cddb.ch/Bulletin Cybersécurité et Menaces Internet #011 – 15 juin 2012

Sommaire

1. En vitesse

Mise à jour des machines virtuelles Java: six failles de sévérité critique permettant l'exécution de code arbitraire à distance viennent d'être corrigées[1]. Patch Tuesday de Microsoft du 12 juin dernier: les corrections de sévérité critique sur trois produits de l'éditeur (Remote Desktop, Internet Explorer et .Net Framework) ont été publiées[2]. Internet Explorer reçoit ainsi un patch corrigeant treize failles de sécurité allant jusqu'au niveau critique, il est à noter que sur les treize failles, douze ont été communiquées à l'éditeur sous confidentialité totale[3]. Un quatrième produit, Core XML services, est lui aussi exposé à une faille de niveau critique mais son correctif n'a pas été inclus dans le bulletin de mardi alors que Google annonce qu'il est activement exploité (infections silencieuses par documents Office). Le correctif est disponible séparément[4]. Mise à jour de l'extension Flash d'Adobe, six failles de sécurité de niveau critique ont été corrigées[5].

Google a communiqué les détails de l'exploit qui visait son navigateur web Chrome. Le code coordonne l'exploitation chaînée de 14 failles de sécurité d'importance respectivement moindre pour finalement réaliser le scénario le plus critique (exécution de code arbitraire). Google a offert 60'000 dollars au chercheur Sergei Glazunov en remerciement des détails de la faille[6].

Dans son prochain bulletin (juillet 12), Microsoft inclura un patch pour son dispositif de mise à jour automatique. Windows Update requerra désormais l'établissement d'un tunnel SSL direct vers les serveurs de Microsoft pour télécharger ses mises à jours. Ce changement intervient suite à l'attaque à grande échelle de nombreuses organisations par le virus Flame (sujet traité en détail plus loin) qui reposait sur cette *tolérance* pour se propager dans les autres machines. Cette mise à jour aura un impact immédiat sur les structures faisant inspecter les flux de mises à jours par un proxy à inspection de trafic SSL[7] [ndlr: oui, vous avez bien lu, le protocole SSL peut absolument être filtré silencieusement au sein d'un réseau d'entreprise. --> CDDB#006]

Une vulnérabilité particulièrement spectaculaire publiée ce 9 juin dernier vise le serveur de bases de données MySQL, distribué librement en source ouverte. La faille, qui touche toutes les versions antérieures également, permet de contourner totalement le dispositif de contrôle d'accès en tentant de s'y connecter à répétition avec un mot de passe quelconque (300 tentatives nécessaires en moyenne). La faille présente une caractéristique très pédagogique: elle est révélatrice du danger que présente une utilisation inadéquate des langages de programmation autorisant des conversions implicites de type de données (*implicit cast*)[8][9].

Après l'enseigne La Redoute[10], c'est autour de Les 3 Suisses d'être confronté à une faille de sécurité sur sa plateforme de commandes en ligne. Un code permettant de commander n'importe quel article du catalogue à 50% de son prix affiché a été diffusé sur des forums lundi dernier. Les internautes se sont bien sûr empressés de commander des équipements informatiques à prix cassé. L'enseigne a annoncé mardi, via sa page Facebook, qu'elle n'honorerait pas les commandes. Elle est aujourd'hui suspectée d'avoir mené une opération dissimulée de collecte de données dans le but de renflouer ses bases de données de clients[11].

L'enquête sur les attaques de déni de service qui ont causé plusieurs paralysies du système d'information de l'aéroport international de Séoul[12] avait initialement abouti à... plusieurs dizaines de milliers de joueurs en réseau, citoyens de Corée du Sud. La suite de l'enquête a révélé un scénario tout aussi spectaculaire que le premier: les joueurs avaient acheté un jeu vidéo massivement multi-joueurs dont le support d'installation avait été préalablement infecté par un cheval de Troie par les services de renseignement de Corée du Nord. L'importation des jeux a été réalisée en 2009, par un jeune distributeur de jeux vidéo qui s'était rendu en Chine afin de les importer à prix cassé. Ses interlocuteurs étaient en fait deux agents du renseignement nord-coréen. Le cheval de Troie en opération sur les machines des joueurs aurait été activé par la Corée du Nord à trois reprises durant 2011, bloquant ainsi l'activité de l'aéroport international[13].

