique de débusquer les fraudeurs potentiels est évident pour Apple, dans la mesure où la firme se positionne à la fois en fournisseur d'équipement qu'en fournisseur de contenus, via sa plateforme iTunes...

Une fois de plus, Apple n'est pas le canard boiteux contrairement à ce que l'on pourrait croire: la grande majorité des sociétés proposant des services d'archivage et synchronisation de fichiers pour particuliers et entreprises ont la fâcheuse habitude de conserver des copies des clés de chiffrement sans que le client n'en réalise les enjeux. A leur décharge, les entreprises inscrites au registre de commerce américain, ainsi que leurs subsidiaires, sont légalement tenues de conserver ces clés de chiffrement à disposition du Gouvernement, grâce à ce cher *Patriot Act*...

-- http://arstechnica.com/apple/news/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy.ars

3. Flashback: un réseau de 600'000 zombies Mac OS infectés, "grâce" à Java

FlashBack a été identifié sur les systèmes Mac OS en septembre 2011. Le nombre de machines infectées est toutefois resté minimal, probablement à cause de son vecteur d'infection basé sur un avertissement déguisé de mise à jour de l'extension Flash[1], ce qui le conditionnait à un clic bienveillant de l'utilisateur.

Une propagation facilitée par des diffusions de correctifs espacées
C'est le 14 février dernier qu'une nouvelle opportunité s'est présentée à ses concepteurs. Oracle (l'éditeur de Java) diffusait alors une série de correctifs de sécurité pour sa technologie, dont la correction d'une faille de sécurité permettant l'exécution de code à travers une simple "applet" Java chargée dans un navigateur[2]. Bien que touchés eux aussi, les systèmes Mac OS sont contraints de se conformer au processus mis en place par Apple pour les mises à jours. Le message est rapidement compris: la majorité des systèmes Mac OS ont l'extension Java installée et cette faille de sécurité (qui leur permet désormais de contourner la contrainte du clic) ne sera probablement pas corrigée par Apple avant plusieurs semaines, voire mois.

Comme attendu, la Pomme a publié son correctif de sécurité le 3 avril[3]. L'écart de six semaines entre la diffusion des deux correctifs a permis aux pirates de compléter la rétro-ingénierie du correctif initial et de modifier FlashBack. Cette optimisation s'est rapidement observée sur Internet: plus de 500'000 machines infectées dans les jours suivant la diffusion du 1er correctif!

Flashquoi?
FlashBack est ainsi nommé cheval de Troie en raison de son dispositif C&C (commande et contrôle). Ce dernier lui permet de récupérer des instructions depuis un serveur prédéfini par les pirates. Un algorithme à temps variable fait varier l'adresse de ce centre toutes les 24 heures, ce qui rend plus ardue une éventuelle collaboration judiciaire internationale[4]. Une machine infectée par Flashback est pour ainsi dire "à disposition" des administrateurs du centre de contrôle. Dans ce contexte, le modèle économique est relativement simple et rôdé: les 600'000 systèmes infectés peuvent être fouillés, pour y trouver des données destinées à la revente (accès bancaires, comptes de messagerie, réseaux sociaux, services payants, etc.) ou loués à des tiers, par exemple, pour des actions de déni de service sur une entreprise concurrente par exemple, ou un ex-employeur indélicat.

Sécurité des ordinateurs Mac OS: un signe de faiblesse?
Le cas FlashBack a permis à des détracteurs de la Pomme de délier leur langue, arguments et chiffres à l'appui. Une propagation sur plus de 600'000 systèmes en moins de deux mois, dont près de la moitié est concentrée uniquement aux Etats-Unis n'est pas moindre. Selon l'éditeur Sophos, 1 ordinateur Mac sur 5 serait actuellement infecté par un logiciel malveillant[5]. L'on observera néanmoins que le nombre de systèmes infectés a diminué de près de 70%, moins d'une semaine après la diffusion du correctif[6]...

1: http://www.symantec.com/security_response/writeup.jsp?docid=2011-093016-1216-99
2: http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
3: http://support.apple.com/kb/HT5228
4: http://news.drweb.com/show/?i=2341&lng=en
5: http://nakedsecurity.sophos.com/2012/04/24/mac-malware-study/
6: http:// symantec.com/connect/blogs/osxflashbackk-suffering-slashback-infections-down

FIN/#008.

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)