Note de Veille Cyber n°2

Du 14 février au 11 mars 2011 par Alix Desforges

Note préalable à la lecture : du fait de la nature du sujet et de l'intérêt d'une note conçue à l'appui de l'ensemble des sources d'information disponibles sur le web (blog, journaux, etc.), la totale fiabilité des informations proposées ne peut être pleinement garantie. Cette note propose d'ouvrir des perspectives. A chacun de poursuivre le travail.

Piratage

Les sites institutionnels et gouvernementaux de plus en plus visés par des attaques informatiques. Source

De nombreux pays ont vu leurs sites web attaqués. Un rapport émis par le CERT de l'Etat chinois, le CNCERT/CC, a estimé que les attaques à l'encontre des sites gouvernementaux chinois ont progressé de 68% en 2010. Selon le rapport, sur les 35 000 sites chinois ayant subi une attaque 5 000 étaient des sites institutionnels ou gouvernementaux. Les sites gouvernementaux deviennent des cibles privilégiées pour les pirates à plusieurs titres :

Le piratage pour détruire. Source

Au cours du week-end du 5 mars, une trentaine de sites gouvernementaux sud-coréens ont par exemple essuyé des attaques informatiques de type DDOS. Les attaques, de faible intensité, n'auraient pas causé de dommage, selon les autorités qui ont immédiatement accusé son voisin du Nord comme responsable.

Le piratage comme acte d'opposition. Source

Un groupe de pirates informatiques se désignant comme l'Iranian Cyber Army a piraté le site d'actualité gouvernementale américain. Les pirates ont détourné le trafic du site vers un second contrôlé par eux-mêmes, sur lequel ils demandaient à Hillary Clinton « d'arrêter de s'ingérer dans les pays islamiques » suite au soutien apporté par la Secrétaire d'Etat américaine aux manifestants en Tunisie et en Egypte. L'action a par la suite été revendiquée par un officiel du gouvernement iranien au nom des Gardiens de la Révolution Islamique.

Le piratage pour espionner. Source

Les Ministères des Finances canadien et français ont été la cible de cyberespionnage. Dans le cas canadien, les pirates étaient à la recherche des mots de passe des agents du Ministère afin d'accéder à des bases de données. En France, l'attaque opérait depuis décembre 2010 et visait « des documents relatifs à la présidence française du G20 ainsi qu'aux affaires économiques internationales », selon Patrick Pailloux directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information. Il s'agissait là d'une vaste opération d'espionnage qui a demandé une phase de préparation importante. Seuls 150 ordinateurs du Ministère auraient été infiltrés. Tous appartenaient à des personnes travaillant spécifiquement sur le G20. Le mode opératoire des pirates « déterminés, professionnels et organisés » selon les termes de Patrick Pailloux laisse à penser à une action organisée par un Etat ou un groupe puissant (altermondialiste ?).

Organisation et doctrine des armées

L'ANSSI en charge de la cyberdéfense des SI de l'Etat. Source

Selon le décret publié au Journal Officiel et modifiant l'article 3 du décret du 7 juillet 2009, l'ANSSI « assure la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité et dans le cadre des orientations fixées par le Premier Ministre, elle décide les mesures que l'Etat met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne l'action gouvernementale ». A la suite de ce décret l'ANSSI a publié un document d'orientation générale intitulé « Défense et sécurité des systèmes d'information : Stratégie de la France ». C'est la même ANSSI, qui a pu, grâce à ses nouvelles prérogatives, intervenir sur les ordinateurs du Ministère des Finances. Un deuxième décret crée la Direction Interministérielle des Systèmes d'Information et de Communication de l'Etat (DISIC) dirigée par Jérôme Filippini, ainsi nommé DSI de l'Etat.

L'Allemagne crée son centre de cyberdéfense. Source

Le Ministre de l'Intérieur allemand a confirmé la création d'un Centre national de cyberdéfense. Le BSI (office fédéral de la sécurité des technologies de l'information) sera en charge de ce centre qui devrait

être opérationnel au 1er avril 2011. Thomas de Maizière a précisé que l'Allemagne ne chercherait pas à acquérir des capacités offensives pointant les difficultés d'identification des auteurs des cyberattaques. « La destruction d'un serveur à l'origine d'une attaque n'est pas la tâche du Centre national de cyberdéfense » a-t-il déclaré.