1: http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html
2: http://technet.microsoft.com/en-us/security/bulletin/ms12-jun
3: http://technet.microsoft.com/en-us/security/bulletin/ms12-037
4: http://technet.microsoft.com/en-us/security/advisory/2719615
5: http://www.adobe.com/support/security/bulletins/apsb12-14.html
6: http://blog.chromium.org/2012/06/tale-of-two-pwnies-part-2.html
7: http://support.microsoft.com/kb/2720211
8: http://thehackernews.com/2012/06/cve-2012-2122-serious-mysql.html
9: http://bugs.mysql.com/bug.php?id=64884
10: http://www.jeuxvideo.com/forums/1-36-16477914-1-0-1-0--fail-une-erreur-de-prix-sur-la-redoute.htm
11: http://pro.clubic.com/e-commerce/actualite-496226-3-suisses-code-promo-offrait-50-site.html
12: http://threatpost.com/en_us/blogs/report-north-korea-accused-ddos-attack-south-korean-airport-060712
13: http://www.geek.com/articles/news/north-korea-uses-infected-games-to-attack-south-korea-2012068/

2. Flame: état des lieux

Flame, le tout dernier virus ultra cybermenaçant identifié dans les systèmes informatiques de plus de 600 organisations et individus établis ou en lien avec des pays arabes, fait couler beaucoup d'encre sur les réseaux. L'enchaînement des révélations apporte un lot quasi quotidien de surprises. L'on pensera tout premièrement à la composition du programme : un noyau minimaliste chargé d'établir une liaison silencieuse avec le réseau de contrôle/commande. Ce noyau était ensuite complété de modules fonctionnels déployés sur mesure selon l'infrastructure compromise. Pas moins de vingt modules ont été identifiés, presque tous destinés soit à de l'acquisition de renseignements (connecteurs pour des bases de données, analyseurs de documents et de flux, captures d'écran, surveillance par le micro et la caméra de la machine, etc.) soit à de l'exfiltration de données (canaux couverts, liaison avec le centre de commandes, etc.) soit à du traitement de données (recoupement, compression, chiffrement), le tout totalisant presque vingt méga-octets de code[1].

Plusieurs versions de Flame étaient en circulation. Elles communiquaient chacune avec un réseau de plus de quatre-vingt centres de commandes et contrôles répartis mondialement[2]. Ces serveurs ont été progressivement mis en place entre 2008 et 2012 et déployés sous des noms de domaines réservés avec de fausses identités. Chaque identité n'a servi que deux ou trois fois. La Suisse fait partie des pays dans lesquels ces domaines ont été réservés sous ces fausses identités. L'infection était effectuée de façon ponctuelle (pas de propagation non contrôlée), probablement par ingénierie sociale, et l'on suspecte l'exploitation de plusieurs vulnérabilités non publiques présentes au sein de la version 32-bits du système Microsoft Windows ou l'un des programmes fréquemment installés sur ce dernier. L'un des modes d'infection les plus surprenants permettait l'exécution silencieuse du code grâce à une signature électronique utilisant un certificat émis par Microsoft[3]. Le programme s'étend et se maintient à jour grâce à un contrôle du dispositif Windows Update dans lequel les modules injectés ont été eux aussi signés[4] [ndlr : oui, vous avez bien lu]. Flame collecte, analyse et traite en priorité les données se trouvant soit dans des documents de type Word, PDF et AutoCAD (le troisième format étant particulièrement utilisé par l'industrie pour documenter les plans de conception et d'architecture).

Pourquoi avoir utilisé l'imparfait dans de nombreuses phrases ci-dessus ?

Quelques heures seulement après la publication de la première analyse technique par le laboratoire Kaspersky, le réseau de serveurs de commandes/contrôles de Flame a été presque entièrement désactivé. Seuls quelques systèmes sont restés opérationnels afin d'envoyer un ordre de… désinstallation sur tous les systèmes infectés[5]. Moins d'une semaine plus tard (le 3 juin), Microsoft a publié un correctif de sécurité hors cycle (les correctifs ne sont diffusés généralement que le second mardi de chaque mois) rendant caduc le certificat électronique utilisé par Flame pour infecter les machines[6]. Selon Microsoft, les certificats utilisés par le service Terminal Server installé dans tous les systèmes Windows étaient mal configurés et permettaient la signature de binaires. Plusieurs experts adhèrent à la thèse d'un cas de déni plausible : il est impossible de déterminer si Microsoft connaissait l'existence de cette porte d'entrée et si l'éditeur a collaboré avec une organisation ou si cette faille a réellement été découverte par des chercheurs externes à l'éditeur[7] [ndlr: màj.15/06/2012: cette hypothèse est désormais la moins privilégiée suite aux nombreuses actions de Microsoft cette semaine].

