

cddb.ch/Bulletin Cybersécurité et Menaces sur Internet #003 – 7 décembre 2011

Sommaire

| | |
|---|---|
| 1. Incident SCADA : une pompe à eau détruite suite à une cyberattaque..... | 1 |
| 2. Incident SCADA (suite): un pirate confirme la faible protection des infrastructures..... | 2 |
| 3. Incident SCADA (suite et fin): finalement, il n'y a pas eu de cyberattaque !..... | 2 |
| 4. Surveillance des téléco: iTunes aurait facilité l'installation de mouchards durant 3 ans | 3 |
| 5. [Analyse] Carrier IQ : un logiciel « espion » dans 142 millions de téléphones portables | 4 |
| 6. En Bref..... | 8 |

1. Incident SCADA : une pompe à eau détruite suite à une cyberattaque

Springfield (Illinois, E.U.) / Le centre de contrôle des services de distribution d'eau de la ville de Springfield aurait, selon un expert proche des responsables, été compromis par des pirates informatiques. Le piratage aurait résulté en la destruction d'une pompe hydraulique.

Selon un expert en sécurité réputé pour son expérience dans la sécurité des infrastructures critiques (systèmes « SCADA »), le centre de commande et supervision de la centrale hydraulique de Springfield aurait identifié la compromission de ses systèmes au début du mois de Novembre[1]. Selon les traces constatées, l'intrusion aurait toutefois eu lieu plusieurs mois auparavant, sans que les pirates n'en fassent un usage particulier.

Les éléments d'authentification utilisés pour franchir les contrôles d'accès indiquent que les pirates avaient connaissance d'informations jusque-là uniquement connues du constructeur des équipements. Selon l'expert, le scénario le plus probable est que le réseau du constructeur a lui-même été piraté au préalable et les pirates ont obtenu des détails permettant d'accéder aux systèmes de ses clients. [cf. sujet Duqu, #002]

Les opérateurs avaient remarqué des comportements suspects sur l'infrastructure durant les deux mois précédant l'incident, en particulier des redémarrages imprévus des pompes hydrauliques. C'est ce comportement qui aurait causé la destruction de la pompe.

Les premiers suspects seraient des pirates opérant depuis la Russie, pays duquel les attaques auraient été initiées selon les traces trouvées dans les systèmes.

L'incident a été confirmé conjointement par le FBI et le DHS (sécurité intérieure). Toutefois, toujours selon les deux agences, aucun élément ne permet de conclure sur l'existence d'un lien causal entre la cyberattaque et la panne [2]. L'expert maintient cependant son hypothèse [3].

1: <http://community.controlglobal.com/content/water-system-hack-system-broken>

2 : <http://www.techspot.com/news/46317-hackers-destroy-pump-at-us-water-utility-plant.html>

3 : <http://www.techspot.com/news/46407-fbi-says-hackers-not-responsible-for-illinois-water-pump-failure.html>

2. Incident SCADA (suite): un pirate confirme la faible protection des infrastructures

Springfield (Illinois, E.U.) / Le département de la sécurité intérieure (DHS) et le FBI ont démenti l'existence d'un risque particulier suite à l'incident survenu en novembre dans une centrale de distribution d'eau. Le présumé pirate d'une autre infrastructure similaire s'est alors exprimé publiquement, dénonçant les *propos rassurants* des autorités devant un risque qu'il estime lui aussi bien plus élevé qu'il n'y paraît.

Comme indiqué précédemment, le DHS (département de la sécurité intérieure) ainsi que le FBI ont officiellement communiqué l'absence d'éléments corroborant la thèse de l'acte de *cybervandalisme*. Cette annonce faisait suite à la destruction d'une pompe hydraulique d'un distributeur d'eau dans l'Etat d'Illinois (E.U.) début novembre, dont le système d'information se trouvait être aux mains de pirates informatiques[1].

Moins de 24 heures après la publication de l'annonce par les journaux, un internaute se présentant sous le pseudonyme *prof* a revendiqué l'attaque d'une autre infrastructure similaire située dans l'Etat du Texas[2], présentant divers éléments de preuve (captures d'écran et données) afin d'appuyer ses dires[3].

