

cddb.ch/Bulletin Cybersécurité et Menaces sur Internet #002 – 16 novembre 2011

Sommaire

1. Chevaux de Troie: à disposition de la police cantonale vaudoise?	1
2. Sécurité logicielle: regards tournés sur la Suisse romande durant deux jours	1
3. Fuites de données personnelles: une faille technique et/ou humaine?.....	2
4. Duqu: un outil de renseignement au service de Stuxnet?.....	3
5. Surveillance des télécommunications: la police londonienne...aussi!	4
6. Le distributeur de contenu en ligne Steam piraté: 40 millions d'enregistrements volés.....	5
7. Analyse : autorités de certification, la confiance est-elle ébranlée ?.....	5
8. En Bref.....	7

1. Chevaux de Troie: à disposition de la police cantonale vaudoise?

Selon le journal Le Matin, la police cantonale vaudoise aurait utilisé un cheval de Troie dans au moins une affaire de pédophilie et compte étendre son utilisation aux *smartphones*.

Le journal Le Matin annonçait jeudi dernier l'existence d'une collaboration au sein du canton de Vaud, entre la police et la Haute Ecole d'ingénierie et de gestion (HEIG-VD) ainsi que l'école des sciences criminelles de l'Université de Lausanne.

Le canton de Vaud a ainsi reconnu avoir utilisé un cheval de Troie dans le but de faciliter l'arrestation d'un pédophile [1]. L'objectif est d'étendre le périmètre d'intervention de l'outil aux *smartphones* et accéder à leurs données de géolocalisation, messages et appels téléphoniques. Selon le journal, des sondes pour les systèmes mobiles Symbian (appareils Nokia) et Android (multimarques) sont déjà au stade de prototypes. Le système iOS, équipant les appareils de type iPhone, est le prochain sur la liste[2].

L'école a également été mandatée pour la réalisation d'une sonde d'interception de signaux d'appels émis sur le réseau GSM. La sonde se positionne en relais (par opposition à un positionnement en écoute passive) et enregistrerait le numéro IMSI (*International Mobile Subscriber Identity*) associé à la puce SIM lors d'un appel émis depuis la zone d'interception[3].

1: <http://www.lematin.ch/flashinfo/suisse/alliance-entre-la-police-et-les-hautes-ecoles-sur-les-technologies-2011-11-03>

2: <http://www.ictjournal.ch/fr-CH/News/2011/11/04/Logiciels-de-surveillance-collaboration-entre-la-police-vaudoise-collabore-et-la-HEIG-VD.aspx>

3: <http://www.lematin.ch/actu/suisse/la-police-veut-infiltrer-les-smartphones-2011-11-02>

2. Sécurité logicielle: regards tournés sur la Suisse romande durant deux jours

Plus d'une centaine de professionnels des TIC étaient réunis les 26 et 27 octobre à Yverdon-les-Bains à l'occasion de l'*Application Security Forum - Western Switzerland*, un forum 100% dédié à la sécurité logicielle.

La Haute école d'ingénierie et de gestion du canton de Vaud a accueilli la seconde édition du Forum romand de la sécurité logicielle, qui s'est tenu les 26 et 27 octobre derniers[1]. Une population, majoritairement composée de développeurs, architectes, chefs de projets et décideurs au sein de plus de 80 organisations et entreprises romandes, a pris part à cette nouvelle formule divisée en une journée "technique" (formations et ateliers pratiques) et une journée de conférences. Un programme d'interventions d'experts régionaux et internationaux venus s'exprimer sur les thèmes forts de la sécurité logicielle (authentification forte et identité numérique, développement sécurisé, applications mobiles, logiciels d'infrastructures critiques, cryptographie, etc.) a été conçu pour l'occasion.

Les organisateurs n'ont pas manqué de clore la manifestation en annonçant le démarrage imminent des préparatifs et des réflexions du concept *Application Security Forum* pour l'année 2012.

Les absents de cette année n'ont pas été oubliés: les conférenciers ont accepté de rendre les supports de leur intervention disponibles à la consultation en ligne et au téléchargement [2].