Se pose finalement la question de la fiabilité du système Microsoft Windows lui-même pour les non américains ou peut-être les « non alliés. » Malgré la mise en œuvre, il y a un peu plus de dix ans, d'un processus destiné à permettre à l'éditeur de produire un système comportant moins de failles de sécurité[8], les récents événements (Flame, Duqu, Stuxnet pour ne pas les mentionner) révèlent un rôle particulièrement central tenu par des vulnérabilités du système Windows dans la commission d'intrusions informatiques de haut vol, sur des systèmes critiques établis dans les nations arabes.

Il faudra probablement encore quelques années d'ici à ce que les nations, en particulier celles dont l'économie ou la stabilité politique dépendent fortement de la confidentialité de leurs échanges électroniques, prennent conscience qu'elles pourraient devoir chacune concevoir et développer leur propre système d'exploitation... La vraie guerre électronique ne se joue peut-être pas déjà sur la "sécurisation" des systèmes d'information mais sur la sécurisation "sélective" de ces derniers. En d'autres termes: "Ce système est sécurisé, pour moi et mes amis uniquement. "

A méditer!

1: http://news.cnet.com/8301-1009_3-57443975-83/behind-the-flame-malware-spying-on-mideast-computers-faq/
2 : http:// securelist.com/en/blog/208193538/Flame_Bunny_Frog_Munch_and_BeetleJuice
3: http://technet.microsoft.com/en-us/security/advisory/2718704
4 : http://news.cnet.com/8301-10805_3-57446466-75/flame-virus-spread-through-rogue-microsoft-security-certificates
5 : http://www.wired.com/threatlevel/2012/06/flame-command-and-control
6 : https://blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx?Redirected=true
7 : https://www.grc.com/sn/sn-356.txt
8 : http://www.microsoft.com/security/sdl/default.aspx

3. Décryptage : les mots de passe de 6,5 millions d'utilisateurs LinkedIn en circulation

Un fichier contenant les codes d'accès de plus de 6,5 millions d'utilisateurs du réseau socioprofessionnel LinkedIn a été diffusé mercredi sur le forum de discussion d'un site web hébergé en Russie. L'éditeur a rapidement confirmé avoir pris connaissance de la diffusion, via le blog et le flux Twitter officiels. Décryptage des informations diffusées.

6 juin 2012
Il est environ 13h30 (heure locale suisse) lorsqu'apparaît sur le site du CERT finlandais (Computer Emergency Response Team) une brève annonçant la fuite sur Internet de 6,5 millions de codes d'accès d'utilisateurs LinkedIn[1]. L'annonce fait suite à la publication, quelques minutes auparavant, d'un message dans un forum de discussion hébergé en Russie.

Le fichier publié pèse 120 méga-octets et comporte environ 6,46 millions de mots de passe, représentés sous leur forme condensée SHA-1, un algorithme de hachage cryptographique couramment utilisé pour stocker des mots de passe. Il est important de mentionner ici que le fichier diffusé n'inclut pas les noms d'utilisateurs mais uniquement les condensés de mots de passe. N'importe qui peut télécharger le fichier. Dans les bureaux de LinkedIn, situés en Californie, la cellule de crise est activée. Il n'est pas encore cinq heures du matin.

A 14h45 (heure suisse), le portail ZDnet relaye l'information en une de page[2]. Toute la communauté européenne et asiatique est bien réveillée pour relayer l'information par tous les moyens disponibles. La montre affiche 5h45 sur les murs de LinkedIn. 20 minutes plus tard, le premier communiqué officiel fait son apparition sur le flux Twitter de la société[3]. La nature du message est typique d'un dispositif de crise maîtrisé : en moins de 140 caractères, l'entreprise quittance la réception de l'information et annonce le déclenchement d'une investigation. Belle performance, lorsque l'on sait que le même éditeur vient d'essuyer en seulement deux semaines les frondes directes de la communauté sécurité, respectivement pour une faille de sécurité permettant l'interception du mot de passe de l'utilisateur[4] et pour avoir siphonné le contenu des rendez-vous de l'agenda sans mentionner clairement ce qu'il se passait en arrière-plan sur le téléphone de ses utilisateurs[5].

Deux heures plus tard, LinkedIn recommunique : l'investigation continue mais il est impossible de confirmer qu'il s'agit bien de données volées à l'éditeur[6]. Il est 17 heures passée en Europe.

Trois heures passent encore (il est désormais 11 heures chez eux, et 20 heures chez nous) et un communiqué en bonne et due forme est diffusé sur le blog de l'entreprise[7]. Cela s'observe immédiatement : la sémantique spécifique à ce type d'incident est activée, l'éditeur rappelle à chaque coin de phrase à quel point il prend au sérieux la protection des données de ses utilisateurs… Le communiqué se limite à brièvement rappeler les risques liés à la création de comptes sur les sites web et les bonnes pratiques en matière de gestion de mots de passe. Deux éléments n'apparaissent pas : il n'est pas explicitement recommandé au lecteur de modifier son mot de passe (mais le lien est proposé) et l'acte d'intrusion informatique n'est pas confirmé.