Le pirate a entre autres précisé que les systèmes de contrôle et supervision dont il avait pris le contrôle étaient protégés par des mots de passes se limitant à trois caractères alphabétiques, tout en étant joignables depuis Internet. Une approche que toute bonne pratique ou référentiel de sécurité condamnerait aujourd'hui sans hésitation...

prof a également mentionné le manque de coordination et l'erreur de jugement dont les autorités semblent avoir fait preuve suite à l'incident de Springfield. Les Etats-Unis disposent en effet de plusieurs services dédiés aux infrastructures critiques lorsqu'un incident de sécurité est identifié ou suspecté : ICS-CERT (*Industrial Control Systems*)[4], Water ISAC (*Information Sharing and Analysis Center - Water*)[5], Multi-state ISAC (inter-états)[6], EPA (*Environmental Protection Agency*)[7], DHS, FBI, ...

1 : http://www.theregister.co.uk/2011/11/17/water_utility_hacked

2 : http://threatpost.com/en_us/blogs/hacker-claims-he-breached-texas-water-plant-111911

3 : <http://pastebin.com/Wx90LLum>

4 : <http://www.ics-cert.org>

5 : <https://portal.waterisac.org>

6 : <http://msisac.cisecurity.org>

7 : <http://www.epa.gov>

3. Incident SCADA (suite et fin): finalement, il n'y a pas eu de cyberattaque !

Le département de la sécurité intérieure a clos l'incident relatif à la destruction matérielle survenue mi-novembre dans une centrale d'approvisionnement hydraulique : le trafic provenant de Russie était celui d'un collaborateur travaillant à distance !

Le département de la sécurité intérieure (DHS) a clos ses dossiers relatifs à la récente cyberattaque d'une centrale d'approvisionnement hydraulique, qui aurait conduit à la destruction d'une pompe à eau. Les conclusions de l'investigation mentionnent qu'aucun élément factuel ne permet d'établir un quelconque lien entre une intrusion informatique et la panne matérielle survenue[1].

En revanche, l'investigation d'un incident relayé à l'échelle mondiale par la presse technologique a toutefois permis d'apporter la lumière sur les faits impliquant l'éventuelle existence de pirates informatiques russes, voire d'espions du gouvernement. L'enquête a en effet révélé que la société en charge de l'exploitation de la centrale hydraulique fait appel à un cabinet de consultants spécialisés dans les systèmes de contrôle et supervision d'infrastructures sensibles. Suite à une urgence survenue plusieurs mois auparavant, un consultant intervenant régulièrement sur ces systèmes avait été amené à s'y connecter à distance. La première fois, depuis l'Allemagne. Et la seconde fois, lorsqu'il se trouvait en vacances avec sa femme et ses enfants... en Russie[2].

Le cas est actuellement traité avec un peu d'humour quelque peu caustique [3] mais l'on ne manquera pas d'observer que, malgré une connaissance plus qu'éprouvée en matière de sécurité des technologies de l'information, des infrastructures pouvant présenter un danger immédiat pour la population sont aujourd'hui encore connectées sur des réseaux utilisés par n'importe quel internaute...

[*ndlr* : En plus d'avoir révélé des incompétences et de nombreux dysfonctionnements de communication entre les acteurs chargés de gérer l'incident, l'affaire a également mis en lumière la quête exacerbée d'un sensationnalisme dénué de toute vérification professionnelle dans le domaine de la sécurité de l'information. Une quête à laquelle semblent joyeusement s'adonner tant des professionnels de la sécurité que les autorités, ou encore les journalistes. Les intérêts de chacun étant particulièrement simples à identifier, il sera probablement difficile de freiner cette tendance. Sur ce sujet, lire l'analyse en fin de ce bulletin.]

1 : <http://www.pcmag.com/article2/0,2817,2396835,00.asp>

2 : <http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved/>

3 : <http://www.engadget.com/2011/12/01/man-on-vacation-confused-for-a-russian-spy-almost-restarts-cold/>

4. Surveillance des téléco: iTunes aurait facilité l'installation de mouchards durant 3 ans

Une récente mise à jour du logiciel iTunes de Apple a interpellé plusieurs chercheurs en sécurité. Cette mise à jour colmate en effet une faille de sécurité qui avait été annoncée à l'éditeur en juin 2008. Selon des informations relayées au Wallstreet Journal, des sociétés ont régulièrement exploité cette négligence de Apple, dont on ne sait si elle est volontaire ou non, comme vecteur pour introduire leurs mouchards dans les ordinateurs de citoyens.

