

## cddb.ch/Bulletin Cybersécurité et Menaces sur Internet #004 – 16 décembre 2011

### **Sommaire**

1. Second drone perdu : l'hypothèse d'une cyberattaque mise en doute .....1
2. Imprimantes d'entreprise vulnérables: action en recours collectif contre HP.....2
3. Cloud Computing: les centres de données européens seraient soumis au Patriot Act.....3
4. Analyse - Phonedog contre N. Kravitz : « Ce compte Twitter m'appartient! ».....4
5. En Bref.....5

### **1. Second drone perdu : l'hypothèse d'une cyberattaque mise en doute**

Plusieurs éléments laissent supposer que la récente capture du drone américain par l'Iran serait le résultat d'une attaque électronique. La perte d'un second drone, ce mercredi, dans les Seychelles, met cependant en doute les capacités de cyberguerre auxquelles prétendrait l'armée iranienne.

La capture probable d'un drone d'exploration appartenant à la CIA a été annoncée le 4 décembre dernier par l'armée iranienne[1]. Le RQ-170 constitue l'un des éléments technologiques les plus sophistiqués actuellement utilisés par la CIA pour le survol des zones de conflit, combinant en particulier un système électronique de reconnaissance/exploration, des systèmes d'interception de données, de détecteurs d'activité nucléaire et une conception rendant l'appareil globalement furtif, donc invisible aux yeux des radars ennemis[2].

Deux hypothèses sont principalement émises quant aux conditions de la perte du drone : une avarie technique/électronique aurait pu causer une rupture du lien de communication ou induit la chute de l'avion. Alternativement, l'observation des dégâts particulièrement légers sur l'appareil, si le contenu de la vidéo est réel[3], impliquerait que le drone a été capturé suite à une intrusion électronique alors qu'il se trouvait encore en vol. Bien qu'il soit particulièrement surprenant que l'engin ne semble pas doté de fonctions d'autodestruction en cas de capture, cette hypothèse confirmerait dès lors les capacités offensives de cyberguerre revendiquées à plusieurs reprises par l'armée iranienne [4][5].

Le scénario de la cyberattaque a été remis en question ce mardi lorsqu'un second drone, similaire à celui capturé en Iran, s'est écrasé dans l'océan indien [6]. Bien entendu, ce second incident pourrait indiquer l'existence d'une avarie ou dysfonctionnement sérieux dans les modèles de type RQ-170. [ndlr : l'incident pourrait aussi être interprété comme une manœuvre de désinformation orchestrée par la CIA...]

De son côté, le gouvernement iranien a annoncé vouloir mettre en œuvre tous les efforts nécessaires, y compris la collaboration avec des nations ennemies des Etats-Unis, pour effectuer la rétro-ingénierie (*reverse engineering*) de l'appareil et pouvoir en lancer une production à l'échelle industrielle [7].

Finalement, les observateurs plus attentifs remarqueront également que le drone RQ-170 est sorti des laboratoires de recherche du concepteur-constructeur avionique Lockheed Martin[8]. L'on se rappellera ici de l'intrusion survenue en mars dernier dans le réseau de l'éditeur de solutions d'authentification forte RSA [9] et dont les données volées avaient permis aux pirates de s'introduire trois mois plus tard dans le réseau informatique de Lockheed Martin. Le constructeur avait déclaré qu'aucun document de conception de ses appareils de défense n'avait été volé[10].

1 : <http://www.presstv.ir/detail/214542.html>

2 : [https://secure.wikimedia.org/wikipedia/en/wiki/United\\_States%27\\_RQ-170\\_capture\\_by\\_Iran](https://secure.wikimedia.org/wikipedia/en/wiki/United_States%27_RQ-170_capture_by_Iran)

3 : <http://www.bbc.co.uk/news/world-middle-east-16098562>

4 : <http://www.airforcetimes.com/news/2011/12/defense-iran-captured-rq-170-how-bad-120911/>

5 : [http://www.cbsnews.com/8301-503543\\_162-57339407-503543/iran-shows-intact-drone-boasts-of-cyberattack/](http://www.cbsnews.com/8301-503543_162-57339407-503543/iran-shows-intact-drone-boasts-of-cyberattack/)

6 : <http://www.nationalturk.com/en/another-us-drone-crash-iran-cyber-war-on-us-drones-started-15440>

7 : [http://latimesblogs.latimes.com/world\\_now/2011/12/iran-us-spy-drone.html](http://latimesblogs.latimes.com/world_now/2011/12/iran-us-spy-drone.html)

