Analyse d'une guerre sur Internet
Avril 2007, attaque de l'Estonie

Olivier Ricou

20 mai 2016

En 2007 l'Estonie, un ancien pays du bloc soviétique d'un peu plus d'un million d'habitants, subit une attaque informatique importante qui met à mal son infrastructure informatique. Pour ce pays le mieux connecté d'Europe l'arrêt du fonctionnement de banques, de l'administration et d'autres service suite à cette attaque a été un choc majeur. Depuis l'OTAN dont fait parti l'Estonie a pris le problème de la cyber-guerre à bras le corps et a mis en place un centre de recherche en cyber-défense à Tallinn.

1 Le contexte

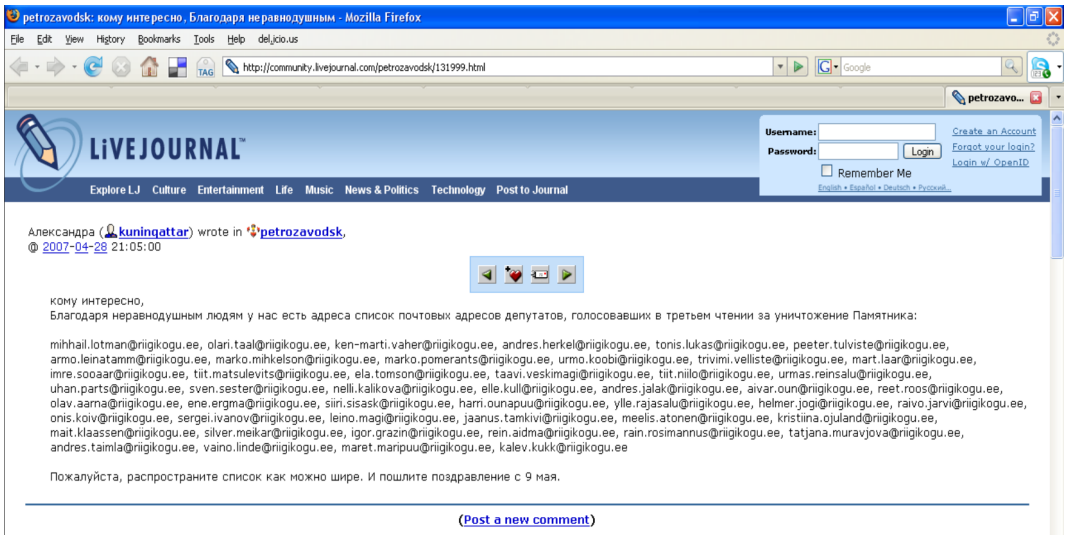
En avril 2007 le gouvernement estonien décide de déplacer la statue du *Soldat de bronze* qui représente la libération du joug nazi par l'Armée rouge en 1944. Cette statue en plein centre ville n'était pas trop apprécié par les lituaniens qui y voyaient plus le symbole de l'occupation russe que celui d'une libération. Par contre pour la forte minorité russophone d'Estonie, environ 25% de la population, cette statue représente le combat soviétique contre les nazis.

La décision a donc soulevé des vagues de protestations tant de la part de la minorité russophone que des russes. Le 26 avril des manifestations liées font un mort et de nombreux blessés. Le lendemain les cyber-attaques commencent.

2 Les cyber-attaques

Les cyber-attaques utilisées en Estonie ont été principalement des dénis de service[1]. Ces dénis consistent à soumettre tellement de requêtes à des serveurs que ces derniers ne peuvent plus répondre et s'effondrent sous la charge. Un raffinement consiste à soumettre des requêtes compliquées voire illogiques qui augmentent la tache du serveur et donc augmentent la charge. Pour soumettre assez d'attaques une technique utilisées a été celle des botnets, à savoir des virus dormants installés sur des ordinateurs de personnes ordinaires que l'on peut activer à distance. Il est ainsi possible de les activer tous ensemble afin qu'ils se connectent tous en même temps vers les cibles. Ainsi des centaines de milliers de botnets de plus de 50 pays, donc les États-Unis, ont envoyé des attaques sur les serveurs estoniens.

Les dénis de service peuvent être aussi de simples mails envoyés par millions à des adresses bien déterminées comme celles des députés listées dans un document partagé par on ne sait qui mais largement utilisé :



Les cibles de la cyber-attaque de 2007 contre l'Estonie ont été :

- le parlement, les sites ministériels, le parti politique au pouvoir,
- les journaux principaux
- les deux plus grandes banques dont la Hansabank
- des universités,
- les infrastructures télécom du pays, le FAI[2] du gouvernement.

[1] Denial of Service en anglais, DoS
[2] Fournisseur d'Accès Internet

Les attaques ont commencé relativement doucement pour atteindre un pic le 9 mai avec 4 millions de paquets à la seconde répartis sur quelques centaines de serveur estoniens.