Le 28 octobre 2011, Apple a annoncé la disponibilité d'une nouvelle version de son logiciel iTunes à ses utilisateurs. Une faille de sécurité y a été corrigée[1]. L'observateur attentif aura remarqué que la faille était renseignée dans une base de données centrale depuis juin 2008, date à laquelle elle avait également été communiquée à la firme et quittancée par cette dernière [2].

D'autres experts avaient également relayé l'information à l'époque, identifiant déjà très clairement les risques que son existence pouvait représenter pour les consommateurs[3]. Plusieurs gouvernements ont en effet été identifiés pour leurs pratiques intrusives en matière de surveillance des télécommunications. Ces mesures vont de la simple analyse de paquets, passive, à l'écoute active, parfois réalisée via l'introduction de mouchards dans les ordinateurs et téléphones portables des citoyens dont un comportement illégal, ou indésirable, est suspecté[4].

Une récente diffusion de documents par l'organisation Wikileaks (lot de données: spy files[5]) a permis d'identifier formellement la Chine, l'Iran, la Lybie, l'Egypte, la Syrie, la Tunisie et le Bahreïn comme consommateurs de ces technologies de surveillance. Les logiciels concernés sont développés et distribués par des sociétés implantées dans des pays majoritairement occidentaux tels que la France, le Danemark, Israël, l'Allemagne, le Royaume-Uni, la République Tchèque, les Etats-Unis. Fait surprenant, deux sociétés suisses ont été identifiées dans les documents diffusés par l'organisation Wikileaks[4].

Selon des journalistes infiltrés à un récent show de technologies de surveillance tenu cet octobre à Washington, le printemps arabe a constitué un « réveil » pour la majorité des 43 gouvernements présents, soucieux de conserver la visibilité sur les échanges entre civils. Ils ont ainsi eu accès à des technologies d'interception passive ou active dont le prix d'acquisition varie de quelques centaines à plusieurs millions de francs. La petite mallette grise placée dans un aéroport, capable d'intercepter toute télécommunication mobile civile (GSM, 3G, wifi, etc.) et d'injecter un mouchard dans les terminaux Nokia, Blackberry, Android ou iPhone, n'est désormais plus strictement réservée aux acteurs de cinéma[6].

Le cas du logiciel iTunes maintenu en circulation dans un état vulnérable constitue un cas d'école: lors du show précité, un éditeur de logiciels de surveillance a montré comment il exploitait régulièrement cette faille de sécurité pour faciliter l'installation, furtive, de son dispositif de télésurveillance dans des ordinateurs personnels[7].

Apple a attendu trois années pour corriger cette faille de sécurité. Il sera bien entendu difficile de démontrer si cette attente a été motivée par un acte de négligence, d'incompétence, de complicité ou tout simplement un retard induit par la complexité du correctif [ndlr: ...].

L'éditeur a confirmé en juin 2011 que 225 millions de personnes avaient le logiciel iTunes installé sur leur ordinateur, et l'utilisaient activement[8].

1 : <http://support.apple.com/kb/HT5030>

2 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3434>

3 :

http://voices.washingtonpost.com/securityfix/2008/07/holes_in_software_autoupdate_f_1.html

4 : <http://www.rawstory.com/rs/2011/12/01/wikileaks-spy-files-pulls-curtain-back-on-global-surveillance-industry/>

5 : <http://wikileaks.org/the-spyfiles.html>

6 : http://www.cbsnews.com/8301-502223_162-57334605/repressive-governments-using-u.s.-made-spy-technology/

7 : http://www.theregister.co.uk/2011/11/22/trojan_exploits_itunes_flaw/

8 : <http://techcrunch.com/2011/06/07/wwdc-highlights/>

5. [Analyse] Carrier IQ : un logiciel « espion » dans 142 millions de téléphones portables

Un développeur d'applications pour la plateforme mobile *Android* a révélé la présence d'un logiciel collectant les interactions entre l'utilisateur et le téléphone. Rapidement élevé au rang de logiciel espion dont seraient dotés plusieurs dizaines de millions de téléphones, il contreviendrait aux Lois les plus élémentaires de protection de la sphère privée. Plaintes à l'appui.