C'est à douze heures trente (21h30 en Suisse) qu'un second communiqué fait surface : le lien est cette fois-ci établi entre la nature des codes d'accès se trouvant dans le fichier et des comptes utilisateurs de la plateforme LinkedIn. L'éditeur adopte toutefois un silence total sur le rapport causal de cette diffusion : il ne confirme toujours pas qu'il y a eu une intrusion informatique dans ses systèmes[8], un détail essentiel lorsque l'on connait les nouvelles réglementations du

gendarme boursier américain, la SEC, qui imposent aux entreprises cotées en bourse de lui communiquer officiellement les détails et conséquences d'une intrusion informatique dans leurs systèmes. Le lecteur attentif remarquera que beaucoup de journalistes et bloggeurs se sont abstenus de mentionner l'absence de cette confirmation…

D'un point de vue boursier, l'action LinkedIn a perdu 1% dans les heures suivant l'annonce de la fuite de mots de passe. La baisse s'est manifestée par un volume de transactions cinq fois supérieur à la moyenne de la semaine précédente.

7 juin 2012
Il est 14h45 lorsque l'éditeur diffuse son troisième communiqué sur son blog[9]. Une chronologie des événements est rappelée au lecteur, elle est suivie d'une précision confirmant que LinkedIn met en œuvre un renforcement de sa sécurité [ndlr : nous y reviendrons sous peu]. Le communiqué précise également qu'aucun compte n'aurait été compromis suite à la diffusion du fichier (trad. : personne n'a utilisé le mot de passe du fichier pour s'authentifier sur le compte d'une tierce personne) et qu'une procédure de renouvellement de mot de passe a été automatiquement déclenchée sur tous les comptes dont le mot de passe a été révélé [ndlr : nous y reviendrons plus tard également]. Aucune phrase ne confirme qu'une intrusion a eu lieu. Du point de vue boursier, un important volume de transactions a également été observé, l'action LinkedIn est toutefois remontée de 2%, la faisant par conséquent atteindre un niveau plus élevé que la veille de l'incident…[10]

Toujours le 7, au soir, le CEO de LinkedIn, Jeff Weiner, copie le message Twitter de la société annonçant le troisième communiqué et le recolle sur son flux Twitter[11]. Le CEO ne s'exprimera pas plus sur l'incident.

9 juin 2012
Un quatrième communiqué est diffusé[12]. Là aussi, l'orchestration est parfaite et respecte les règles de communication auxquelles les grandes sociétés américaines nous ont habitué : après 48-72 heures la sémantique peut basculer dans le registre autoritaire. Les excuses et le discours rassurant cèdent ainsi leur place à la rétorsion légale, et l'argument « nous ne pouvons pas donner de détails car nous devons protéger l'investigation » est avancé afin de contrer les accusations nombreuses de manque de transparence sur l'origine du vol. S'ensuivent des « le FBI investigue sur l'incident », « cet acte de nature criminelle est pris très au sérieux », et « tous les efforts sont déployés pour une recherche agressive des coupables de ce crime».

Le message se termine par un dégagement partiel de responsabilité : LinkedIn annonce que la mauvaise pratique de gestion des mots de passe [ndlr : nous y reviendrons plus tard] avait été identifiée grâce à une équipe « hors pair d'experts de classe mondiale en sécurité de l'information », recrutée en partie déjà en 2010. Le problème a été corrigé et les bases de données ont été mises à jour déjà bien avant que l'incident ne survienne.

Quelle faute technique est reprochée à LinkedIn et pour quelle raison ?
L'élément le plus flagrant apparaissant sur Internet est le reproche lié au stockage des mots de passe. LinkedIn a en effet stocké les mots de passe de plus de 65 millions d'utilisateurs sous une forme reconnue par la communauté comme insuffisante, à savoir sous la forme d'un condensé SHA-1 non salé (la gestion des mots de passe est d'ailleurs l'un des rares domaines aujourd'hui où l'on recommande l'utilisation de sel sans modération !)

Pour le lecteur non technique, les notions de condensé, ou hachage, et de sel correspondent à des transformations cryptographiques d'une donnée. L'analogie la plus simpliste est de comparer ce traitement au mécanisme du hachoir d'un boucher : il est impossible de reconstituer l'original d'un steak haché et seul le steak original peut produire exactement un steak haché donné. Le problème que nous avons aujourd'hui dans l'informatique, si l'on poursuit l'analogie du steak haché, est que des pirates ont entrepris de cataloguer la grande majorité des viandes bovines, sous différentes formes et tailles, et le résultat de leur hachage. Ainsi, lorsqu'ils goûtent un steak haché, ils n'ont qu'à regarder dans leur catalogue pour retrouver à quel steak original correspond un steak haché.

