Sécurité : les 10 principales menaces de 2014

Le **Panorama sur la cyber-criminalité 2013 du Clusif** (du nom d'un cercle de référence de responsables de sécurité IT en entreprise) livre une bonne synthèse des grandes menaces auxquelles sont confrontés les utilisateurs. Délinquance numérique, internationalisation de la criminalité, intensification des assauts par déni de service distribué…

Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013. Silicon.fr a dégagé dix tendances sur la cyber-sécurité et la cyber-criminalité qui se sont propagées courant 2013 et que l'on retrouvera inéluctablement sur 2014.

1) Espionnage d'Etat : les armées de l'ombre

Selon le Clusif, un rapport d'un éditeur de sécurité IT américain émis en 2013 a permis de faire la lumière sur les pratiques de cyber-espionnage et de piratage menées ou soutenues par des autorités étatiques. C'est le cas de la Chine avec un groupe de hackers probablement issu de l'armée populaire. L'Unité 61398, basée à Shanghai, a visé 140 entreprises de 20 secteurs d'activité différents. « Les moyens alloués étaient importants puisque la masse de données collectées et stockées s'évaluerait en téraoctets. »

2) Snowden : le renseignement américain mis à nu

Edward Snowden aura marqué l'année 2013. Les multiples révélations de cet ancien consultant informatique rattaché à la NSA portant sur les pratiques de cyber-espionnage à grande échelle (programme Prism) ont choqué le monde. Au-delà des canaux surveillés (téléphones, messageries, câbles télécoms sous-marins…), le Clusif évoque un véritable « entonnoir d'espionnage » industrialisé bien que l'administration Obama se targue de mener ses opérations au nom de la lutte contre le terrorisme. Même le Président des Etats-Unis a considéré que les agences de renseignement sont allées trop loin dans la surveillance de hauts dirigeants de pays alliés, comme ce fut le cas pour Angela Merkel, la Chancelière allemande. « Les capacités de collecte et d'analyse y sont particulièrement élevées et la possibilité de rechercher des informations ciblées impressionne », estime le Clusif. Malgré une réforme des pratiques des agences de renseignement annoncées par Barack Obama et malgré l'embarras des géants du Web (Google, Microsoft, Yahoo, Facebook sont accusés de connivence alors qu'ils prônent davantage de transparence et qu'ils s'engagent à renforcer le chiffrement dans les réseaux respectifs), il est difficile de parler de réels progrès.

3) Libertés numériques bafouées, données

personnelles en sursis ?

L'année 2013 a été agitée en termes de débat sur le cadre juridique dans la société de l'information. Avec les débats portant sur la loi de programmation militaire, un article spécifique (20) a suscité une vague de protestations parmi les organisations professionnelles et militantes de l'Internet. Mais que vient faire cet encadrement de l'interception administrative des données de connexion qui a vocation à être élargi ? « La rédaction de l'article 20 'particulièrement floue' permet d'envisager des questions prioritaires de constitutionnalité ou une révision du texte dans les années à venir », estime le Clusif. Alors qu'un Net-entrepreneur expérimenté (premier Président du Conseil national du Numérique, actuel représentant de la France devant la Commission européenne sur les enjeux numérique), évoque un premier pas vers une dictature numérique. Dans le dernier projet de loi examiné par le Parlement portant sur la géolocalisation dans les affaires pénales, l'avis consultatif de la CNIL pour réviser l'approche n'a pas été réellement suivi.
On peut également s'interroger sur ce qu'il va advenir de la révision de la directive sur la protection des données personnelles, actuellement soumis aux gouvernements. L'Union européenne devrait adopter le nouveau cadre en 2014, « mais ce délai semble compromis », estime le Clusif. Ce projet divise les acteurs du secteur du numérique, mais aussi les pays membres, voire oppose les autorités nationales de protection des données personnelles à la Commission européenne.

4) Hacktivisme : ne réveillez pas l'ours qui dort ?

Selon un constat dressé par le Clusif, le mouvement des Anonymous a perdu de sa force. De nombreuses interpellations dans le réseau hacktiviste se sont produites aux États-Unis dans le courant de l'année 2013. Elles ont découragé ses sympathisants. Et toujours selon les révélations d'Edward Snowden, sur la foi de documents de la NSA datant de 2012, les services secrets britanniques (GCHQ) ont mené plusieurs actions contre des membres d'Anonymous, de LulzSec et de la Syrian Electronic Army.

