Thierry Berthier
Maître de Conférences en mathématiques à l'Université de Limoges, chercheur au sein de la Chaire de cybersécurité & cyberdéfense Saint-Cyr – Thales -Sogeti

LES BLOGS

Armée électronique syrienne: quelles motivations et quel mode de fonctionnement?

INTERNATIONAL - Dès le début du conflit syrien en 2011, une armée électronique syrienne (SEA) a été créée par les soutiens de Bachar El Assad dans le but de "contrer sur le cyberespace l'agression internationale dont est victime la nation syrienne".

15/02/2015 10:16 CET | **Actualisé** 05/10/2016 03:03 CEST

Il n'existe désormais plus aucun conflit, plus aucune guerre, révolte ou insurrection qui ne se projette immédiatement sur l'espace numérique. L'actualité nous démontre quotidiennement que le cyberespace focalise en lui toutes les tensions, les concurrences, les haines et les duels idéologiques humains. Dernièrement, c'est l'Ukraine qui a été la cible de violentes cyberattaques visant ses intérêts numériques. Ces agressions ont rapidement été attribuées à la Russie, avec comme toujours dans ce cas, une réelle difficulté à apporter une preuve tangible et indiscutable de l'origine de l'attaque. L'affaire du hacking (a priori commercial) de Sony Pictures a très vite pris une tonalité géopolitique avec la mise en accusation quasi immédiate de la Corée du Nord par le gouvernement américain comme étant l'État responsable de cette cyber-opération spectaculaire. Comme on peut l'imaginer, le conflit syrien n'échappe pas à cette règle de projection sur l'espace numérique.

La projection numérique du conflit syrien

Dès le début du conflit syrien en 2011, une armée électronique syrienne (SEA) a été créée par les soutiens de Bachar El Assad dans le but de « contrer sur le cyberespace l'agression internationale dont est victime la nation syrienne ». Plus qu'une simple extension de territorialité, l'espace numérique apporte des fonctionnalités nouvelles, puissantes et procure aux acteurs des conflits modernes des effets de leviers particulièrement efficaces. La SEA est, en ce sens, un modèle de structure inédite

capable d'adapter en temps réel sa « cyber-hacktivité » à l'actualité du conflit et à ses contraintes stratégiques. Entre 2011 et 2014, ce sont des centaines de sites web occidentaux qui ont été touchés par ses attaques par défacement (le défacement désigne une attaque de basse intensité consistant à modifier la page d'accueil d'un site en y apposant un message de revendication de l'attaque). La SEA a également ciblé de nombreux comptes twitter officiels avec parfois des conséquences systémiques en cascade, non prévues par l'attaquant. Ainsi, le 23 avril 2013, la SEA prenait le contrôle du compte twitter officiel de l'agence Associated Press et publiait le message « Breaking : Two explosions in the White House and Barack Obama is injured ». Ce faux tweet provoquait alors en moins de cinq minutes la chute vertigineuse des principaux indices boursiers mondiaux et des turbulences financières à hauteur de 136 milliards de dollars, avant que l'agence de presse ne reprenne le contrôle de son compte et ne publie un démenti. L'échelle temporelle avait été parfaitement compatible avec la stratégie des hackers de la SEA et leur avait permis de déstabiliser, au delà de leurs espérances et à peu de frais, l'ensemble des marchés sur une courte période. La SEA a également ciblé des systèmes de paiement en ligne comme Paypal et a procédé au vol de données bancaires de comptes clients. Elle a maintenu une pression constante sur les sites de la rébellion syrienne et a cherché à en identifier les membres actifs sur le cyberespace. En tant que cellule opérationnelle de hacking, elle a su faire preuve d'une grande cohérence dans son action en ciblant successivement la plupart des médias occidentaux selon un rythme parfaitement planifié. Lorsqu'elle jugeait que ces médias ne rapportaient pas la situation de manière satisfaisante, elle le faisait savoir par une opération de hacking d'influence et par des communiqués justifiant cette opération. Entre 2011 et 2013, la communauté occidentale a soutenu sans réserve la rébellion syrienne modérée et a même envisagé des frappes aériennes contre le régime syrien en 2013. Durant cette période, l'activité de la SEA a atteint sa vitesse de croisière en produisant une attaque toutes les 48 heures sur des cibles visibles et emblématiques occidentales. En 2014, lorsque l'éventualité d'une intervention occidentale s'est éloignée durablement, la SEA a diminué l'intensité et le rythme de ses cyberattaques sur les intérêts numériques occidentaux et a concentré ses agressions numériques sur le Qatar, l'Arabie Saoudite et la Turquie qui représentaient de fait le premier cercle de ses ennemis. Alternant les périodes offensives et les pauses tactiques, la cellule a diversifié ses activités en allant jusqu'à construire et diffuser une distribution Linux « maison » intitulée SEANux. Elle a ensuite rendu publics des documents confidentiels collectés durant ses opérations de hacking menées durant la période 2011-2013.

La guerre des données

Le site « SEA Leaks » a été spécialement conçu pour mettre en ligne l'ensemble des données collectées par la SEA durant ses nombreuses attaques. La diffusion des données captées a débuté en novembre 2012 avec la publication d'un ensemble de fichiers confidentiels de la ligue des pays arabes (LAS) et de ses responsables, soit 71 messages accompagnés de leurs pièces jointes. En janvier 2013, ce sont 519 messages et fichiers « Qatar » qui ont été mis en ligne sur le site de la SEA répartis dans quatre catégories : Ministère des affaires étrangères du Qatar, Forces armées du Qatar, Amiri Diwan, et Moza Bint Office. Les courriers électroniques diffusés datent de 2012 et présentent tous un caractère officiel et confidentiel.

Le 7 février dernier, la SEA a mis en ligne sur son site deux ensembles de données confidentielles qui concernent cette fois l'Arabie Saoudite (5 catégories, 367 messages et pièces jointes) et la Turquie (14 catégories, 967 messages et leurs pièces jointes). On retrouve les cibles privilégiées de la SEA : le Ministère des affaires étrangères, le Ministère de la Défense, les industries de défense, des personnalités de premier plan du gouvernement dont le Premier Ministre. Les messages, souvent classifiés, datent de 2012 et 2013. Des échanges en marge de contrats d'armement assortis de pièces jointes contenant des catalogues de munitions et de matériels militaires américains et européens sont disponibles au téléchargement. Des échanges classifiés entre des chancelleries européennes et le gouvernement turc figurent aussi en grand nombre dans les messages piratés. Il est possible de lire sans aucune restriction des courriers échangés entre diplomates anglais, allemands, français et turcs...

Cette mise en ligne massive démontre, une fois de plus, la fragilité et la vulnérabilité de nos systèmes de messageries électroniques utilisés en particulier lors d'échanges diplomatiques. Même si les communications sensibles sont sécurisées, rien ne dit que le correspondant n'est pas lui même victime d'une attaque furtive et que ses échanges ne sont pas systématiquement collectés. L'attaquant a toujours l'avantage sur la défense, c'est ce que démontre le tour de force actuel de la SEA...

Lire aussi :

» Lutte contre le terrorisme : L'UE teste sa détermination à agir rapidement

» Ukraine, Irak, Soudan... la carte des réfugiés des conflits de 2014

» La Turquie bombarde des positions kurdes du PKK sur son propre sol

» Pour suivre les dernières actualités en direct sur Le HuffPost, cliquez ici

Retrouvez les articles du HuffPost sur notre page Facebook.