8 : [http://en.wikipedia.org/wiki/Lockheed\\_Martin\\_RQ-170\\_Sentinel](http://en.wikipedia.org/wiki/Lockheed_Martin_RQ-170_Sentinel)

9 : <http://www.engadget.com/2011/03/18/rsa-hacked-data-exposed-that-could-reduce-the-effectiveness-o/>

10 :

<http://www.dailytech.com/Reports+Hackers+Use+Stolen+RSA+Information+to+Hack+Lockheed+Martin/article21757.htm>

## **2. Imprimantes d'entreprise vulnérables: action en recours collectif contre HP**

Des chercheurs de l'université de Columbia ont révélé la présence d'une fonction de mise à jour à distance activée par défaut dans la majorité des imprimantes de la marque HP déployées dans les entreprises. Cette faille les exposerait à des attaques informatiques et, fait surprenant, à un risque accru d'incendie.

L'entreprise HP, mondialement réputée pour ses équipements informatiques, est actuellement exposée à une plainte en recours collectif (*class action*), qui l'accuse d'avoir négligé la sécurité de ses clients en activant par défaut la fonction de mise à jour à distance sans authentification dans ses imprimantes[1]. Correctement exploitée, cette faille permettrait non seulement l'exécution de programmes d'intrusion depuis une imprimante mais, selon les chercheurs, permettrait également la mise à feu de cette dernière[2].

Le cas a été révélé suite aux travaux de recherche de deux étudiants de la faculté de sciences informatiques à l'université de Columbia (New York)[3]. En lançant un balayage aléatoire sur Internet, les chercheurs ont identifié plus de 40'000 imprimantes vulnérables, joignables à distance, depuis l'extérieur de leur réseau.

Une plainte en recours collectif pour négligence a été déposée contre HP[4]. L'entreprise a publié un bulletin de sécurité informant sur la procédure à appliquer pour désactiver la fonction de mise à jour à distance[5].

1 : [http://redtape.msnbc.msn.com/\\_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say](http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say)

2 : <http://www.wired.com/threatlevel/2011/11/hp-printer-hack/all/1>

3 : <http://www.wired.com/wiredenterprise/2011/12/hp-printer-lawsuit/>

4 : <http://docs.google.com/gview?url=http://docs.justia.com/cases/federal/district-courts/california/candce/5:2011cv05779/248220/1/0.pdf?1322863230>

5 : [https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr\\_na-c03102449&ac.admitted=1323904302007.876444892.199480143](https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03102449&ac.admitted=1323904302007.876444892.199480143)

### 3. Cloud Computing: les centres de données européens seraient soumis au Patriot Act

Considérée comme l'une des lois les plus intrusives en matière de télécommunications, le Patriot Act, originalement conçu pour la lutte contre le terrorisme, exposerait les données de certains centres de données destinés à des services en nuagerie (*cloud computing*) commercialement présentés à la clientèle comme « strictement européens. »

Le texte de Loi Patriot Act, voté par l'administration Bush en octobre 2011 juste après les attentats terroristes du 11 septembre la même année, étend les libertés d'action déjà octroyées par le FISA (*Foreign Intelligence Surveillance Act*) dès 1978 en autorisant les services de renseignement à détenir une personne, ou des données, soupçonnées d'être impliquées dans un projet de nature à exposer la sécurité du territoire, sans qu'inculpation ne soit prononcée au préalable et à l'échelle internationale[1]. Sur le territoire européen, la mise en œuvre du Patriot Act peut ainsi constituer une atteinte directe aux dispositions prévues par la directive sur la protection des données 95/46/EC[2].

Cette situation expose tout particulièrement les projets d'externalisation de services vers des infrastructures de type SaaS (*software as a service* ou *cloud computing*). Dans la mesure où ces services induisent fréquemment la mise à disposition physique de données de l'entreprise, ou de la personne, à un tiers, le propriétaire des données peut se retrouver être la cible d'une acquisition de données sans qu'aucune communication ne lui soit adressée. Le cas BAE fait figure de cas d'école depuis ce 7 décembre dernier, lorsque le constructeur de systèmes militaires aériens a publiquement annoncé exclure l'offre d'hébergement de services de messagerie proposée par Microsoft (Office 365) pour des motifs liés au Patriot Act[3].