1: <http://event.appsec-forum.ch>

2: <http://slideshare.net/asf-ws>

3. Fuites de données personnelles: une faille technique et/ou humaine?

Des chercheurs de l'université de British Columbia (Canada) ont éprouvé l'efficacité du mécanisme de protection des données personnelles de Facebook. En quelques jours, près de 60% des utilisateurs de l'échantillon ont autorisé une personne totalement fictive au sein de leur cercle "privé".

Pour réaliser leur étude[1], les chercheurs se sont inspirés du modèle "zombie/maître", très prisé des propriétaires de réseaux de machines infectées par des chevaux de Troie. Cette approche leur a ainsi permis de constituer un échantillon de 102 profils de personnes totalement fictives sur le réseau Facebook, publiant aléatoirement des statuts, eux-mêmes inspirés de citations de célébrités.

Les chercheurs ont élaboré une première vague de demandes d'amitié à plus de 5'000 membres du réseau Facebook qui avaient au préalable rendu leur profil inaccessible aux inconnus. En six jours, plus de 19% des sondés ont accepté la demande d'amitié et ainsi rendu leur profil accessible aux chercheurs. Sur cette base ainsi constituée, les chercheurs ont finalement pu créer un lien d'amitié avec plus de 3'000 membres, faisant jouer la carte du "nous avons des amis communs".

L'accès à près de 60% de l'échantillon de profils initialement "protégés" a rendu possible l'extraction à large échelle sur plus d'un million de profils (amis d'amis), résultant en une collecte de plus de 250 giga-octets de données personnelles dont 500'000 dates d'anniversaire, 50'000 adresses vérifiées de messagerie électronique et 14'500 adresses postales.

Suite à la publication des résultats, plusieurs journaux[2][3] ont attribué la responsabilité de la faille de sécurité au réseau social lui-même, par opposition à ses utilisateurs...

- 1: http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf
- 2: http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=10764441
- 3: <http://www.cbc.ca/news/technology/story/2011/11/07/technology-facebook-socialbots.html>

4. Duqu: un outil de renseignement au service de Stuxnet?

Le virus Duqu, dont les premières analyses techniques révèlent l'existence de similitudes avec le ver Stuxnet, infiltre les systèmes Windows grâce à un exploit de type 0-day embarqué dans des documents Word.

18 octobre au matin, des experts de la société Symantec annoncent[1] avoir collaboré avec une équipe indépendante de sécurité établie en Hongrie (CrySys)[2] sur l'étude d'un nouveau *malware* montrant les signes d'un niveau de sophistication supérieur à la normale. L'élément est alors baptisé Duqu, un nom tiré du préfixe des noms de fichiers qu'il crée.

La rétro-ingénierie de l'exécutable révèle rapidement l'existence de nombreux éléments, près de la moitié[3], repris du code source de Stuxnet; ce qui laisserait penser que soit les créateurs sont identiques, soit le code source de Stuxnet est en vente/distribution sur les marchés sous-jacents.

L'infection de la machine est facilitée par la présence de binaires signés par des autorités de certification approuvées au sein de la PKI actuellement en œuvre dans les systèmes Windows. Tout comme dans le cas de Stuxnet, le piratage informatique de l'autorité de certification n'est pas la première hypothèse mais plutôt une intrusion physique au sein même de l'organisation pour entreprendre la signature du code[4].

Duqu se différencie tout particulièrement de Stuxnet par sa charge offensive (*payload*), visant non pas à déstabiliser des systèmes industriels mais plutôt à offrir à son "maître" un canal de contrôle et commande à distance (RAT) particulièrement robuste et furtif pour des missions d'exfiltration de données et documents.

Duqu exfiltre les données au moyen d'un canal à la fois chiffré et dissimulé au sein d'images JPEG, rendant plus difficile l'identification des données volées. Duqu n'est pas doté de routines d'auto-propagation mais est programmé pour se supprimer de lui-même, et effacer toute trace de son passage, 36 jours après son activation au sein d'une machine.