Polémique

Mi-novembre 2011, un développeur d'applications pour la plateforme mobile *Android* de Google identifie, dans son téléphone, un logiciel dénommé Carrier IQ. L'application est installée par défaut dans son téléphone avant son achat et sans le consentement de son propriétaire. Le chercheur assimile rapidement le logiciel à un mouchard, ou logiciel espion, collectant les données personnelles des utilisateurs contre leur gré. Le logiciel ne peut être installé qu'avec des connaissances avancées, et son existence n'est pas clairement communiquée à l'utilisateur. Trevor Eckhart publie les résultats de sa recherche sur son blog[1], le tout accompagné d'une vidéo qui sera visionnée plus d'un million et demi de fois en une semaine.

Tout le monde y passe...sauf

Moins d'une semaine s'écoule avant que les acteurs majeurs de la presse technologique ne relayent l'information, annonçant la présence d'un mouchard préinstallé dans environ 145 millions de téléphones portables de grande consommation. La polémique cible notamment les appareils dotés du système d'exploitation *Android* maintenu par Google, et équipant de nombreux appareils actuels des marques Samsung, HTC, Sony Ericsson, LG et Motorola. Il est toutefois rapidement allégué que les appareils dotés des systèmes *Symbian* (Nokia) et *Blackberry* (RIM) sont eux aussi dotés du *logiciel espion*[2].

Comme l'on pouvait s'y attendre, les premiers articles (eux aussi totalement infondés) recommandant aux lecteurs de s'orienter vers l'appareil iPhone ne tardent pas à apparaître[3]. Ils seront estompés moins d'un jour plus tard par des travaux de recherche confirmant l'existence du logiciel Carrier IQ, déjà présent depuis la troisième version du célèbre téléphone produit par la firme à la pomme croquée[4]. Apple confirme, mais annonce que le logiciel bien qu'étant présent, n'est plus activé depuis la cinquième version de son système[5]. Nokia dément également officiellement toute présence du logiciel dans ses appareils[6]. Un seul et unique système grand public est épargné : Windows Phone 7[7].

Tout cela est bien entendu publié sans compter la prise de position de l'éditeur lui-même[8], annonçant que ce n'est pas le constructeur qui prend les décisions mais l'opérateur, qui décide si oui ou non le logiciel doit être installé et avec quelle envergure. Comme l'on pourrait s'y attendre après lecture de ce paragraphe, les opérateurs devraient tout naturellement devenir les futures cibles d'actions en recours collectif....faux.

CIQ, éditeur du logiciel, prend position

La société éditrice du logiciel émet un communiqué de presse officiel sur son site le 1^{er} décembre[8]. Des éléments d'information essentiels y sont annoncés. L'éditeur communique en premier lieu sur la finalité de la collecte de données opérée par leur logiciel, indiquant que les données se destinent aux opérateurs à des fins d'amélioration de service et de diagnostic d'incidents. Il communique également sur la nature des données collectées, indiquant par exemple que le contenu des messages n'est pas envoyé à l'extérieur du téléphone. Propos s'opposant ainsi directement aux allégations émanant des travaux de recherche du développeur à l'origine de la polémique.

Le second point abordé par l'éditeur est l'annonce de mesures de sécurité, garantissant à l'utilisateur que ses données sont collectées, traitées et transmises en conformité avec les lois et que des moyens sont déployés pour en assurer leur protection (transmission chiffrée et exclusive à l'opérateur avec lequel l'utilisateur a conclu un contrat).

Finalement, l'éditeur rappelle que le champ et la proportion des données collectées dans l'appareil sont imposés par l'opérateur lui-même et non par l'éditeur du logiciel. Le lecteur attentif remarquera ici le passage du témoin aux opérateurs téléphoniques...

La cible des attaques est-elle donc bien choisie ?

La vidéo dans laquelle le chercheur révèle l'existence d'une collecte de données[9] a été consultée plus d'un millions et demi de fois. L'on y observe un téléphone connecté à un terminal et la console affiche les données émises par le canal de diagnostic du téléphone (fonctionnalité *USB debugging* des systèmes *Android*). A plusieurs reprises, il est démontré que Carrier IQ est en mesure d'annoncer le contenu détaillé de plusieurs données personnelles, comme les messages SMS et les paramètres saisis dans le navigateur durant des connexions sécurisées SSL.

En revanche, deux éléments factuels essentiels sont restés absents des contenus référencés au grand public.

En premier lieu, rien ne permet d'affirmer que les données confidentielles affichées sur la console de diagnostic du téléphone sortiront effectivement de l'appareil via les ondes aériennes, pour être transmises à un tiers. Cet élément n'est pas confirmé, ni contredit, il est occulté dans la vidéo.