Afin de rendre la procédure de retour en arrière plus difficile, on recommande aux « bouchers » « d'épicer » leur viande, afin de donner au steak haché un « gout » unique. LinkedIn a « haché » les mots de passe, mais a omis de leur rajouter du « sel ». Les pirates sont ainsi ralentis, mais juste un peu, car ils disposent de catalogues (bases de données) et n'ont qu'à les parcourir pour retrouver le mot de passe original. La conséquence immédiate de ce manquement est la grande facilité avec laquelle il est possible de revenir au mot de passe original.

François Pesce, ingénieur auprès de l'éditeur Qualys, a publié les résultats de sa cryptanalyse de la liste des mots de passe de LinkedIn[13]. En laissant tourner durant quatre heures un outil gratuit automatisant l'opération de cassage de mots de passe, il a pu retrouver la forme originale de plus de 900'000 mots de passe. En reconduisant l'opération plusieurs fois, avec un ordinateur relativement dépassé, Pesce a cassé près de 2 millions d'entrées. C'est plus de 30% de l'échantillon original cassé en une journée et avec des moyens domestiques !

La méthode n'est pourtant pas inconnue de la communauté. La fondation OWASP publie un standard d'évaluation de sécurité logicielle (ASVS)[14] recensant la liste des contrôles à mettre en œuvre au sein d'une application pour accroître sa robustesse contre les attaques. La recommandation d'utiliser un condensé agrémenté de sel s'y trouve (clé 2.13) depuis la version publiée en 2008.

Quelle est l'étendue et la gravité de l'incident ?
Premièrement, le fichier contient 6,5 millions de mots de passe. Bien qu'il ne représente que 4% du nombre de comptes actifs annoncés par LinkedIn (150 millions en février dernier), l'on est tenu de penser au paradoxe des anniversaires. Ce paradoxe postule en effet qu'il suffit en moyenne de réunir 57 personnes dans une même pièce pour qu'il y ait 99% de chances que deux personnes soient nées le même jour. Par extension, il est tout à fait probable qu'une base de 6,46 millions de mots de passe soit représentative des mots de passe choisis par 150 millions de personnes.

Deuxièmement, le fichier diffusé aux internautes ne contient pas les noms d'utilisateur associés à chaque mot de passe, ce qui en réduit ainsi la valeur. Toutefois, l'on ne sait pas si un second fichier, contenant les associations utilisateur/mot de passe, existe. L'on ne sait pas non plus, le cas échéant, qui aurait accès à ce fichier.

Troisièmement, la date de diffusion du fichier est connue mais pas celle de la liste s'y trouvant : le vol a pu avoir lieu il y a plusieurs jours, semaines, voire mois. Bien qu'il soit facile de tomber dans le piège d'une association rapide, cette information n'a pas encore été corrélée publiquement avec certitude [ndlr : à notre connaissance, la liste aurait une ancienneté d'une année] et l'ancienneté exacte de la liste est encore à déterminer. Reste à évaluer l'assiduité avec

laquelle les utilisateurs suivent les deux recommandations majeures, à savoir, changer leur mot de passe régulièrement et ne pas le réutiliser sur plusieurs plateformes…

Quatrièmement, plusieurs experts estiment qu'obtenir l'accès à un compte LinkedIn n'a pas de grande valeur[15]. Il n'est pas mentionné si l'évaluation tient compte du risque de fuite d'informations stratégiques ou confidentielles stockées dans les messages échangés entre utilisateurs ainsi que du risque de désinformation/réputation si des CV appartenant à des profils de haut niveau sont modifiés de manière suffisamment subtile pour que cela ne se remarque pas facilement.

Cinquièmement, la diffusion de la liste pourrait n'être qu'un petit élément d'information en comparaison de ce qui a réellement été obtenu à travers ce vol (cf. quatrième observation).

Finalement, et c'est l'élément absent des communications de LinkedIn : la liste a-t-elle été volée grâce à une intrusion informatique ou a-t-elle été obtenue par d'autres moyens (vente par un collaborateur, piratage d'un partenaire ou prestataire de services, etc.) ?

Ces circonstances rappellent légèrement le cas de l'intrusion auprès de l'éditeur RSA, révélée au public en mars 2011 : il est impossible pour les utilisateurs de LinkedIn d'évaluer la gravité de ce vol sur des bases factuelles, dans l'attente que d'autres révélations ne fassent surface.

