Simply Voting

5253 Decarie Boulevard, Suite 250
Montreal, QC, H3W 3C3 Canada
1 (800) 585-9694

Mémoire de Simply Voting présenté au Comité spécial sur la réforme électorale

Présenté par Brian Lack,
le 20 septembre 2016

Contexte

1. Simply Voting inc. est une société de Montréal qui offre des services complets et sécurisés de vote par Internet. L'entreprise compte plus de 1 000 clients dans de nombreux secteurs tels que des universités, des associations, des syndicats, des partis politiques et des collectivités de Premières Nations. Tous les jours, elle gère simultanément une centaine d'activités de vote et n'a jamais été victime d'un incident de sécurité.

2. D'ailleurs, mentionnons au Comité que Simply Voting a offert un service de vote par Internet et par téléphone à plusieurs municipalités lors des élections municipales de 2014 en Ontario. De plus, le plébiscite sur le renouvellement démocratique à l'Île-du-Prince-Édouard se fera sur sa plateforme; il s'agira du premier scrutin provincial par Internet dans toute l'Amérique du Nord.

3. Le président et fondateur de Simply Voting inc., Brian Lack, a développé son premier système de vote en ligne en 2003. Il est titulaire d'un baccalauréat ès sciences de l'Université McGill.

Une menace élevée

4. Actuellement, le vote par Internet a été utilisé au Canada lors d'élections municipales en Ontario et en Nouvelle-Écosse. La technologie de vote s'est révélée un succès. Chaque cycle d'élection amène de plus en plus de municipalités qui en font l'essai. On prévoit que le nombre de provinces qui permettront le vote par Internet augmentera dans l'avenir.

5. Toutefois, plus le nombre de votes par Internet augmentera, plus le risque d'attaques s'intensifiera. Les pouvoirs économiques et politiques du gouvernement fédéral sont considérablement plus importants que ceux des administrations municipales. Les budgets de campagne dans le cadre d'élections fédérales sont gigantesques par rapport à ceux des campagnes

municipales; ils s'élèvent souvent à des dizaines de millions de dollars[1]. Les enjeux lors des élections fédérales sont également bien plus importants. Les candidats, les partis, les sympathisants, les parties intéressées et même le crime organisé déploient donc des ressources importantes pour en influencer le résultat et pourraient être tentés d'attaquer le système de vote.

6. Même des entités externes s'intéressent aux résultats des élections fédérales. Le crime organisé à l'étranger, des groupes de pirates informatiques comme Anonymus, la Russie, la Chine et même la National Security Agency des États-Unis sont tous des puissances dans la guerre de l'information. D'ailleurs, les systèmes d'inscription au vote électronique en Arizona et en Illinois ont récemment été piratés par de présumés acteurs étrangers. Cet exemple nous montre que la menace est bien réelle[2].

7. En appliquant d'importantes ressources technologiques, un pirate peut profiter des vulnérabilités ci-dessous du système de vote par Internet. Ces vulnérabilités sont attribuables aux limites de la technologie Web en général et ne sont pas le propre du système de vote par Internet.

Logiciel malveillant ciblé

8. Un logiciel malveillant est un programme destiné à nuire à un système informatique en infectant un ordinateur à l'insu et contre la volonté du propriétaire. Certains logiciels malveillants, comme le ver informatique Stuxnet qui a détruit les centrifugeuses iraniennes d'enrichissement d'uranium[3], sont conçus pour viser une cible et un objectif en particulier. Il serait donc possible qu'un logiciel malveillant soit développé spécifiquement pour détourner un vote en particulier du système de vote par Internet. Par exemple, si un électeur se connecte au système de vote par Internet à partir d'un ordinateur infecté et clique sur le candidat A, le logiciel malveillant remplacerait le vote par un vote pour le candidat B, et ce, sans que l'électeur le sache.

9. Pour que le logiciel malveillant puisse réellement changer l'issue du vote, il doit être installé sur un nombre suffisant d'ordinateurs utilisés par les électeurs. Le logiciel peut se propager de lui-même, ou un pirate seul peut prendre le contrôle de tous les ordinateurs grâce à un réseau de zombies

[1] https://fr.wikipedia.org/wiki/Financement_des_partis_politiques_au_Canada
[2] http://www.theverge.com/2016/8/29/12692756/voter-registration-hack-arizona-illinois-election- security
[3] https://fr.wikipedia.org/wiki/Stuxnet

(botnet) composé de nombreux ordinateurs personnels infectés par un certain virus informatique. De grands réseaux de zombies qui comprennent des centaines de milliers d'ordinateurs existent réellement[4]. Souvent, ils sont utilisés à des fins de pollupostage, d'attaques par déni de service et d'activités frauduleuses. Il serait facile pour un pirate d'utiliser un grand réseau de zombies et d'installer un logiciel malveillant sur les ordinateurs.

10. Peu importe le niveau de perfectionnement du système de vote par Internet sur le plan de la sécurité, les ordinateurs à partir desquels sont enregistrés les votes ne peuvent être sécurisés. Ce type d'attaque est très difficile à détecter et encore plus à stopper, sauf si des codes de vote personnalisés sont utilisés. Toutefois, ces codes nuisent à la commodité et à l'accessibilité, deux arguments en faveur du vote par Internet.

Vulnérabilités aux attaques du jour zéro

11. Les pratiques exemplaires en matière de sécurité Internet sont appliquées aux systèmes de vote par Internet de pointe, ce qui permet de les protéger en général contre les techniques connues de piratage. Le réel danger provient des techniques de piratage appelées « attaques du jour zéro ». Les cybercriminels et les services du renseignement découvrent, recueillent et exploitent les vulnérabilités aux attaques du jour zéro qui pourraient servir à accéder aux serveurs ou à décrypter les données chiffrées[5]. À titre d'exemple, le ver informatique Stuxnet mentionné précédemment a utilisé plusieurs vulnérabilités aux menaces du jour zéro pour attaquer efficacement sa cible.

12. Il est extrêmement difficile pour les services en ligne de se protéger contre des menaces inconnues et aucun serveur Internet ne peut être totalement sécurisé. Lorsqu'une vulnérabilité aux attaques du jour zéro est exploitée, elle devient connue de la communauté de la sécurité et devient par le fait même moins puissante. Les pirates ne gaspilleront donc pas une attaque du jour zéro sur une cible d'une faible valeur. Une élection fédérale demeure toutefois une cible de grande valeur.

Conclusion

13. Malgré le fait que Simply Voting est une entreprise canadienne et un

[4] https://fr.wikipedia.org/wiki/Botnet
[5] https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_Zero_day

5253 Decarie Boulevard, Suite 250
Montreal, QC, H3W 3C3 Canada
1 (800) 585-9694

important fournisseur de systèmes de vote par Internet, il recommande de **ne pas utiliser le vote par Internet aux élections fédérales**. Le degré élevé de menaces lors des élections fédérales nécessite un niveau de sécurité que le vote par Internet ne peut offrir. Les risques sont trop grands.

14. Cependant, il est à noter que le **vote par Internet est une excellente solution** pour les plébiscites, les élections territoriales et municipales ainsi que les élections des Premières Nations puisque les mesures de sécurité sont extrêmement élevées par rapport au niveau de la menace. Si le Comité conclut que le vote par Internet n'est pas suffisamment sûr pour les élections fédérales, il serait important d'apporter des réserves à la recommandation et de ne pas indiquer que la technologie comporte des failles ou est inutilisable en général.