Bulletin Cybersécurité et menaces Internet #001 / Octobre 2011
http://cddb.ch

Si vous souhaitez recevoir automatiquement les prochains bulletins par email, envoyez un message avec pour sujet "inscription" à:
cddb-pdf@nxtg.net (texte brut + version PDF en pièce jointe)
cddb-text@nxtg.net (texte brut uniquement)

Sommaire

SEC: obligation aux entreprises cotées de notifier les incidents de cybersécurité

Le communiqué n'a pas encore de valeur réglementaire mais annonce très clairement la position de la SEC, qui joue aujourd'hui sur les entreprises américaines cotées un rôle s'apparentant à celui d'un gendarme, concernant la divulgation d'incidents de sécurité informatique dont les entreprises pourraient avoir été victimes. Le message n'est pas un exemple de limpidité mais a le mérite d'annoncer la couleur!

"A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences."

Traduction: il ne sera pas suffisant de présenter des facteurs de risque inhérents à tous les acteurs de l'industrie concernée mais il faudra informer les investisseurs quant aux risques spécifiques auxquelles l'organisation est exposée, en particulier, celui résultant d'un incident survenu dans l'organisation ou auprès de l'un de ses partenaires ou fournisseurs.

On notera que le critère déterminant ne sera pas constitué d'éléments internes à l'intrusion mais des impacts liés à la perte financière induite par ce dernier:

- délai nécessaire pour le retour à la pleine capacité de production
- conséquences légales et réglementaires de l'incident
- accroissement imprévu des coûts de cybersécurité (modifications organisationnelles, déploiement de nouveau personnel et technologies, formation, engagement d'experts/consultants, etc.)
- perte financière directe induite par un départ de clients
- frais juridiques et évaluation du dommage sur la réputation générale de l'organisation

1: http://sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
2: http://www.computerworlduk.com/news/security/3311262/us-regulators-push-firms-to-disclose-cyberattacks/

Guerre en Lybie: les États-Unis disposaient d'une stratégie électronique

Le NY Times rapporte que des hauts responsables à la Défense ont confirmé qu'une stratégie d'intrusion par les voies électroniques a été conçue pour assister le démantèlement du gouvernement Khadafi.

Les éléments tactiques de l'opération n'ont pas été divulgués mais le Président aurait pris la décision à la dernière minute de ne pas confirmer son lancement, en particulier, car cela aurait causé un précédent probablement encourageant aux yeux de la Chine et de la Russie. Des soldats au sol assistés de drones de combat ont donc été privilégiés, encore une fois.

L'objectif de l'opération aurait été de pénétrer les systèmes de défense aérienne du gouvernement libyen et de prendre le contrôle, ou le cas échéant de les rendre inopérants, des radars prenant part au bouclier aérien.

Une stratégie similaire avait été préparée pour soutenir le commando d'intervention déployé au sol lors de la mission d'exécution du leader Al-Quaidiste, Ousama Ben Laden.

"Les américains ne veulent pas être ceux qui briseront la glace dans cette nouvelle forme de conflit", James Andrew Lewis, Center for Strategic and International Studies

1: http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1

DQ: Stuxnet, version 2.0

L'Iran, et d'autres organisations européennes, pourrait avoir été la cible d'une seconde cyberattaque majeure (la première étant la propagation du ver Stuxnet dans les centrifugeuses nucléaires, survenue en 2009) cet été, témoignent des experts sécurité de l'éditeur Symantec dans une récente analyse [1].

DQ, à prononcer "dix culs" pour ceux qui osent en parler, est composé en grande partie de code emprunté dans les entrailles du ver original Stuxnet[2]. Les charges hostiles ainsi que les mécanismes d'auto-propagation ont été retirés du code, transformant le ver en un cheval de Troie essentiellement "inoffensif" si ce n'est qu'il permet à l'attaquant de contrôler un système à distance.

En raison de l'absence d'un mécanisme de propagation couplé à une présence marquée au sein de plusieurs organisations européennes, les analystes concluent que le logiciel présente les signes d'une cyberattaque ciblée et organisée dont plusieurs organisations européennes auraient été victimes.