En second lieu, les systèmes d'exploitation mobiles sont réputés mettre en œuvre un dispositif de cloisonnement (*sandboxing*) des applications garantissant qu'elles ne peuvent communiquer entre elles sans l'aval du dispositif de contrôle d'accès central, pour des raisons évidentes de sécurité. La vidéo publiée par le chercheur révèle que le logiciel Carrier IQ a accès aux interactions de l'utilisateur avec le navigateur web et l'application de messagerie SMS. Elle ne permet toutefois pas d'inférer que Carrier IQ intercepte ces données sans l'autorisation explicite, soit par l'utilisateur (permissions lors de l'installation d'une application), soit par le constructeur (contournement des mécanismes de sécurité autorisé dans certains cas), ou finalement, par l'exploitation d'une éventuelle faille de sécurité... Ce second élément n'est, lui aussi, ni confirmé, ni contredit, et reste occulté dans la vidéo.

En plus d'être fondée sur l'absence notable d'éléments concordants, la polémique Carrier IQ reflète une fois encore, au travers de la rapidité et de l'amplitude avec lesquelles l'information a été véhiculée et à quel point le consommateur doit rester vigilant quand à la nature des faits associés aux conclusions qui lui sont communiquées.

Un débat presque philosophique prochainement tranché

L'affaire a pris une tournure de l'ordre du débat d'école: doit-on imputer une responsabilité à l'éditeur d'un logiciel dont l'installation et la configuration sont effectués sous la direction des opérateurs téléphoniques?

Le consommateur trouvera probablement une partie de la réponse dans les conclusions de la multitude d'actions en recours collectif (*class-actions*) déposées l'une après l'autre suite à l'intervention du Sénat américain[10] le 1^{er} décembre dernier. Les plaintes ont été déposées contre CIQ (l'éditeur), les constructeurs Samsung, HTC, Apple et Motorola.

Comme annoncé plus haut dans cette analyse, le lecteur constatera que la première salve de plaintes a été adressée à l'éditeur du logiciel et aux constructeurs de téléphones. Quelques nuits

de sommeil ont suffi pour que la sagesse s'oriente enfin vers les opérateurs...les plaintes venant d'être déposées contre les opérateurs téléphoniques Sprint et AT&T.

En Europe ?

L'affaire est suivie en Europe également, bien que peu d'éléments permettent d'affirmer que les pratiques ont été copiées par les opérateurs outre-Atlantique. Le préposé allemand à la protection des données a exigé une prise de position du constructeur Apple[11]. Les préposés britannique, irlandais, français et italien ont également annoncé entreprendre des mesures.

Comme on pourra rapidement le constater en prenant connaissance des différents articles publiés ci-et-là dans la presse, cette affaire sera avant toute autre chose un cas d'école majeur d'interprétation des Lois sur la protection des données personnelles dans un contexte extrêmement complexe en raison de la multiplicité des considérations territoriales (quelle loi appliquer dans quel pays ?), des acteurs investis dans un téléphone portable (constructeur, éditeur de logiciels, éditeur de systèmes, opérateur mobile et...utilisateur), et de la perception biaisée des consommateurs (« mon téléphone et son contenu m'appartiennent-ils? »).

- 1 : <http://www.wired.com/threatlevel/2011/11/secret-software-logging-video>
- 2 : <http://www.geek.com/articles/mobile/how-much-of-your-phone-is-yours-20111115/>
- 3 : <http://www.extremetech.com/mobile/107337-carrier-iq-is-the-best-reason-yet-to-switch-to-iphone>
- 4 : <http://blog.chpwn.com/post/13572216737?831dd5c8>
- 5 : http://articles.businessinsider.com/2011-12-01/tech/30462142_1_ios-apple-encrypted-form
- 6 : <https://twitter.com/#!/jurthys/status/141856513542205440>
- 7 : <http://wmpoweruser.com/carrieriq-spyware-now-found-on-ios-android-blackberry-and-symbian-only-windows-phone-not-implicated-so-far/>
- 8 : http://www.carrieriq.com/CIQ_Press_Statement_DEC_1_11.pdf
- 9 : http://www.youtube.com/watch?v=T17XQI_AYNo
- 10: <http://paidcontent.org/article/419-samsung-and-htc-hit-by-wiretapping-lawsuit-over-tracking-software>
- 11 : <http://paidcontent.org/article/419-carrier-iq-responds-more-to-privacy-allegations-but-many-questions-remain/>

