cddb.ch/Bulletin Cybersécurité et Menaces Internet #012 – 6 juillet 2012

Sommaire

1. L'actualité, en bref.....1
2. Décryptage - Le marché noir des failles de sécurité : quels enjeux pour le citoyen ?.....5

1. L'actualité, en bref

Syria Files – Wikileaks : diffusion de 2,4 millions de messages confidentiels
La fondation WikiLeaks a diffusé jeudi 5 juillet au matin un lot de plus de 2 millions de messages échangés entre officiels et représentants du gouvernement syrien. Le contenu des messages peut être consulté librement en ligne. Fait anecdotique : plus de 42'000 messages (1,7% du lot) sont vecteurs d'un cheval de Troie destiné à s'exécuter une fois la machine du destinataire atteinte. L'analyse du contenu des messages par plusieurs organismes de presse est en cours, l'un des objectifs est d'identifier la liste exhaustive des entreprises européennes ou américaines qui ont profité de la situation politique du pays pour commercialiser des solutions de surveillance et d'analyse des communications électroniques des citoyens. Ces outils constitueraient, selon plusieurs sources, les piliers de la stratégie de répression supposément mise en place dans le pays. Aucune entreprise suisse n'a, cette fois, été identifiée pour l'instant.
-- http://wikileaks.org/syria-files/

Piratage de comptes bancaires : moins de cas de vol mais plus d'agressivité
Le Financial Services Information Sharing and Analysis Center, un interlocuteur bancaire représentant 95 institutions financières américaines, a recensé plus de trois cents cas de piratage de comptes bancaires ayant résulté en un détournement de fonds durant l'année 2011, ce qui représenterait une croissance de plus de 30%. Les banques interrogées ont également communiqué avoir massivement investi, l'an dernier, dans la mise en place de l'authentification forte et le blocage automatique de compte en cas de comportement anormal sur les applications d'accès à distance. Le mécanisme d'authentification forte le plus privilégié serait l'appel téléphonique informatisé sur le numéro mobile du client afin de confirmer la transaction. [ndlr : on notera la corrélation avec le sujet traité dans CDDB#008 sur l'augmentation des cas de détournement et de fraude à la carte SIM...]
-- http:// computerworld.com/s/article/9228139/

Vol de mots de passe LinkedIn : recours collectif (class action) pour négligence
Une plainte en recours collectif contre LinkedIn a été déposée devant les Tribunaux de Californie. Il est reproché à l'éditeur d'avoir agi par négligence en ne respectant pas les bonnes pratiques de sécurité en matière de stockage de mots de passe et d'avoir enfreint ses obligations contractuelles. En effet, une clause contractuelle garantit que les bonnes pratiques seront mises en œuvre pour protéger les données des membres. Le plaignant exige 5 millions de dollars en réparation.
-- http://www.scribd.com/doc/97699996/LinkedIn-Lawsuit-Over-Stolen-Passwords

Paypal récompensera les chercheurs qui lui communiqueront des failles de sécurité
La solution de paiement électronique Paypal a annoncé la mise en place d'un programme de rémunération destiné aux chercheurs qui souhaiteraient lui communiquer des failles de sécurité. La démarche de l'éditeur s'inscrit dans celle d'autres éditeurs comme Google, Facebook, Mozilla et Samsung pour ne citer qu'eux. L'éditeur n'a pas indiqué le montant moyen des rétributions mais s'il s'aligne sur Google, le budget devrait atteindre 400'000 dollars par année. On notera que Paypal précise toutefois que seules quatre types de failles de sécurité sont concernés par le programme : les failles XSS, les failles CSRF, les injections SQL et les contournements de leur mécanisme de contrôle d'accès.
-- http://threatpost.com/en_us/blogs/paypal-starts-bug-bounty-program-security-research-062112