L'armée américaine affine sa stratégie dans le domaine cyber. Source

La Stratégie militaire nationale des Etats-Unis pour 2011, récemment publiée, mentionne à plusieurs reprises l'importance du cyberespace et de l'espace dans la stratégie américaine. Le document met également en avant la nécessité de mener une réflexion au niveau international comme le cyberespace et l'espace font partie des global commons. « Notre capacité à opérer efficacement dans l'espace et le cyberespace en particulier est de plus en plus essentielle pour faire face à une agression ». Dans ce cadre, le Pentagone serait sur le point d'ajouter le cyberespace à la liste des champs de bataille, d'après le Secrétaire d'Etat à la Défense. Baptisée Cyber 3.0, cette nouvelle stratégie donnerait au DoD la responsabilité de défendre les réseaux gouvernementaux.

Au niveau de l'US Cyber Command, son chef Keith Alexander a réclamé que sa structure soit responsable de la protection des infrastructures critiques tant publiques que militaires et privées. Au sein de l'USCYBERCOM, l'Army tente également d'organiser son propre Cyber Command. La division du Colonel Brian Moore (l'US Army Cyber Command) n'a pas encore choisi son QG et n'est pas opérationnelle. Elle devrait compter à termes 1000 personnes, civiles et militaires.

Comme en témoignent ces nombreuses initiatives, les armées américaines sont très concernées par le cyberespace et se préparent à faire face à ses menaces. Cela commence aussi par la formation. L'US Naval Academy vient, à ce titre, d'intégrer dans sa formation un cursus consacré à la cybersécurité et à la défense des réseaux pour former les futurs militaires. Il faut cependant noter que l'US Military Academy et l'US Air Force Academy avaient déjà intégré la cybersécurité à leurs formations il y a plus de 10 ans.

Le Sri Lanka également en ordre de bataille. Source

Le chef de l'armée sri-lankaise a déclaré que le Sri-Lanka se devait d'être prêt à faire face aux cybermenaces. Il définit dans ce cadre le terme de « cyberguerre ». Selon lui, il s'agit de toutes « actions d'Etats ou de groupes pour pénétrer les ordinateurs, réseaux ou sites web d'autres Etats via le cyberespace dans le but de causer des dégâts voire d'interrompre le service ».

Menaces

Une nouvelle analyse de Stuxnet. Source

Les experts de Symantec ont publié de nouvelles informations sur le ver Stuxnet. Ils ont notamment pu établir que le ver a touché cinq organisations différentes, mais toutes présentes en Iran, contaminant près de 12 000 ordinateurs. Ils ont également identifié différentes phases d'infection. Trois de ces organisations n'ont été attaquées qu'une seule fois, deux ont été visées deux fois et une trois fois entre juin 2009 et mai 2010. Le ver compte 3 variantes apparaissant successivement en juin 2009, mars 2010 et avril 2010.

Table 1
W32.Stuxnet Timeline

Date	Event
November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.
April, 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June, 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.
March, 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.
July 17, 2010	Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

Craintes d'attaques informatiques à l'encontre des infrastructures critiques ou l'effet Stuxnet. Source

Un sondage mené par le Center for Strategic and International Studies pour McAfee révèle que les industriels craignent des attaques contre les réseaux de distribution d'électricité et de gaz. En outre plus de 40% des sondés pensent que ces attaques pourront causer des arrêts dans la distribution d'au moins 24h et pourraient éventuellement coûter des vies humaines. Si beaucoup des sociétés distributrices d'énergie sont conscientes des risques qui pèsent sur leurs réseaux, seulement deux tiers expliquent planifier des mesures de protection spécifiques pour leurs réseaux. A l'heure où la France et la Grande Bretagne développent des réseaux smart grid, ce sondage révèle les enjeux de la sécurisation de ces réseaux intelligents.

La lutte contre les botnets, un enjeu international, selon l'ENISA. Source

L'European Network Information Security Agency pointe, dans un rapport, le manque de coopération internationale, de partage de l'information et la faiblesse des lois nationales dans la lutte contre les botnets. Le rapport évoque les mesures à mettre en place. Il souligne notamment le bon exemple allemand où l'Etat a financé un programme pour aider les FAI à mettre en place les technologies nécessaires pour

l'identification des ordinateurs zombies, qui permettent les attaques de type DDOS.

Initiatives

Le projet de loi « Kill Switch » fait toujours débat aux Etats-Unis. Source Source

L'opposition au projet de loi surnommé « Kill Switch » ou Protectect Cyberspace as a National Asset se fait de plus en plus importante. L'Electronic Frontier Foundation, puissant lobby pour les libertés civiles sur le Net, s'inquiète de voir confier « à n'importe qui le pouvoir de couper toutes les communications électroniques à n'importe quel instant ». Le Sénateur Libermann, porteur du projet de loi, martèle que ce projet ne vise pas à couper Internet mais uniquement les réseaux des infrastructures critiques. Dans ce contexte, un autre projet de loi a été posé pour compléter le premier et limiter les pouvoirs du Président. Le Cybersecurity and Internet Freedom Act interdit à quiconque, y compris au Président, d'avoir le pouvoir de couper Internet. Il indique également que les pouvoirs du Président concernant la coupure des communications électroniques seront limités aux prescriptions du Communication Act of 1934, qui définit les possibilités de couper les communications en temps de guerre.