L'objectif est clairement identifié: là où Stuxnet est aujourd'hui assimilé à la première arme aboutie de guerre électronique destinée à saboter et provoquer des dommages physiques au moyen d'une propagation entièrement autonome, Duqu est à l'inverse assimilé à un dispositif furtif de reconnaissance et de renseignement, dont le choix des cibles relèverait d'une approche chirurgicale (attaque sociale sur la cible visée) plutôt que d'une propagation automatisée à large échelle[5].

Jusqu'à présent identifié comme un objet inclus dans un document Word, la simple ouverture du fichier déclenche l'infection de la machine et aucune intervention supplémentaire par l'utilisateur n'est requise (confirmation, alertes ou autre). Un serveur maître de contrôle/commande a été identifié en Belgique, mais l'éditeur Kaspersky n'exclut pas que plusieurs réseaux soient à l'œuvre[6].

L'éditeur Microsoft a confirmé être en train de constituer un correctif pour ses systèmes. Les organisations désireuses de protéger leurs systèmes les plus exposés (ordinateurs portables, postes de travail) peuvent déjà appliquer une procédure de contournement dans l'attente du correctif officiel [7].

- 1: http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet
- 2: <http://www.crysys.hu/>
- 3: <http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/231902150/what-is-duqu-up-to.html>
- 4: <http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/231901080/researchers-precursor-to-son-of-stuxnet-spotted-in-the-wild.html>
- 5 : <http://www.spiegel.de/international/world/0,1518,778912,00.html>
- 6: http://www.securelist.com/en/blog/208193206/The_Mystery_of_Duqu_Part_Three
- 7: <http://technet.microsoft.com/en-us/security/advisory/2639658>

5. Surveillance des télécommunications: la police londonienne...aussi!

La police londonienne aurait récemment acquis un logiciel permettant l'interception de signaux GSM, afin de faciliter l'identification et la localisation de personnes utilisant un terminal mobile dans une zone surveillée.

Information révélée au public par le journal The Guardian[1], annonçant l'acquisition récente par la police londonienne d'un équipement d'interception de télécommunications mobiles. Le dispositif, se réduisant à la taille d'une valise transportable contrôlée à distance, est capable de simuler la présence d'une cellule GSM "prioritaire" sur un rayon d'environ une dizaine de kilomètres carrés.

L'appareil intercepte les signaux d'appels et messages, et enregistre le numéro IMSI (pas besoin de décrire ces initiales à nouveau, cela a été cité quelques lignes plus haut...) de la carte SIM utilisée dans le téléphone. Le système est également doté de fonctionnalités de positionnement par triangulation, permettant ainsi de suivre les déplacements d'une personne donnée dans le rayon d'interception.

Le dispositif matériel coûte environ 200'000 francs suisses (hors services). Le journal n'a pas réussi à savoir si le dispositif fonctionne en impasse (appels/messages n'aboutissant pas) ou en relais (l'utilisateur ne se rend pas compte que la communication est surveillée, voire enregistrée). La police londonienne avait déjà fait l'acquisition en 2010 d'un logiciel permettant de géolocaliser les citoyens à travers la surveillance automatisée des réseaux sociaux[2].

- 1: <http://www.guardian.co.uk/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance>
- 2: <http://www.guardian.co.uk/uk/2011/may/11/police-software-maps-digital-movements>

[note]

Le Royaume-Uni fait office de cas d'école dans le débat sur la légitimité d'initiatives de surveillance de télécommunications, et leurs potentielles dérives sur la protection de la sphère privée. L'on notera que le pays se caractérise (contrairement à la Suisse) par l'absence d'une constitution formelle spécifiant les droits de ses citoyens. Difficile de déterminer quel texte

prime sur l'autre lorsqu'il s'agit de confronter la protection des données personnelles au maintien de la sécurité du territoire.

6. Le distributeur de contenu en ligne Steam piraté: 40 millions d'enregistrements volés

Le distributeur de contenu en ligne Steam, particulièrement réputé dans le secteur de la distribution en ligne de jeux vidéos, a confirmé avoir été victime d'une intrusion informatique. Les comptes de 40 millions d'utilisateurs ont été exfiltrés.