L'éditeur Microsoft avait déjà clairement annoncé lors du lancement de sa suite de services en nuagerie destinés aux entreprises en juin dernier, que "aucune entreprise proposant des services d'hébergement de données ne peut garantir être exclue du champ d'action du Patriot Act"[4]. Bien sûr, les données personnelles ne sont pas le seul souci des entreprises considérant le service externalisé: les données médicales patient (*patient health information*) et les données financières sont elles aussi exposées au risque de traitement par des agences américaines.

1 : [https://secure.wikimedia.org/wikipedia/en/wiki/USA\\_PATRIOT\\_Act](https://secure.wikimedia.org/wikipedia/en/wiki/USA_PATRIOT_Act)

2:

[http://europa.eu/legislation\\_summaries/information\\_society/data\\_protection/l14012\\_en.htm](http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm)

3: <http://www.computerweekly.com/blogs/it-fud-blog/2011/12/bae-systems-office365.html>

4: <http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225>

#### 4. Analyse - Phonedog contre N. Kravitz : « Ce compte Twitter m'appartient! »

Californie - Un conflit oppose actuellement Noah Kravitz, expert réputé pour ses analyses technologiques, à son ex-employeur, Phonedog ; ce dernier lui ayant demandé de restituer les codes d'accès au compte Twitter de l'entreprise, comptant plus de 17'000 abonnés, ainsi qu'une réparation pour pertes causées à hauteur de 340'000 dollars.

Le modèle d'affaires de la société *Phonedog Media* (Phonedog), basée en Californie (mais siégeant dans le Delaware), est constitué des revenus générés grâce au trafic de son site web d'actualité technologique [www.phonedog.com](http://www.phonedog.com). Ce dernier attire plus de 2,5 millions de visiteurs uniques, par mois[1].

En octobre 2010, et après quatre années de collaboration, l'éditeur en chef de Phonedog, *Noah Kravitz* (N.K.), annonce son départ. Il rejoindra moins de deux mois plus tard l'éditeur TechnoBuffalo, société dont le modèle d'affaires est en de nombreux points similaires à celui de Phonedog (édition de contenus d'actualité technologique).

Durant sa collaboration avec Phonedog, N.K. a créé un compte sur le service de messages courts « Twitter », qu'il a intitulé « @phonedog\_noah » et au travers duquel il a pu régulièrement interagir avec plus de 17'000 abonnés. Le jour de son départ de la société, un mot d'adieu fut publié sur le site web. N.K.[2]. Dans ce billet, N.K. fait explicitement mention de son compte Twitter, intitulé « @noahkravitz » et invite le lecteur à s'y connecter pour suivre la suite de ses aventures. Le compte Twitter « @noahkravitz » était en réalité le compte « @phonedog\_noah », dont N.K. était le seul à détenir les codes d'accès et qu'il venait tout juste de renommer[3].

Le conflit entre les deux parties, aujourd'hui escaladé devant les tribunaux, se fonde sur la propriété du compte Twitter. N.K. affirme que ce compte a été alimenté durant plusieurs années au travers d'un lien personnel avec les abonnés (le service Twitter permettant également d'échanger des messages privés entre les membres) et qu'il n'a pas été officiellement revendiqué autrement que par l'intermédiaire de la plainte. De l'autre côté, l'éditeur revendique une stratégie marketing qui visait à associer sur Twitter la marque Phonedog tout en mettant en valeur chacun de ses rédacteurs (@phonedog\_prenom)[4]. En quittant l'entreprise, N.K. aurait donc du remettre les « clés » à son employeur.

Dans sa plainte, Phonedog réclame le montant de 340'000 dollars à titre de dommages, en plus de la restitution du compte. Ce montant a été déterminé sur la base du nombre d'abonnés au compte (17'000) et des estimations de cabinets indépendants, valorisant un abonné Twitter pour un compte entreprise à environ 2,50 dollars/mois. La plainte a été déposée huit mois après le départ du collaborateur.

L'affaire est en cours, la décision du Juge pourra être consultée sur le site web de la Cour de Californie[5]. D'ici-là, il peut être utile aux sociétés mettant en œuvre une présence sur les réseaux sociaux, tout comme aux collaborateurs gérant ces identités, de formaliser/contractualiser certains aspects de la relation, tels que:

- Le propriétaire du compte et des contenus
- Les règles d'usage du compte à des fins personnelles
- Les procédures à suivre en cas de départ du collaborateur
- La gestion des codes d'accès et des adresses associées à la récupération du compte
- La responsabilité engagée, ou non, des propos émis au travers du compte

Dans le cas de l'affaire opposant N.K. à son ancien employeur, la formalisation des éléments ci-dessus aurait probablement permis aux deux parties d'éviter le dépôt d'une plainte.