Une clé de chiffrement de 923 bits cassée par des chercheurs
Des chercheurs de l'université de Kyushu ont réussi à casser un élément chiffré par une clé d'une longueur de 923 bits. La clé a été obtenue en 148 jours en combinant l'effort de 21 ordinateurs, totalisant 252 cœurs de calcul. Pas d'inquiétude pour l'instant, l'exercice a porté sur un système cryptographique (Pairing-Based Cryprographic System) encore à l'état de recherche et qui n'est (normalement...) pas encore utilisé en dehors des milieux académiques. L'intérêt de ces travaux est toutefois prépondérant : il était estimé jusque-là qu'une telle longueur de clé ne pouvait être cassée qu'après plusieurs milliers d'années de calcul.
-- http://www.lemondeinformatique.fr/actualites/lire-des-chercheurs-reussissent-a-casser-une-cle-de-923-bits-49386.html

Facebook: une fonction de découverte d'utilisateurs se trouvant à proximité du téléphone
Facebook a ajouté une nouvelle fonctionnalité à la version mobile du réseau social qui permet à un utilisateur de trouver des utilisateurs se trouvant physiquement à proximité de son téléphone. La fonctionnalité n'affiche, pour l'instant, que des utilisateurs ayant explicitement autorisé cette fonctionnalité dans les paramètres de leur compte. Une fonctionnalité qui s'avèrera très intéressante si elle est adoptée par les utilisateurs (ou activée par défaut...) car elle permettra par exemple de détecter la présence de personnes dans un environnement sensible tel que dans les locaux d'une entreprise ou à une manifestation...
- - http://news.cnet.com/8301-1023_3-57459535-93/facebook-adds-find-friends-nearby-feature-for-web-mobile/

Apple Mac OS Mountain Lion 10.8 : nouvelles fonctionnalités de sécurité
La dernière mise à jour destinée aux développeurs désireux d'évaluer la prochaine mouture du système d'exploitation équipant les ordinateurs de la firme Apple a été dotée d'une fonctionnalité de mise à jour automatique. Activée, une recherche quotidienne de mises à jour pour le système sera effectuée automatiquement sans intervention de l'utilisateur. L'éditeur en a également profité pour modifier le slogan principal sur la sécurité de son système de "*doesn't get PC viruses*" à "*built to be safe*"...
-- http://
appleinsider.com/articles/12/06/25/apple_tones_down_language_touting_os_x_security_measures.html

Crypto-Tokens : plusieurs modèles répandus seraient vulnérables au *padding oracle*
Une étude récemment publiée à l'INRIA (Institut national de recherche en informatique et en automatique) aurait démontré que plusieurs modèles de jetons cryptographiques largement utilisés par les organisations (Aladdin e-Token, Gemalto Cyberflex, RSA SecurID 800, Safenet Ikey 2032, Siemens CardOS) seraient vulnérables à une attaque de type *padding oracle* (en résumé : une attaque consistant à révéler progressivement une clé de chiffrement en soumettant des contenus erronés à répétition à un système cryptographique un peu trop bavard).
-- http://hal.inria.fr/docs/00/70/47/90/PDF/RR-7944.pdf

Réglementation européenne des autorités de certification : 24 heures pour notifier !
Le projet de directive européenne destinée à réglementer les autorités de certification (délivrance de certificats électroniques) fournissant leurs services aux agences et administrations des états européens est en phase de finalisation. Le texte inclut entre autres un article imposant aux organismes de certification de notifier l'autorité compétente sous un délai maximal de 24 heures dès qu'une intrusion informatique est suspectée. Il inclut également un article imposant l'exécution d'audits de sécurité, et la communication des résultats à l'autorité compétente sur une base annuelle.
--
http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf

Mise à jour du logiciel gratuit John the Ripper: craquage par GPU et nouveaux formats
Une nouvelle version du logiciel libre de craquage de mots de passe John the Ripper est disponible. Cette version ajoute l'utilisation des processeurs graphiques et le support de nouveaux formats de fichiers protégés par mot de passe. L'utilisation des processeurs présents sur les cartes graphiques, réputées pouvoir décupler la vitesse des opérations de craquage de mot de passe, demandait jusque-là des étapes techniques qui pouvaient tenir à distance quelques *pirates* manquant de motivation... Du côté des nouveaux formats de fichiers supportés, l'on reconnaîtra les fichiers Office au format Open Document (docx, xlsx, pptx, etc.), le conteneur *keychains* des systèmes Mac OS X, des trames de paquets chiffrées par WPA-PSK (réseaux wifi) ainsi que les bases de données de mots de passe des logiciels Firefox (accès aux sites web) et Thunderbird (codes d'accès aux messageries).
-- http://www.h-online.com/open/news/item/John-the-Ripper-now-able-to-crack-office-files-and-use-GPUs-1631901.html