Valve Corporation, propriétaire de la plate-forme de distribution Steam a confirmé le 10 novembre dernier avoir été victime d'une intrusion dans son système d'information. Le piratage des forums de discussion était soupçonné en premier lieu mais les investigations ont rapidement permis d'identifier que l'intrusion s'est étendue sur d'autres systèmes, dont la base de données hébergeant les profils des clients et leurs données financières.

Le vol de la base de données n'a pas été confirmé. Elle est composée de 40 millions d'enregistrements, incluant noms d'utilisateurs, mots de passes (sous forme hachée/salée), historique d'achats, adresse email, coordonnées postales, et données de carte de crédit (sous forme chiffrée).

Selon le Directeur de la plate-forme, aucune utilisation frauduleuse des données de crédit n'a encore été identifiée. Il est toutefois recommandé aux 40 millions d'utilisateurs de « surveiller scrupuleusement les relevés de leur carte de crédit » et de changer leur mot de passe, en particulier s'il est réutilisé sur d'autres plateformes.

7. Analyse : autorités de certification, la confiance est-elle ébranlée ?

Un fournisseur malaysien de certificats numériques destinés à équiper les services SSL/TLS a été compromis. Cela porte à quatre le nombre d'autorités de certification ayant confirmé avoir été compromises cette année.

Contexte

Un fichier PDF intrusif particulièrement intéressant est actuellement en circulation sur les réseaux et a été repéré par les analystes de l'éditeur F-Secure[1]. Le fichier est doté d'un agent de téléchargement, s'exécutant après l'exploitation d'une vulnérabilité présente dans le programme Adobe Reader en version 8. Une fois téléchargé, le binaire infectant est exécuté sur la machine. L'exécution se faisait en silence (le certificat a expiré en septembre), en raison de la présence d'une signature électronique reconnue comme valide.

La certification de binaires

L'élément le plus intéressant réside dans le certificat électronique dont est doté le binaire. Certaines organisations font en effet l'effort (soulignons-le !) d'acquérir un certificat électronique destiné à la signature de binaires (*code signing certificate*). Cette catégorie de certificats électroniques permet aux partenaires ou clients d'une organisation (généralement, les éditeurs de logiciels) de s'assurer que l'origine d'un binaire qu'elle distribue est connue et certifiée. Cette procédure offre deux avantages majeurs: l'exécution du binaire signé est rendue possible sur les systèmes configurés pour exiger cette mesure, et l'intégrité du binaire est garantie entre l'instant où il a été signé et celui où il est exécuté sur un système de production[2].

Des signatures réellement authentiques ?

Le certificat joint au binaire est identifié comme appartenant au gouvernement malaysien et est signé de l'autorité de certification Digisign Server Id (DigiCert Sdn.Bhd), elle aussi établie en Malaisie. Cette autorité a la particularité d'être un sous-signataire autorisé par Entrust, qui n'est autre que l'une des cinq autorités majeures de certification mondialement approuvées sur la quasi-totalité des systèmes informatiques (CAcert, Entrust, GlobalSign, Microsoft et Verisign)[3].

La certification du binaire est possible selon quatre hypothèses:

- Le gouvernement malaisien a signé l'exécutable intrusif (corruption ? intrusion ?)
- Le certificat du gouvernement malaisien a été volé (idem)
- Un tiers a réussi à forger le certificat (voir ci-après)
- Un tiers a réussi à faire signer un certificat au nom du gouvernement malaisien, directement auprès de l'autorité de certification (voir ci-après)

Forgerie du certificat, possible....mais

Bien que les deux premières hypothèses restent les plus probables, il est intéressant de ne pas négliger la troisième (forgerie du certificat). La forgerie est en effet théoriquement possible dès lors que l'on dispose soit de suffisamment de puissance de calcul (force-brute) soit d'une énorme chance (il est important de ne jamais oublier que même une signature authentifiée sur une base RSA de 4096 bits peut être découverte en 3 millisecondes par un *smartphone* si l'on est extrêmement chanceux).