Le logiciel utilise les canaux HTTP et HTTPS pour établir son canal de commande/contrôle et diffuse les données volées en les dissimulant à l'intérieur de fichiers images (JPEG) anodins. Après 36 jours, le logiciel se retire de lui-même des systèmes infectés, rendant dès lors la détection d'une infection plus difficile à établir.

Selon les organisations dans lesquelles l'attaque aurait été détectée, le rôle exact du logiciel serait de collecter des informations de conception spécifiques à des éléments couramment utilisés dans les entreprises industrielles. En quelque sorte: il s'agirait d'alimenter une version plus hostile du prochain Stuxnet en lui insérant des connaissances techniques préalables pour mieux infecter ses futures cibles[3].

Analyse technique détaillée disponible au téléchargement[4].

1: http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet
2: http://frontpagemag.com/2011/10/21/second-cyber-attack-on-iran/
3: http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet
4: http://goo.gl/NGtdd (fichier pdf)

Cyberattaque du NASDAQ: impacts difficiles à évaluer

Les pirates du groupe Anonymous avaient largement annoncé cette menace l'an dernier mais elle n'a probablement pas été prise autant au sérieux qu'elle ne l'aurait dû. En octobre dernier (2010), une attaque contre les systèmes d'information du NASDAQ (après le NYSE, second plus grand marché d'échange d'actions au monde) avait été détectée et, selon les communiqués, n'avait pas fait de dégâts particuliers. L'évaluation des dégâts a depuis été revue à la hausse: l'investigation du FBI[1] a récemment identifié que les pirates n'avaient pas visé directement les systèmes boursiers, contrairement à ce qui avait été cru, mais un outil bien particulier: Directors Desk, couramment utilisé lors des réunions de conseils d'administration d'entreprises inscrites au NASDAQ.

Directors Desk est basé sur une architecture web et assiste les réunions de conseils d'administration durant lesquels les membres ne sont pas tous physiquement présents en un même lieu. Il permet en particulier l'échange *sécurisé* de documents et de messages entre intervenants. Les pirates ont réussi à infiltrer le service et y injecter du code qui leur aurait permis durant plusieurs mois d'observer les échanges entre les différents conseils d'administration.

Les investigateurs ne savent toujours pas avec précision depuis quand Directors Desk était sous contrôle externe, malgré la découverte de l'incident il y a à présent une année.

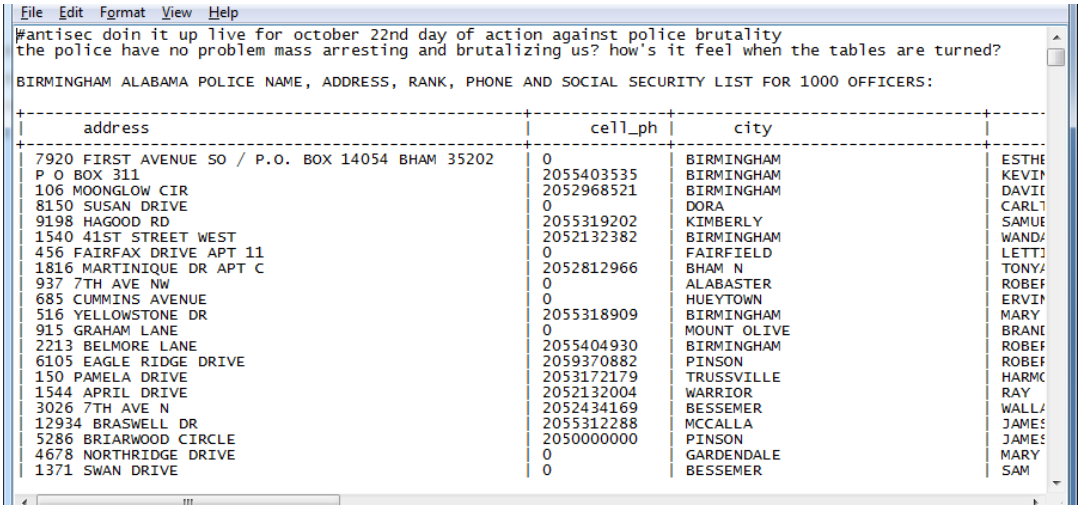
Les motivations d'une telle attaque ne sont pas difficiles à identifier, dès lors que l'on sait qu'elle permettait aux pirates de se tenir au courant des échanges lors des réunions de conseils d'administration des plus importantes entreprises américaines...