Microsoft installe Skype "par erreur" sur les stations de travail des entreprises
Une surprise attendait les responsables de parcs informatiques mercredi dernier : le dispositif de déploiement automatique de mises à jours de Microsoft (WSUS) a silencieusement déployé le logiciel Skype sur les postes de travail. Skype a été racheté par Microsoft en octobre dernier et l'annonce avait été reçue avec un certain pessimisme par la communauté, craignant que l'éditeur allait compliquer l'accès au produit. Après avoir intégré l'ajout de publicités affichées lors des sessions vidéo, Microsoft a intégré Skype dans la liste des logiciels automatiquement surveillés par son service WSUS. WSUS était censé déployer Skype uniquement si ce dernier était déjà installé dans la machine...
-- http://social.technet.microsoft.com/Forums/en-GB/winserverwsus/thread/74a93b2b-e820-40ef-a45d-2815b57d164e

Find and call: premier malware disponible sur l'iOS App Store?
L'éditeur de logiciels de sécurité Kaspersky a été notifié ce mercredi de l'existence sur l'iOS App Store d'un logiciel au comportement malveillant: Find and Call. Une fois installée sur un appareil iPhone, le logiciel collecte l'intégralité du carnet de contacts de l'appareil et le dépose sur un serveur. Les données de contact sont ensuite immédiatement réutilisées dans des campagnes de spam, diffusées massivement par SMS. L'on notera qu'il s'agit de la "première fois qu'une telle application est identifiée par le public" mais que l'on ne sait toujours pas si d'autres applications ont déjà été retirées par Apple avant que le public n'ait pu s'en rendre compte...
-- http://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam

Arrêt des relais DNSChanger le 9 juillet: plus de 270'00 systèmes seront privés d'Internet
Pour rappel, des relais DNS avaient été mis en place en novembre dernier, suite à l'intervention du FBI sur une organisation pirate qui avait réussi à infecter plus de 4 millions de machines avec le virus DNSChanger. Lors de leur perquisition, le FBI aurait du retirer les serveurs maîtres du réseau mais une telle action aurait déclenché la déconnexion de plus de 4 millions de machines infectées dans le monde. L'agence avait alors demandé une autorisation de la Cour Fédérale pour remplacer les serveurs pirates par des relais DNS "propres", offrant ainsi une période de "grâce" de six mois aux 4 millions de systèmes infectés. Le FBI arrêtera définitivement les relais DNSChanger le 9 juillet prochain, ce qui déconnectera les 277'000 machines encore infectées par le virus.
-- http://news.discovery.com/tech/dns-changer-fbi-warning-july-9-doomsday-120426.html

2. Décryptage - Le marché noir des failles de sécurité : quels enjeux pour le citoyen ?

Le cycle de diffusion des failles de sécurité serait en pleine mutation et ce serait au détriment total de l'individu et des petites entreprises, si l'on en croit la publication de A.G., journaliste au magazine économique Forbes[1]. Un chercheur en sécurité peut aujourd'hui revendre ses recherches à des prix variant entre 5'000 et 250'000 dollars par faille de sécurité logicielle.

L'on a pu observer ces dernières années une tendance croissante, presque louable, de la part des éditeurs majeurs à établir le contact avec les chercheurs en sécurité afin qu'ils leur communiquent les détails des failles de sécurité qu'ils trouvent dans leurs produits. Ainsi, des éditeurs de produits ou services tels que Facebook, Microsoft, Google, Mozilla, Paypal et Barracuda Networks proposent des programmes de reconnaissance, ou de rétribution financière (*bug bounty program*) destinés à motiver les chercheurs à collaborer avec eux. Ces programmes rétribuent un chercheur lorsqu'il lui communique confidentiellement le détail d'une faille de sécurité. Dans le cas des failles de sévérité maximale (exécution à distance de code arbitraire sans intervention de l'utilisateur), le chercheur peut être rémunéré jusqu'à plusieurs milliers de dollars.