Chine et Etats-Unis coopèrent dans la lutte contre le spam. Source

L'East West Institute et l'Internet Society of China, agence du gouvernement chinois, élaborent conjointement un rapport sur la sécurité informatique. Cette initiative fait suite à un accord signé entre Barack Obama et Hu Jintao pour joindre leurs efforts en matière de cybersécurité et en particulier dans la lutte contre le spam.

Un premier traité de cyber-paix ? Source

Le Japon et les Etats-Unis auraient signé un accord pour une « cyber-alliance » qui interdirait aux deux parties de s'attaquer mutuellement. Cet accord résulterait de la crainte commune du Japon et des Etats-Unis du développement des capacités nord-coréennes et chinoises en matière de cyberguerre.

Les Etats-Unis augmentent leur budget cyber. Source

Les questions de cybersécurité font partie des priorités du gouvernement Obama à en croire les prévisions budgétaires pour l'année 2012. Dans de nombreuses agences, les budgets alloués à cette problématique sont en constante augmentation. Par exemple, le budget prévisionnel du DoD prévoit d'octroyer à la DARPA un demi-milliard de dollars pour la R&D en technologies cyber. En outre, 1,3 milliard de dollars pour la formation d'analystes cyber. Des crédits devraient également être débloqués pour la mise en place d'un centre des opérations interarmées au sein de l'US Cyber Command.

Publications récentes

Rapports

- Symantec, W32.Stuxnet Dossier, février 2011
- Internet Security Alliance, White Paper « Improving our Nation's Cybersecurity through the Public-Private Partnership », Mars 2011
- ENISA, Botnets : Detection, Measurement, Disinfection & Defence, Mars 2011

Publications universitaires et comptes-rendus de conférence

- Pierre Zanger, Coercition dans le cyberespace, sécurité et discours sécuritaire, conférence du 8 février au Cercle Européen de la SSI, février 2011
- Kenneth Geers, Sun Tzu and Cyber War, OTAN, 9 février 2011
- Martin Libicki, Cyberdeterrence and Cyberwar, RAND Corp., conférence « Rethinking the future international security environment », février 2011
- Strategic Studies Quartely, spring 2011, Vol5, N°1, Air University Press
- Jack Goldsmith, Cybersecurity Treaties : A Skeptical View, Future Challenges in National Security and Law, 2011

Stratégies nationales

- ANSSI, Défense et sécurité des systèmes d'information, Stratégie de la France, février 2011
- Ministerio de Defensa, Cibersecuridad, retos y amenazas a la seguridad nacional en el ciberespacio, diciembre 2010
- Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, février 2011
- Gouvernement des Pays Bas, Nationale Cyber Security Strategie : Slagkracht door samenwerking, février 2011

Evènements

Retour sur la conférence RSA. Source

Les évènements de sécurité de l'année 2010 ont mis la problématique de la cyberguerre au cœur des débats de la conférence RSA. Les experts ont discutés le terme de cyberguerre et ses enjeux. Pour certains, l'utilisation massive du mot cyberguerre est un abus de langage. Le cyber-tsar à la Maison Blanche, Howard Schmidt, réclame d'ailleurs l'arrêt de l'amalgame entre la

cyberguerre, le cyberespionnage et la cybercriminalité. « Les mots ont leur importance » a-t-il martelé. Si Bruce Schneier, expert en cybersécurité, partage cette analyse, il rappelle également que cette rhétorique guerrière fait partie d'une lutte intestine entre les agences fédérales pour le contrôle des politiques en matière de cybersécurité et sert les industriels qui cherchent à vendre leurs produits. Selon lui, « tous ces exemples ne relèvent pas vraiment de la guerre mais si vous les qualifiez ainsi, vous enclenchez, dans les esprits, une série de boutons psychologiques ».

La conférence a également évoqué les négociations à l'ONU pour un traité international de désarmement du cyberespace. Pour Howard Schmidt, ce traité « ne résoudra pas tous les problèmes. Tout le monde ne pense pas unilatéralement dans le monde entier ». D'autres estiment néanmoins que les négociations ont avant tout le mérite d'ouvrir le débat.