1: http://www.firstpost.com/fwire/long-term-impact-of-nasdaq-cyber-attack-unknown-113316.html

La base de données des agents de la Police de Birmingham diffusée

La vague d'attaques visant à divulguer les bases de données des autorités policières à l'échelle nationale (Etats-Unis) s'étend cette fois-ci à Birmingham, dans l'Etat de l'Alabama[1]. Les données personnelles d'un peu plus d'un millier d'agents ont été diffusées sous la forme d'un fichier en texte brut:

Le fichier a été rendu disponible pendant quelques minutes avant d'être rapidement retiré des plateformes sur lesquelles il avait été posté. Le fichier comportait un listing détaillé de plus d'un milliers d'agents de Police de la ville de Birmingham, incluant leur adresse personnelle, leur numéro de mobile personnel, noms, prénoms, rang au sein de la Police sans oublier leur numéro de sécurité sociale (SSN), un élément considéré comme plus que confidentiel aux Etats-Unis car il sert d'authentifiant auprès de nombreuses autorités administratives.



File Edit Format View Help

#antisec doin it up live for october 22nd day of action against police brutality
the police have no problem mass arresting and brutalizing us? how's it feel when the tables are turned?

BIRMINGHAM ALABAMA POLICE NAME, ADDRESS, RANK, PHONE AND SOCIAL SECURITY LIST FOR 1000 OFFICERS:

address	cell_ph	city	
7920 FIRST AVENUE SO / P.O. BOX 14054 BHAM 35202	0	BIRMINGHAM	ESTHE
P O BOX 311	2055403535	BIRMINGHAM	KEVIN
106 MOONGLOW CIR	2052968521	BIRMINGHAM	DAVID
8150 SUSAN DRIVE	0	DORA	CARLT
9198 HAGOOD RD	2055319202	KIMBERLY	SAMUE
1540 41ST STREET WEST	2052132382	BIRMINGHAM	WANDA
456 FAIRFAX DRIVE APT 11	0	FAIRFIELD	LETTI
1816 MARTINIQUE DR APT C	2052812966	BHAM N	TONYA
937 7TH AVE NW	0	ALABASTER	ROBER
685 CUMMINS AVENUE	0	HUEYTOWN	ERVIN
516 YELLOWSTONE DR	2055318909	BIRMINGHAM	MARY
915 GRAHAM LANE	0	MOUNT OLIVE	BRAND
2213 BELMORE LANE	2055404930	BIRMINGHAM	ROBER
6105 EAGLE RIDGE DRIVE	2059370882	PINSON	ROBER
150 PAMELA DRIVE	2053172179	TRUSSVILLE	HARMO
1544 APRIL DRIVE	2052132004	WARRIOR	RAY
3026 7TH AVE N	2052434169	BESSEMER	WALLA
12934 BRASWELL DR	2055312288	MCCALLA	JAMES
5286 BRIARWOOD CIRCLE	2050000000	PINSON	JAMES
4678 NORTHRIDGE DRIVE	0	GARDENDALE	MARY
1371 SWAN DRIVE	0	BESSEMER	SAM

1: http://thenewcivilrightsmovement.com/occupy-wall-street-anonymous-hack-police-leak-passwords-personal-data/politics/2011/10/21/28969

EVENT: Forum romand de la sécurité logicielle (Yverdon-les-Bains, 26-27oct2011)

C'est pour sensibiliser les développeurs mais également les décideurs que l'APSEL (Association pour la Promotion de la Sécurité Logicielle en suisse) reconduit pour la seconde année consécutive l'Application Security Forum, les 26 et 27 octobre prochains.

La journée du 26 octobre sera dédiée à des séminaires de transfert de connaissance se déroulant sur une demi-journée (ateliers) ou la journée entière (formations). La journée du 27 octobre basculera sur un programme inédit de dix-huit conférences. Cette approche offrira à chaque participant(e) l'opportunité de vivre une expérience « à la carte », s'adaptant au mieux à ses attentes, tout comme à ses connaissances techniques.

Entrée gratuite aux conférences, sur inscription
Réduction de 25% sur tous les ateliers/formations: promocode "CDDB" à saisir lors de l'inscription.

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

FIN/#001.