Toutefois, deux modèles viennent concurrencer ces *programmes*. Le premier, particulièrement développé depuis 2007, se concentre sur une poignée de sociétés dont le modèle d'affaire consiste à commercialiser les vulnérabilités sous la forme de binaires opérationnels (attaque "clé-en-main") et à les revendre aux entreprises intéressées. D'un point de vue déontologique, ces entreprises se positionnent en communiquant sur leur mise en place d'une sélection très stricte de leur clientèle ; ceci, dans le but "exprimé" de ne pas voir leurs produits être détournés et réutilisés dans un contexte criminel. Ainsi l'une de ces entreprises, établie en France (le nom est volontairement omis), indique compter exclusivement des autorités judiciaires, des entreprises majeures (Fortune 1000, établissements financiers et entreprises technologiques) et des prestataires de services d'analyse et de conseil en matière de sécurité informatique parmi sa clientèle.

D'autres sociétés proposent un modèle alternatif, beaucoup plus discret et rémunérateur, consistant à se positionner en courtiers d'information entre les chercheurs en sécurité et des organisations dont ils garantissent l'anonymat. Le chercheur en sécurité n'a dès lors aucune idée de qui se cache réellement derrière la transaction : il vend la faille de sécurité à un courtier (qui encaisse bien entendu une commission au passage) qui la revend à son tour à un ou plusieurs organismes. Le maintien du voile entre le chercheur et l'acheteur de ses travaux permet au premier de dormir la tête reposée et la conscience tranquille ; le déni plausible étant de rigueur : "je ne savais pas du tout que cette information allait être réutilisée par X!".

En plus d'être très juteux pour le chercheur (les failles sont rémunérées soit ponctuellement, entre 5'000 et 250'000 dollars, soit sur la base d'une rétribution régulière, tant que la faille n'a pas été découverte publiquement), ce second marché est particulièrement intéressant pour trois catégories bien spécifiques d'acheteurs :

- les gouvernements désireux d'introduire les systèmes citoyens ou ceux d'un autre pays ;
- les entreprises désireuses d'informations stratégiques (concurrence, recherches);
- les organisations criminelles ou mafieuses désireuses d'obtenir des informations pouvant leur servir de levier dans la conduite de leurs opérations.

Ce modèle repose en effet sur la rareté de l'information : tant que la vulnérabilité n'est pas connue de l'éditeur, il est impossible, ou peu probable, que ce dernier la corrige et diffuse une mise à jour, à moins d'avoir éventuellement mis en place un programme robuste de sécurité logicielle. L'acheteur peut ainsi, parfois durant plusieurs années, exploiter cette faille de sécurité sur les systèmes dans lesquels ils souhaite s'introduire.

Lorsque la faille est ciblée sur un produit spécifique et conçu sur mesure pour une entreprise de haute valeur, la rémunération s'envole et peut alors dépasser le million de dollars. A ce stade, il n'est pas difficile d'identifier les cibles les plus évidentes :

- Plateformes d'accès électronique à des institutions bancaires, de gestion ou financières
- Applications d'accès pour tiers/partenaires/fournisseurs dans les entreprises effectuant de la recherche et du développement
- Agences et gouvernements
- Cabinets d'avocats protégeant des personnalités ou gérant des litiges entre entreprises

Quatre groupes qui présentent la particularité commune d'affectionner le déploiement d'applications permettant l'accès à distance à leurs données, généralement accessibles depuis Internet. De plus, ces applications font régulièrement usage de technologies de toute dernière génération dont les enjeux et les aspects sécuritaires ne sont encore que trop rarement maîtrisés par les acteurs impliqués.

Comme indiqué plus haut, ce contexte place l'individu et les entreprises ne pouvant s'offrir les grands moyens pour protéger leurs données, ou les acquérir, au cœur d'une dynamique économique qui leur est particulièrement désavantageuse en tous points. Ainsi les systèmes informatiques présentent des failles de sécurité dont seuls des acteurs disposant à la fois de connexions et d'un poids financier solide peuvent avoir connaissance, et en tirer profit.