1 : [http://blogs.computerworld.com/19279/who\\_owns\\_your\\_twitter\\_account\\_your\\_employer](http://blogs.computerworld.com/19279/who_owns_your_twitter_account_your_employer)

2 : <http://www.phonedog.com/2010/10/18/noah-s-farewell-post/>

3 : <http://venturebeat.com/2011/11/11/phonedog-v-kravitz/>

4 :

[http://blogs.computerworld.com/19292/phonedog\\_hits\\_back\\_re\\_noahkravitz\\_twitter\\_lawsuit](http://blogs.computerworld.com/19292/phonedog_hits_back_re_noahkravitz_twitter_lawsuit)

5: <http://apps.alameda.courts.ca.gov/domainweb/html/index.html> (# de cas: RG11579535)

## 5. En Bref

---

### **Autorités de certification : une de plus.**

Pays-Bas - L'autorité de certification Gemnet, basé aux Pays-Bas, aurait subi une intrusion informatique mercredi dernier (7.12). Gemnet est le fournisseur principal de certificats électroniques pour plusieurs agences du gouvernement, telles que les ministères de la Justice et Sécurité, la police ainsi que la banque centrale du pays. Les pirates auraient exploité l'absence d'un mot de passe sur le portail d'administration des bases de données (via le logiciel phpMyAdmin) pour s'introduire dans les systèmes. Selon un communiqué officiel de la société KPN (propriétaire de Gemnet), les systèmes de l'infrastructure destinée à la signature électronique n'ont pas été touchés par l'intrusion.

-- [http://www.scmagazineuk.com/dutch-certificate-authority-reportedly-hacked-after-access-gained-through-php-myadmin/article/218672/?DCMP=EMC-SCUK\\_Newswire](http://www.scmagazineuk.com/dutch-certificate-authority-reportedly-hacked-after-access-gained-through-php-myadmin/article/218672/?DCMP=EMC-SCUK_Newswire)

### **Autorités de certification: la PKI de GlobalSign sort indemne de l'attaque de septembre**

Belgique - L'autorité de certification GlobalSign, basée en Belgique, avait subi une attaque informatique dans ses systèmes durant le mois de septembre 2011. L'entreprise a rendu publics les détails de l'investigation qui s'est terminée récemment. L'on y lit, entre autres, que l'activité cœur (production de certificats) a été interrompue durant 9 jours suite à l'identification de l'incident de sécurité. L'entreprise annonce également avoir entrepris une séparation physique et logique de ses activités critiques, à savoir: serveurs web, système de paiement électronique, services CRM, systèmes de délivrance de certificats et systèmes de gestion des certificats racine.

--

<http://www.darkreading.com/authentication/167901072/security/news/232300600/global-sign-certificate-infrastructure-untouched-in-hack.html>

### **Chevaux de Troie pour mobiles : l'arnaque « SMS Premium »**

Russie - Des analystes auprès de l'éditeur F-Secure ont identifié deux applications à vocation malveillante, s'installant sur les terminaux téléphoniques Android. L'application est cataloguée sous la forme d'un jeu de hasard et inclut une fonctionnalité cachée de type « SMS-Premium. » Après installation, le logiciel débute, en tâche de fond, l'envoi régulier de SMS à destination de numéros surtaxés localisés à l'étranger. Un observateur attentif des permissions demandées lors de l'installation (autorisation d'envoyer des SMS) pourrait éventuellement déceler la fraude. Selon les analystes, les utilisateurs géolocalisés en Russie semblent être les premières cibles visées par les pirates.

-- <http://www.f-secure.com/weblog/archives/00002278.html>

### **Revente d'informations personnelles : 200\$ par profil**

États-Unis – Un homme et une femme, respectivement âgés de 28 et 31 ans, et travaillant au service des automobiles de l'état du New Jersey, ont été inculpés pour corruption, recel et vol d'identité. Les deux collaborateurs constituaient des fichiers d'usagers (nom, adresse, date de naissance et numéro de sécurité sociale) qu'ils revendaient en moyenne 200 dollars/identité. Ils encourent chacun jusqu'à dix années d'emprisonnement. Les informations concernant le réseau d'acheteurs et l'utilisation des identités n'ont pas été communiquées à la presse.