Quelles opportunités cet incident présente-t-il?
Au premier abord et sans données supplémentaires, les conséquences pour l'utilisateur et leur employeur sont moindres. La médiatisation de l'incident présente toutefois un grand avantage : elle fait office de piqûre de rappel à deux catégories d'entreprises : celles qui n'auraient pas encore mis en place un processus de stockage de mots de passe digne des bonnes pratiques actuelles, et celles qui n'ont absolument aucune idée de la façon dont les mots de passe de leurs applications sont stockés.

Du point de vue de la communauté d'experts et de sociétés œuvrant dans la sécurité logicielle, le cas LinkedIn a lui aussi fait office de piqûre de rappel et ramené à la réflexion quant à la réelle efficacité des recommandations souvent promulguées en matière de stockage de mots de passe. Ainsi, en moins de 72 heures, plusieurs dizaines d'articles ont été publiés sur la façon dont les mots de passe doivent être enregistrés dans une base de données. Ces articles reflètent pour la majorité un changement de position survenu peu après l'aube du 6 juin, rendant dès lors caduques de nombreuses prescriptions jusque-là en vigueur. A bon entendeur.

1 : https://www.cert.fi/tietoturvanyt/2012/06/ttn201206061430.html
2 : https://www.zdnet.com/blog/btl/646-million-linkedin-passwords-leaked-online/79290
3 : https://twitter.com/LinkedIn/status/210356987576324096
4: http://securityaffairs.co/wordpress/5572/hacking/linkedin-vulnerability-in-the-authentication-process-and-related-risks.html
5: http://danhon.com/2012/06/06/a-possible-usage-for-the-linkedin-plaintext-calendar-vulnerability/
6 : https://twitter.com/LinkedIn/status/210390233076875264
7 : http://blog.linkedin.com/2012/06/06/updating-your-password-on-linkedin-and-other-account-security-best-practices/
8 : http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/
9 : http://blog.linkedin.com/2012/06/07/taking-steps-to-protect-our-members/
10 : https://www.google.com/finance?q=linkedin

11: https://twitter.com/jeffweiner/status/210871742191771648
12 : http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/
13 : https://community.qualys.com/blogs/securitylabs/2012/06/08/lessons-learned-from-cracking-2-million-linkedin-passwords
14 : https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
15 : http://media.grc.com/sn/sn-356-lq.mp3

4. Décryptage : pourquoi IBM bannirait-il l'usage de Dropbox, Siri et consorts?

IBM a confirmé par voie de presse avoir mis en place une politique de restriction logicielle sur les terminaux mobiles de ses collaborateurs. Les restrictions concernent, entre autres, l'application de reconnaissance vocale pour iPhone Siri, et les applications de sauvegarde et partage de fichiers telles que Dropbox. La décision fait suite au constat d'un manque accru de sensibilité de la part des collaborateurs, pourtant censés s'engager dans la protection des données de leur employeur lorsqu'ils demandent à pouvoir utiliser leur téléphone personnel pour se connecter aux services de l'entreprise.

Pour faire plaisir aux technophiles avant-gardistes
En 2010, IBM faisait figure de leader en appliquant la politique « BYOD », *bring your own device*, une politique permettant aux collaborateurs d'accéder aux services internes de la société depuis leur téléphone portable personnel. Une décision se traduisant, entre autres, par une économie d'achat de près de 80'000 terminaux si l'on en croit le nombre d'employés ayant accepté de se plier aux règles du jeu pour bénéficier de l'accès[1]. Toutefois, un récent audit conduit auprès des collaborateurs a révélé un niveau de sensibilisation largement inférieur aux attentes du programme BYOD.

L'autorisation d'utiliser un terminal personnel au sein d'IBM n'est pas sans conditions. Le collaborateur doit en effet accepter une charte d'utilisation des ressources informatiques à partir d'un équipement personnel et son téléphone doit être remis au personnel IT pour approbation. Le collaborateur est ensuite intégré à l'un ou plusieurs des douze profils d'utilisation définis, chacun de ces profils autorisant l'accès à des services spécifiques. Le collaborateur d'un département peut ainsi n'avoir accès qu'à sa messagerie alors que son voisin aurait accès à tous ses documents de travail. Dans la majorité des cas, l'élément clé de la politique de restriction est le téléphone : un appareil récent, dans lequel il est possible d'installer les applications d'accès sécurisé au réseau d'entreprise tout en permettant une configuration renforcée (tunnel VPN, mot de passe complexe, verrou automatique, chiffrement des mémoires, et désolidarisation de l'appareil à distance), bénéficiera plus facilement de privilèges d'accès.

La procédure a tout récemment été renforcée avec la mise en œuvre de restrictions logicielles portant sur des applications pourtant très appréciées des utilisateurs. L'exemple relayé par la presse concerne en particulier les applications permettant le partage et stockage de fichiers (*Dropbox* et consorts) à distance (*cloud storage*), sans oublier le cas plus anecdotique de l'application de reconnaissance vocale *Siri*, présente dans les terminaux de type iPhone.