Dans un pays aussi connecté que l'Estonie cela a eu des conséquences terribles. Ainsi les clients de l'Hansabank n'avait plus accès à leur compte via Internet, service utilisé par 97% des clients, mais aussi le système de vérification des transactions était hors service ce qui a perturbé fortement le fonctionnement des distributeurs de billets et a bloqué les connexions avec les banques à l'étranger donc interdit aux clients de cette banque à l'étranger d'utiliser leur carte de paiement. Les services institutionnels étaient bloqués pour un grand nombre et l'infrastructure télécom elle même a été touchées à des endroits pourtant pas connus du grand public normalement.

La défense estonienne a mis en place une cellule de crise pour gérer la défense. Cette cellule a obtenu l'aide de pays étrangers comme l'Allemagne, l'Italie ou l'Espagne et bien des pays baltes voisins la Lituanie et la Lettonie. Elle a aussi été assistée par les FAI étrangers qui ont bien voulu couper la communication aux ordinateurs les plus agressifs qui passaient sur leur réseaux. Mais surtout, après 3 semaines d'attaques et de chaos, le gouvernement estonien a pris la décision de couper les connexions à l'international ce qui a coupé l'Estonie de l'Internet mais ce qui a réussi à réduire assez les attaques pour réagir et remettre en état le réseau.

Le 19 mai les attaques ont arrêté.

3 Les responsabilités

Si la coordination des attaques était visible sur des sites web russe où il était indiqué les adresses IP des cibles et les dates des attaques, rien n'indiquait a priori que le gouvernement russe était aux commandes. Des activistes auraient pu être à l'initiative des attaques comme, plus tard, les Anonymous l'ont fait lors de l'Operation Payback contre les entreprises ayant, de leur propre initiative, bloqué les comptes de Wikileaks.

Cependant l'ampleur de l'attaque et son excellente coordination rendent plus probable l'implication des autorités russes avec a priori au moins un accord implicite de la présidence. Le gouvernement estonien a déclaré avoir relevé des adresses IP d'ordinateurs de l'administration centrale russe parmi les attaquants. Pour l'Estonie, l'implication de la Russie est évidente.

Mais aujourd'hui il n'y a toujours pas de preuve formelle du niveau d'implication des autorités russes. De plus ces dernières ont toujours déclaré officiellement ne pas être liées à ces attaques. Seuls des officiels russes ont déclarés en leur nom que tel ou tel groupe d'activistes avait mené l'attaque avec eux, mais rien de convainquant a priori.

On trouve ici une caractéristique de la cyber-guerre, l'agresseur préfère garder l'anonymat même s'il peut avoir de forts soupçons, qui d'ailleurs peuvent arranger l'agresseur.

4 Les réactions

La statue a été transférée dans le cimetière militaire où les autorités estoniennes l'avaient décidé[3].

L'Estonie a profité de l'ampleur de l'attaque pour s'afficher en victime et bénéficier de la sympathie occidentale. Elle a pu également se servir de l'évènement pour pousser sa demande de cyber-défense au niveau de l'OTAN.

En 2008 le Centre d'Excellence de Coopération en Cyber Défense de l'OTAN a été créé à Tallinn. Les pays qui ont aidé l'Estonie durant la crise on rejoint le centre dès le début. Les États-Unis l'on rejoint en 2011, la France et l'Angleterre en 2014. Son but est de partager entre ses membres les connaissances en cyber-défense.

Tant à travers ce centre que par des accords avec les entreprises privées et les citoyens, l'Estonie a depuis développé sa cyber-défense. Un des éléments visibles est la réserve citoyenne d'informaticiens certifiés par l'OTAN qui peut être mobilisée en cas de nouvelle cyber-guerre.

Sources

- Antoine Chalvin, *L'ombre du soldat de bronze*, Le courrier des pays de l'Est 2007, https://www.cairn.info/revue-le-courrier-des-pays-de-l-est-2007-4-page-6.htm
- Jason Richards, *Denial-of-Service : The Estonian Cyberwar and Its Implications for U.S. National Security*, International Affairs Review, http://www.iar-gwu.org/node/65
- *Estonia Cyber Attacks 2007*, meeting Afrinic 2011, https://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf
- *Cyber attacks, NATO - and angry birds*, NATO review magazine 2013, http://www.nato.int/docu/review/2013/Cyber/Cyber-attacks-NATO-angry-birds/FR/index.htm
- *L'Estonie accueille le premier centre de cyberdéfense*, Le Monde 2008, http://www.lemonde.fr/europe/article/2008/05/26/l-estonie-accueille-le-premier-centre-de-cyberdefense_1049705_3214.html

[3] contrairement à ce que j'avais toujours pensé, comme quoi voila un rapport utile.