5) Vol de données numériques : la plaie parfois béante

Difficile de ne pas évoquer deux grandes déperditions massive de données sur le courant de l'année 2013, l'affaire de l'éditeur de logiciels Adobe a fait couler beaucoup d'encre : des fichiers contenant 152 millions de comptes évaporés sur le Web (2,9 millions d'internautes avaient laissé leurs coordonnées bancaires). Dans le domaine de la grande distribution, le cas de l'enseigne américaine Target a également marqué les esprits : les données bancaires de plus de 110 millions de personnes auraient été dérobées à la suite d'un assaut.

En France, où la loi du silence est pourtant souvent la règle, Orange a récemment admis le vol de données personnelles de 800 000 de ses clients.

6) Ramsonware, le chantage à l'ère numérique

La gendarmerie française sait de quoi il s'agit et la tendance est confirmée par le Clusif : l'utilisation croissante des « ransomwares » du nom de programmes qui chiffrent les données et verrouillent les postes de travail des utilisateurs. Pour retrouver la liberté d'accès, il faut payer une rançon. Faute de versement, les données seront détruites. En mars 2013, la Haute autorité pour la diffusion des œuvres et de protection des droits sur Internet (Hadopi) était devenue le prétexte pour la diffusion d'un « rançongiciel ». L'utilisateur était accusé de télécharger illégalement des œuvres. Par conséquent, il devait payer pour reprendre le contrôle de son ordinateur. Selon un article du Figaro daté du 28 janvier 2013, plus de 1280 plaintes ont été déposées en France contre ce type d'arnaque depuis novembre 2011. Un dossier bien suivi par des experts comme le colonel Éric Freyssinet, chef de la division de lutte contre la cybercriminalité de la gendarmerie. Désormais, l'emploi de ces ransomwares se diversifie sur les plateformes Mac et Android.

7) Cyber-criminalité : EC3, « vigie-pirate » en Europe

Au-delà des autorités compétentes dans les 28 Etats membres, l'Union européenne a inauguré début 2013 l'EC3, une cellule anti-cybercriminalité à La Haye (Pays-Bas) qui n'a pas de vocation à enquêter à la place des polices nationales. En revanche, l'European Cybercrime Centre (EC3) a vocation à « aider à surpasser les cyber-criminels en intelligence et en vitesse afin de prévenir et de combattre leurs actes », a expliqué Troels Oerting, directeur du centre de veille pour faciliter la traque des organisations commercialisant des images de pédophilie, se livrant au « phishing » et aux arnaques en ligne diverses et variées.

8) Malaise avec les malwares sur mobile

On ne cesse de répéter qu'Android est la plateforme OS mobile favorite des pirates. « Nous voyons presque 2 000 nouvelles variantes de malwares par jour sur des échantillons Android. Il y a un an, on n'en recensait que 50 par jour. Cela va très vite et la tendance va s'accentuer », considère Ondrej Vlček, le directeur technique d'Avast. Selon le Clusif, Obad.a est l'un des malwares sur système Android les plus sophistiqués du moment.

9) Monnaies virtuelles, dangers réels

Incontestablement, l'année 2013 a été celle du bitcoin du nom de cette monnaie P2P qui dispose de partisans résolument acquis à la cause mais aussi de détracteurs puissants (comme la Banque de France). Si le mécanisme bitcoin séduit, son écosystème est loin d'être stable. Des failles de sécurité au niveau des plateformes des intermédiaires ont entraîné de véritables hold-up à l'ère numérique. Et les doutes sur des possibles canaux de blanchiment d'argent demeurent, malgré la fermeture par le FBI de Silk Road surnommé l'Amazon de la drogue au regard des trafics observés sur cette plateforme underground acceptant le bitcoin comme monnaie d'échange. La récente interpellation du vice-président de la Bitcoin Foundation risque encore de diminuer la crédibilité du système. D'autres monnaies virtuelles comme Liberty Reserve, tout aussi suspectes aux yeux des autorités américaines, ont été bloquées

10) Objets connectés : trendy mais risky

Voitures, montres, lunettes, brosse à dents, thermostats…Bienvenue dans le monde du tout connecté. Mais des experts en sécurité avertissent des risques associés à l'essor des capteurs sur les vêtements, les accessoires de modes et autres exploitations pour le quotidien, les loisirs ou le travail. Au-delà des webcams piratées, des proofs of concept montrent que les Google Glass pourraient être détournées à l'insu des porteurs des lunettes connectées. Récemment, un cas de frigo connecté transformé en relais zombie a été signalé. Dans une tribune diffusé sur Wired, Bruce Schneier, expert en sécurité IT, considère qu'il faut s'interroger sur le réel degré de sécurité des systèmes embarqués, comme l'Internet des objets « criblé de vulnérabilités et pour lequel il n'existe pas de méthode pour patcher les logiciels employés ».

Credit photo : Kheng Guan Toh / Shutterstock.com

En complément :

– Toute l'actualité de la sécurité sur Silicon.fr