Comprendre la motivation d'une interdiction d'installer des applications de stockage à distance de fichiers peut sembler assez trivial : l'on chercherait à réduire le risque de fuite de documents, par distraction, par erreur, ou pire, par faux sentiment de sécurité. La sensibilisation des collaborateurs pourrait suffire à lui donner une envergure acceptable mais… il reste le problème de la fiabilité de l'outil lui-même…

Partage et stockage de fichiers sur le cloud : quid des promesses de sécurité ?
Les applications de stockage de fichiers sont sujettes à un engouement croissant tant auprès des particuliers que des entreprises. A titre d'exemple, l'application Dropbox, automatisant le stockage de fichiers sur des environnements cloud tout en facilitant leur synchronisation sur diverses machines, est aujourd'hui active sur plus de 250 millions de systèmes[2] ! Tout comme

de nombreux magazines proposent à leurs lecteurs d'incroyables techniques d'amincissement pour l'été à venir, les revues technologiques ne manquent pas de vanter une offre proposant 'miraculeusement' le stockage à distance de plusieurs dizaines de giga-octets de données. La Suisse n'est pas en reste, l'offre s'étend jusqu'aux fournisseurs d'accès Internet, qui proposent leur solution de stockage virtuel. Le tout, bien entendu, en toute sécurité et très souvent, gratuitement ! Malheureusement, des analyses couvrant les enjeux ou motivations menant à une profusion soudaine de ces offres, ou leur réel niveau de sécurité offert, restent beaucoup plus difficiles à trouver. Rappelons-le tout de même, un enfant de 9 ans est aujourd'hui le potentiel auteur d'une application mobile installée sur plus d'un million de téléphones[3]!

Avec la disponibilité accrue, l'argumentaire cryptographique constitue le pilier du discours sécuritaire des fournisseurs de services de stockage de fichiers. Ces derniers le traduisent généralement en deux garanties : le transfert et le stockage des données sous forme chiffrée. L'utilisateur sensible aux problématiques induites par l'usage de la cryptographie cherchera, en vain, des réponses à d'autres éléments de risque pourtant dévastateurs pour un système cryptographique :

- Quels algorithmes de chiffrement ont-ils été choisis par l'éditeur ? Quelle configuration avec quelle implémentation ?
- Comment l'entropie des clés de chiffrement est-elle garantie ?
- Quel rôle le secret (mot de passe de l'utilisateur) joue-t-il dans le système de stockage ? Le mot de passe est-il la clé de chiffrement ? Est-il utilisé pour la construire ou donne-t-il accès à cette dernière ?
- Combien de versions des clés de chiffrement sont créées, où sont-elles disséminées et comment leur accès en est-il respectivement protégé ?
- L'éditeur a-t-il déployé, intentionnellement ou non, une autorité de séquestre (une infrastructure lui permettant lui aussi de lire les données en cas de force majeure) ? Si oui, pour quelle raison ? Le confort du client est-il la seule motivation ou est-ce dans le but de remettre les données à un gouvernement en cas de demande d'entraide judiciaire ?
- Un collaborateur indélicat travaillant pour l'éditeur ou l'un de ses partenaires est-il en mesure de lire les données des clients ?
- L'éditeur est-il soumis à une contrainte légale lui intimant de conserver une copie des clés de chiffrement, par exemple en raison de la localisation géographique de son siège social ou des données ?
- Les suppressions et rotations des clés de chiffrement sont-elles cascadées sur les archives et les sauvegardes des données des clients ?
- Etc.

On le devine à la lecture de cette liste : la simple annonce d'un service proposant le chiffrement intégral du transport et du stockage des données laisse une porte ouverte à de nombreuses voies d'erreur et de confusion.

Quid du blocage de l'assistant vocal ?

La décision d'IBM de bloquer la fonctionnalité d'assistance vocale 'Siri', présente dans les terminaux de type iPhone, peut laisser les décideurs un peu plus dubitatifs. Y-a-t'il un risque avéré ? Deux éléments semblent répondre: la fiche de spécification technique du téléphone et ses conditions d'utilisation, que tout détenteur est censé avoir lu, compris et approuvé avant de pouvoir en faire usage...