Lorsqu'une configuration aussi asymétrique est en œuvre, une intervention de l'Etat (qui, rappelons-le, a pour mission de protéger ses citoyens) semble être la seule issue envisageable. L'Etat dispose en effet de deux outils, pour contrer cette ascension, qu'il est utile de rappeler ici. En premier lieu l'outil législatif. La vente d'informations permettant le contournement de dispositifs de sécurité de systèmes d'information est une infraction pénale dans la grande majorité des payés industrialisés. La Convention européenne sur la cybercriminalité (STE-185), que la Communauté européenne et la Suisse ont ratifié, érige en infractions les actes de diffusion de techniques ou informations utiles au cassage ou contournement de dispositifs de sécurité[2]. L'effort entrepris dans l'application de ces lois n'est pas clairement exposé aux yeux du citoyen.

Le second outil à disposition de l'Etat est le soutien des acteurs locaux. Rares sont les Etats européens qui, aujourd'hui, déploient des moyens concrets pour qu'un effort proactif de lutte contre les aspects de la cybercriminalité cités ci-dessus. Il est difficile d'identifier à ce jour, sur le plan européen ou Suisse, des éléments concrets de motivation ou de sensibilisation qui permettraient, soit, de canaliser l'énergie déployée par des chercheurs en sécurité, à des fins de protection des systèmes informatiques, soit, d'encourager le développement d'outils ou de savoirs ayant pour finalité une meilleure protection des systèmes à l'échelle nationale ou régionale (p.ex.: antivirus maîtrisés localement, relais DNS accessibles aux citoyens, procédures officielles de renforcement de systèmes et services informatiques, etc.). L'approche anglo-saxonne pourrait, sur ce point précis, être une inspiration...

Le débat politique (et ses acteurs les plus proéminents ?) présente les signes d'une *atrophie intellectuelle*. La limite semble en effet avoir été atteinte lorsque l'on constate le temps et l'énergie investis dans trois préoccupations porteuses d'intérêts démagogique (traque du cyberpédophile), sensationnaliste (utilisation d'adolescents comme défouloir pénal et politique dans les cas d'attaques par déni de service) et économique/lobbyiste (lutte contre la contrefaçon entièrement focalisée sur les industries du luxe et de l'audiovisuel). L'enjeu à long terme que peut jouer la cybercriminalité sur l'économie locale (fuite des cerveaux vers l'étranger, vol de connaissances et savoirs stratégiques, sabotages et déstabilisations) ne semble, à première vue, pas encore avoir été compris par nos *élus*.

Devant une telle inertie, il n'est peut-être pas illusoire de penser que la sensibilisation va devoir être effectuée en aval, à savoir par les citoyens, les entrepreneurs et par les chefs d'entreprises. Le refus massif par le Parlement européen, le 4 juillet dernier, du projet de Loi ACTA, pourtant initialement largement soutenu, est un bon exemple de piqûre de rappel que peut provoquer une mobilisation citoyenne et entrepreneuriale [3]...

1: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits
2: http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm
3: http://www.lemonde.fr/technologies/article/2012/07/04/le-parlement-europeen-vote-contre-le-traite-anti-contrefacon-acta_1729032_651865.html

FIN/#012.

DESORMAIS PLUS DE 100 ABONNES A LA LETTRE D'INFORMATION CDDB,
UN GRAND MERCI POUR VOTRE CONFIANCE !

VOTRE PARTICIPATION EST LA BIENVENUE :
> Avez-vous apprécié le format de ce bulletin ?
> Souhaitez-vous qu'un sujet soit traité en particulier?
> Avez-vous des recommandations d'amélioration ou des corrections à communiquer ?
--> écrivez à mailing@cddb.ch ou commentez sur le blog : http://cddb.ch

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 1 à 2 semaines après sa diffusion par email
- Tarif : gratuit
Protection des données:
- Mesures: best effort, liste d'abonnés stockée sur conteneur chiffré, envois en copie carbone
- Conservation: les adresses email et la date d'inscription/désinscription sont conservées
- Diffusion : aucune (sauf cas de force majeure ou *retour de manivelle*)
- Suppression et correction: sur demande, par email à cddb-mailing@nxtg.net
- Tiers: fournisseurs d'accès (pour les bulletins envoyés par courrier électronique)