-- <http://arstechnica.com/tech-policy/news/2011/11/government-employees-accused-of-selling-identities-for-200-a-pop.ars>

### **Adobe Flash: un exploit 0-day disponible à la vente**

Russie - La société de sécurité InteVyDis, basée en Russie, vend depuis un peu plus d'une semaine deux exploits pour l'extension Adobe Flash. Les deux exploits sont opérationnel et permettent ainsi l'exécution de code arbitraire sur des systèmes de type Windows 7 ou XP contenant un navigateur Firefox, Internet Explorer ou Chrome, même lorsque tous ces logiciels sont maintenus à jour (pour l'instant). Les exploits sont en vente à une clientèle intéressée. InteVyDis, dont le Directeur avait publiquement annoncé ne plus vouloir communiquer gratuitement les résultats de leurs recherches aux éditeurs. La simple consultation d'un site web sur lequel est déployé l'un de ces deux exploits déclenche l'exécution de code sur la machine de l'internaute, sans que ce dernier n'en soit informé.

-- <http://www.infoworld.com/d/security/two-zero-day-vulnerabilities-found-in-flash-player-181344>

### **Adobe PDF Reader: exploit 0-day utilisé contre une société de Défense**

États-Unis – Une société de Défense travaillant essentiellement pour le gouvernement américain a été la cible d'une attaque informatique utilisant une faille de sécurité non identifiée sur le logiciel Adobe PDF Reader. Les pirates ont fait parvenir des fichiers PDF aux collaborateurs de la société, ces fichiers étaient équipés d'un cheval de Troie s'installant en fond après l'exploitation d'une vulnérabilité encore non identifiée le 16 décembre dernier.

[ndlr: on notera, une fois encore, que la vulnérabilité se situe dans le moteur de traitement Javascript intégré dans Adobe Reader. Ce vecteur quasi-exclusivement utilisé par les pirates depuis 2006 et est encore couramment maintenu activé dans les environnements professionnels.]

-- <http://www.gmanetwork.com/news/story/241912/scitech/technology/new-adobe-based-cyberattack-targets-defense-contractor>

### **Patch Tuesday: Microsoft corrige 17 failles de sécurité, et en laisse une de côté**

L'éditeur Microsoft a publié ce mardi 13 mises à jours corrigeant pas moins de 17 failles de sécurité dans ses logiciels Windows, Internet Explorer, Office et Media Player. On notera deux éléments importants. 1. La présence du correctif extrêmement attendu contre l'exploit Duqu. Duqu avait notamment permis en novembre dernier à des pirates d'introduire un cheval de Troie dans les systèmes de plusieurs fournisseurs de services et équipements utilisés dans le cadre d'activités d'enrichissement nucléaire. 2. L'absence du correctif destiné à prémunir les systèmes contre l'attaque BEAST (interception de flux sécurisés SSL). Bien que ce correctif existe, il a été retiré en dernière minute de la mise à jour automatique car il pouvait provoquer des incompatibilités avec les produits de SAP [ndlr: ...].

--

[http://www.computerworld.com/s/article/9222639/Microsoft\\_scratches\\_BEAST\\_patch\\_at\\_last\\_minute\\_but\\_fixes\\_Duqu\\_bug?taxonomyId=85](http://www.computerworld.com/s/article/9222639/Microsoft_scratches_BEAST_patch_at_last_minute_but_fixes_Duqu_bug?taxonomyId=85)

**L'Indonésie souhaiterait interdire les services dédiés aux téléphones BlackBerry**

L'autorité indonésienne de régulation des télécommunications a annoncé jeudi dernier considérer l'interdiction d'accès aux services BBM (messagerie instantanée) et BIM (autres services Internet) sur le territoire indonésien. Cette décision fait suite à l'annonce du constructeur RIM de vouloir placer ses serveurs et centres de données "Asie du sud-est" à Singapour. L'Indonésie souhaite que ces centres soient déployés sur son territoire, invoquant des motifs de sécurité. Toutes les données arrivant dans des terminaux Blackberry transitent actuellement par le Canada et le gouvernement indonésien ne peut pas surveiller ce trafic.

-- <http://www.thejakartapost.com/news/2011/12/09/govt-threatens-end-blackberry-messenger-service.html>

FIN/#004.

Conditions et tarifs:

- Inscription : envoyer un email avec sujet "inscription texte" ou "inscription pdf" à [cddb-mailing@nxtg.net](mailto:cddb-mailing@nxtg.net)
- Désinscription: envoyer un email avec sujet "désinscription" à [cddb-unmailing@nxtg.net](mailto: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](mailto:cddb-mailing@nxtg.net)
- Tierces parties connues: fournisseur d'accès (messagerie SMTP pour l'envoi des bulletins)