En excluant la chance de notre scénario, il reste la force brute. Tout le monde s'attend à une résistance théorique moyenne de 1024 ou 2048 bits imposée par l'autorité de certification (à juste titre)...mais un observateur de l'actualité aura remarqué que la révocation mondialement déployée sur les systèmes Windows ce 10 novembre dernier avait pour objectif de révoquer une autorité de certification (établie en...Malaisie) qui signait des certificats avec une clé de...512 bits [4]. L'on pourrait penser qu'il s'agit d'une « petite autorité de certification locale » mais il n'en est rien : Digisign Server ID est une autorité directement subsidiaire de...Entrust. Traduction : il était au début de ce mois encore possible de laisser circuler des exécutables signés par une clé de 512 bits et reconnus comme hautement certifiés par la majorité des systèmes informatiques actuellement en production[5].

Compromission de l'autorité ?

Ce cas ajoute une nouvelle pierre à l'édifice d'autorités de certification majeures compromises sur l'année 2011, telles que Diginotar, Comodo et KPN (qui a tout récemment découvert que son réseau était compromis depuis près de 4 ans [6]). Le cas Digisign Server Id reste encore flou, dans la mesure où l'on ne sait pas si l'organisation ne mettait pas en œuvre de bonnes pratiques de sécurité (qui vérifiait ?) ou si leur dispositif de configuration des certifications a été compromis afin d'abaisser la résistance cryptographique des certificats émis pour les tiers (l'investigation est-elle en cours et/ou possible ?).

La confiance : pilier du mécanisme « SSL »

Plusieurs gouvernements, dont la Suisse, ont franchi le pas d'accorder la valeur légale à la signature électronique pour authentifier les transactions impliquant des organisations ou des citoyens. Toutefois, ce modèle repose encore en grande partie sur une confiance, parfois aveugle, accordée aux autorités de certification nativement reconnues par les systèmes d'exploitation et navigateurs web majoritairement présents sur le marché.

Dès lors, quelles opportunités sont-elles disponibles aujourd'hui pour les organisations désireuses de s'assurer que les infrastructures à clés publiques peuvent être exploitées en toute confiance ?

- 1 : <http://www.f-secure.com/weblog/archives/00002269.html>
- 2 : <http://msdn.microsoft.com/en-us/library/ms537361%28v=vs.85%29.aspx>
- 3 : http://en.wikipedia.org/wiki/Root_certificate
- 4 : <http://technet.microsoft.com/en-us/security/advisory/2641690>
- 5 : <http://www.entrust.net/advisories/malaysia.htm>
- 6 : <http://www.computing.co.uk/ctg/news/2123198/-hack-raises-ssl-alarm>

8. En Bref

Facebook : plusieurs millions de comptes ont été infectés par un « *virus* » diffusant des contenus à caractère pornographique dans les profils[1]. L'attaque « self-XSS » (l'utilisateur copie-colle lui-même le script offensif dans la barre d'adresse du navigateur) aura peut-être finalement son moment de gloire...

- 1 : http://www.cbsnews.com/8301-205_162-57325428/facebook-yes-we-have-a-porn-problem/

Censure et contrôle du web: moins d'une semaine après avoir été contraint par la Cour britannique de filtrer les requêtes adressées au service de téléchargement de fichiers Newsbin2, l'opérateur British Telecom a été *sollicité* par la BPI (un lobby pour la défense des intérêts des distributeurs de musique) pour appliquer la même mesure au site The Pirate Bay[1].

- 1 : <http://www.telegraph.co.uk/technology/broadband/8869645/Record-labels-demand-BT-blocks-access-to-the-Pirate-Bay.html>

FIN/#002.

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> une semaine après sa diffusion par email
- Tarif: gratuit

Protection des données personnelles:

- Mesures de protection: best effort + liste d'abonnés stockée sur fichier local chiffré
- Données conservées: adresse email + date d'inscription/désinscription uniquement
- Diffusion des données: aucune (sauf cas de force majeure ou incroyable distraction)
- Destruction des données: sur demande, par email à cddb-mailing@nxtg.net
- Tierces parties connues: fournisseur d'accès (messagerie SMTP pour l'envoi des bulletins)