Non, le téléphone portable ne fait pas de la reconnaissance vocale…
La reconnaissance vocale est une technologie particulièrement gourmande en ressources informatiques. Contrairement à ce que la publicité pourrait nous laisser croire, les téléphones placés en main des utilisateurs sont rarement capables d'effectuer la totalité des calculs nécessaires à la reconnaissance vocale en un temps acceptable pour l'utilisateur. D'un autre côté, des éditeurs comme Apple ou Google disposent à ce jour d'une immense puissance de calcul sur leurs serveurs. L'astuce est donc simplissime : l'éditeur solutionne la puissance limitée du téléphone portable en faisant appel à son atout : sa connectivité. Lorsqu'une interrogation vocale a lieu, le téléphone compresse puis transmet l'enregistrement à un centre de traitement. Ce dernier va effectuer les opérations d'analyse, de traitement et de recherche pour finalement retourner la liste de résultats au téléphone. Tout cela va vite. L'utilisateur ne s'en rend pas compte et reste absolument ravi de son investissement.

D'un point de vue strictement technique, il est crucial de retenir ici qu'Apple, au travers de la fonctionnalité Siri, n'est absolument pas plus reprochable que ses concurrents. Le système de reconnaissance vocale installé dans les terminaux Android, par exemple, fonctionne exactement selon le même procédé. Les techniciens de la gestion du risque identifieront qu'il s'agit essentiellement d'une décision relative à l'engouement plus marqué des utilisateurs iPhone pour la reconnaissance vocale.

Le second aspect sensible réside dans les termes d'utilisation. En effet, ces derniers mentionnent explicitement [ndlr : la phrase est d'ailleurs rédigée en gras] que l'utilisateur « *accepte et convient qu'Apple et ses filiales et agents transmettent, recueillent, conservent, traitent et utilisent ces informations, y compris les entrées vocales et les Données utilisateur, pour offrir et améliorer Siri, la Dictée et d'autres produits et services Apple* ». La phrase suivante mentionne que l'envoi de la localisation géographique de l'utilisateur sera également communiquée à Apple lorsque l'assistant vocal Siri est interrogé[4]. Un message clair, sans équivoque, et dont il serait difficile de se décharger d'une éventuelle responsabilité en cas d'incident de sécurité.

Sans éléments supplémentaires, IBM aurait simplement lu et intégré cette information dans une logique de gestion de risque : en utilisant la fonctionnalité Siri, que ce soit volontairement ou par erreur, les collaborateurs mettraient à disposition d'Apple diverses informations telles que leurs déplacements, leurs interrogations de l'assistant et d'autres données qui lui sont typiquement transmises. IBM est démuni : aucune garantie légale, contractuelle ou technologique ne rassure quant au risque de corrélation de données entre plusieurs utilisateurs, de transmission à des partenaires ou de communication à des gouvernements en cas de sollicitation juridique.

Pour conclure.
Une réflexion *réciproque* pourrait être tout aussi intéressante à investiguer : d'autres organisations tablent aujourd'hui sur une politique du « téléphone d'entreprise », permettant ainsi un contrôle étendu de l'appareil par le service informatique. Dans ces cas, le risque est-il réellement amoindri lorsque l'on sait que les collaborateurs vont résolument compenser les restrictions de leur téléphone professionnel par une utilisation accrue de leur appareil personnel, souvent encore plus sophistiqué, de l'autre poche du veston ?

Dans l'état actuel des informations publiées, difficile de qualifier la décision d'IBM d'exemple à suivre ou de coup de tête.

Une chose est certaine toutefois: la problématique de la fuite des données via des applications installées par le collaborateur sur son terminal mobile s'inscrit dans la liste des risques à gérer. En particulier, lorsque la publication de photos, de coordonnées GPS et/ou "d'observations" publiées sur des réseaux publics pourrait avoir des conséquences sur la compétitivité de l'entreprise, ou ses engagements auprès de ses clients…

1 : http://www.technologyreview.com/business/40324/
2 : http://en.wikipedia.org/wiki/Dropbox_(service)
3 : https://en.wikipedia.org/wiki/Lim_Ding_Wen
4 : http://images.apple.com/legal/sla/docs/ios51.pdf

5. Quelques ressources à télécharger ou consulter

42 bonnes pratiques pour protéger des applications iOS et Android contre des attaques
https://viaforensics.com/resources/reports/best-practices-ios-android-secure-mobile-development/
Développement pour iOS : comprendre les mécanismes de protection intégrés à l'iPhone
http://cocoamanifest.net/linked/2012/05/ios-application-insecurity.html
Guide de renforcement de la configuration des terminaux mobiles iOS (NSA)
http://www.nsa.gov/ia/_files/os/applemac/Apple_iOS_5_Guide.pdf

FIN/#011.

BIENTOT 100 ABONNES! VOTRE PARTICIPATION EST LA BIENVENUE:
> Avez-vous apprécié le format de ce bulletin ?
> Souhaitez-vous qu'un sujet particulier soit traité ?
> 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
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)