[*ndlr* : pour les plus curieux, le lien ci-après (et sa date de publication) pourraient amener de nouvelles réflexions : <http://infectedrom.com/content.php/154-HTCs-User-Behavior-Logging>]

6. En Bref

Facebook : un cheval de Troie bancaire en propagation à travers les murs des "amis"

Un ver se propageant à travers les profils du réseau social Facebook invite les *amis* du compte infecté à récupérer un écran de veille. Ce dernier n'est autre qu'une toute récente variante du cheval de Troie Zeus, spécialement dotée de fonctionnalités de détournement de fonds lorsqu'il détecte la présence d'une connexion à l'e-banking des principales banques mondiales.

-- http://www.theregister.co.uk/2011/11/29/facebook_worm_spreads/

Téléphones Android : le dispositif de permissions peut être contourné

Des chercheurs en Caroline du Nord ont identifié un moyen de contourner le mécanisme des permissions du système mobile Android. Ainsi exploitée, cette technique permettrait à des applications ne disposant de permissions particulières d'accéder à des contenus confidentiels d'autres applications.

-- <http://www.linformaticien.com/actualites/id/22446/decouverte-d-une-faille-critique-dans-android.aspx>

Réponse urgente en cas d'incident : mise à jour de la carte européenne des CERTs

L'agence européenne de sécurité des systèmes d'information (ENISA) a publié mardi dernier la version 2.6 de sa carte localisant les centres CERT européens. L'on notera en premier lieu la mention de six centres de réponse d'urgence en Suisse : CC-SEC, CERN CERT, ETHZ-NSG, IP+ CERT, OS-CIRT, SWITCH-CERT. L'on notera en second lieu qu'aucun d'entre eux ne se destine directement à fournir de l'assistance aux PME suisses...

-- <http://www.enisa.europa.eu/media/news-items/new-updated-map-v2.6-of-digital-fire-brigades-certs>

Facebook: une faille permettant de consulter les photos privées dévoilée au public

Un internaute a publié samedi dernier les détails d'une vulnérabilité de sécurité concernant le réseau social Facebook. Le message détaille en peu de mots une méthode permettant d'accéder aux photos volontairement protégées ou cachées par un utilisateur, sans devoir disposer de connaissances techniques particulières. Les détails de la faille ayant été rendus publics, l'éditeur a été contraint de rapidement colmater la brèche. Le message annonçant la faille a été publié sur le forum d'un site communautaire pour amateurs de musculation...

-- <http://gawker.com/5865642/mark-zuckerberg-cant-protect-his-own-facebook-photos>

Suisse: le téléchargement d'œuvres protégées n'a pas besoin d'encadrement supplémentaire

Le Conseil Fédéral s'est prononcé en défaveur d'une modification du cadre juridique entourant le téléchargement d'œuvres protégées via Internet. Les trois alternatives proposées, à savoir, la riposte graduée (modèle français HADOPI), la surveillance du trafic (packet inspection) et la taxe sur les médias ont été refusées. Le Conseil Fédéral a jugé qu'elles constituaient un facteur de risque principalement aggravant, respectivement, en accordant trop de pouvoir aux majors, en empiétant sur la sphère privée des citoyens et en créant une incompatibilité avec les accords internationaux en vigueur.

-- <http://www.ejpd.admin.ch/content/ejpd/fr/home/dokumentation/mi/2011/2011-11-30.html>

Plus de 4'000 sites web infectés au moyen d'une injection SQL

Une opération d'infection à large échelle de postes clients a été identifiée jeudi dernier par des lecteurs du Sans Internet Storm Center. Le mode opératoire des attaquants consiste à balayer de façon automatisée des sites web les uns après les autres en compromettant ceux présentant des vulnérabilités de type SQL Injection (applications transmettant des paramètres client aux bases de données sans les contrôler au préalable) et reliés à un système SQL Serveur. Plus de 4'000 sites infectés ont été recensés par Google 12 heures après l'annonce. Lorsque l'infection est en place sur le site, tout internaute qui le consulte avec un système ne disposant pas des dernières mises à jour est exposé à l'infection par un cheval de Troie. La signature de l'attaque est disponible dans le lien fourni.

-- <http://isc.sans.edu/diary.html?storyid=12127>

FIN/#003.

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)