Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Décision de Conformité et Enquêtes CRTC 2022-132

Version PDF

Ottawa, le 19 mai 2022

Numéros de dossiers : 9094-201500417-001 et 9094-201500417-002

1882914 Ontario Inc., faisant affaire sous le nom de Datablocks Inc., et 2348149 Ontario Inc., faisant affaire sous le nom de Sunlight Media Networks Inc. – Violations présumées de la Loi canadienne anti-pourriel

Le Conseil détermine que les éléments de preuve au dossier de la présente instance ne sont pas suffisants pour conclure que 1882914 Ontario Inc., faisant affaire sous le nom de Datablocks Inc., et 2348149 Ontario Inc., faisant affaire sous le nom de Sunlight Media Networks Inc., ont aidé à sept installations d'un programme d'ordinateur sur l'ordinateur d'une autre personne sans le consentement exprès du propriétaire ou d'un utilisateur autorisé. Par conséquent, conformément à l'article 25 de la Loi canadienne anti-pourriel (LCAP), le Conseil détermine qu'aucune violation de l'article 9 de la LCAP n'a été commise et, par conséquent, les sanctions administratives pécuniaires énoncées dans les procès-verbaux de violation ne seront pas imposées.

Introduction

1. En 2015, le personnel d'enquête du Conseil a recensé cinq adresses de protocole Internet (IP) canadiennes liées à 1882914 Ontario Inc., faisant affaire sous le nom de Datablocks Inc. (Datablocks), et 2348149 Ontario Inc., faisant affaire sous le nom de Sunlight Media Networks Inc. (Sunlight Media) [collectivement les entreprises] qui semblaient rediriger les utilisateurs vers des pages Web hébergeant des trousses d'exploit[1].

2. Sunlight Media[2] exploitait un réseau publicitaire en ligne et servait de courtier entre les annonceurs et les éditeurs de telles publicités. Sunlight Media a utilisé le logiciel et l'infrastructure de routage de réseau de Datablocks, qui permettent la diffusion de publicités en ligne grâce à un système d'enchères en temps réel entièrement automatisé.

3. Au cours de l'enquête approfondie du personnel d'enquête du Conseil, un avis de communication a été émis en juin 2016 à Services partagés Canada (SPC) afin

[1] Le Centre canadien pour la cybersécurité décrit un exploit comme « un code malveillant qui permet de tirer avantage d'une vulnérabilité non corrigée. Une " trousse d'exploit " est une collection d'exploits qui ciblent les applications logicielles non sécurisées. Les trousses d'exploit sont adaptées de manière à chercher des vulnérabilités spécifiques et à exécuter l'exploit correspondant à la vulnérabilité relevée. »

[2] Sunlight Media a achevé sa dissolution volontaire le 16 novembre 2018.

d'obtenir des renseignements et des données concernant le trafic dirigé vers ou depuis les adresses IP du gouvernement du Canada (GC) et les cinq adresses IP d'intérêt. L'objectif de l'avis de communication était également d'obtenir tous les fichiers de capture de paquets réseau (fichiers pcap)[3] et les échantillons de logiciels malveillants (échantillons de fichiers pcap) liés aux cinq adresses IP concernées.

4. Le 9 juillet 2018, le chef de la conformité et des enquêtes (personne désignée[4]) a dressé un procès-verbal de violation à Sunlight Media et à Datablocks, en vertu de l'article 22 de la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications* (Loi canadienne anti-pourriel [LCAP]). Les procès-verbaux de violation peuvent faire l'objet d'une révision indépendante par le Conseil.

5. Dans les procès-verbaux de violation, la personne désignée a informé les entreprises qu'il y avait des motifs raisonnables de croire qu'entre le 8 février 2016 et le 30 mai 2016, les entreprises ont chacune commis une violation de l'article 9 de la LCAP, en contribuant, par leurs actes et omissions, à sept actes contraires au paragraphe 8(1) de la LCAP, à savoir l'installation, par une personne inconnue, d'un programme d'ordinateur sur l'ordinateur d'une autre personne sans son consentement exprès.

6. Plus précisément, la personne désignée a indiqué que dans sept cas, le domaine de Sunlight Media a fourni des instructions directes à un ordinateur du GC pour qu'il se connecte à un serveur, lequel a installé à son tour un programme d'ordinateur malveillant sur l'ordinateur du GC sans son consentement exprès.

7. La personne désignée a également conclu que Datablocks a fourni à Sunlight Media le logiciel et l'infrastructure qui ont permis aux clients de Sunlight Media de participer au processus d'enchères en temps réel.

---

[3]Les fichiers pcap font référence à l'interception de paquets de données lors de leur déplacement sur un réseau informatique pendant une période donnée.

[4]En vertu de l'article 14 de la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications,* le Conseil peut désigner des personnes pour exercer les pouvoirs liés aux objectifs des articles 15 à 46, ce qui comprend la délivrance de procès-verbaux de violation.

8. Les procès-verbaux de violation, qui étaient chacun accompagnés du rapport d'enquête de la personne désignée et des preuves recueillies au cours de l'enquête, prévoyaient une sanction administrative pécuniaire (sanction) de 150 000 $ pour Sunlight Media et de 100 000 $ pour Datablocks.

9. Dans leurs observations conjointes datées du 24 septembre 2018, les entreprises ont argué, entre autres, que le rapport d'enquête et les éléments de preuve fournis à l'appui des conclusions de la personne désignée ne démontraient pas que les entreprises avaient commis une quelconque violation de la LCAP. Les entreprises ont également présenté un rapport d'expert qu'elles ont commandé. Sur la base de ce rapport, les entreprises ont soutenu que l'analyse technique et les preuves numériques figurant au dossier ne prouvaient pas les installations présumées, par une personne inconnue, de programmes d'ordinateur malveillants.

10. En 2019, le Conseil a retenu les services d'un expert externe en informatique judiciaire (spécialiste externe) pour l'aider à mieux comprendre les arguments techniques et les preuves numériques inclus dans le dossier de la présente instance (rapport d'expertise externe), indépendamment des preuves soumises par la personne désignée et les entreprises.

11. Dans une lettre datée du 18 août 2020, le Conseil a ajouté le rapport d'expertise externe au dossier de l'instance de révision et a donné à la personne désignée l'occasion de commenter le rapport d'expertise externe, tout en donnant aux entreprises l'occasion de répondre aux commentaires de la personne désignée et le rapport d'expertise externe.

12. Dans une lettre ultérieure datée du 22 décembre 2020, le Conseil a précisé que les commentaires devaient se limiter à la méthodologie et aux outils utilisés par le spécialiste externe pour évaluer les preuves numériques, ainsi qu'aux constatations d'ordre technique et aux conclusions fondées sur ces preuves[5].

13. En plus des lettres procédurales mentionnées ci-dessus, le dossier de la présente instance contient ce qui suit :

    - les procès-verbaux de violation émis à l'endroit des entreprises le 9 juillet 2018;
    - un rapport d'enquête exposant les preuves, l'analyse et les conclusions de la personne désignée à l'appui des procès-verbaux de violation;
    - les observations conjointes faites par les entreprises le 24 septembre 2018 pour répondre aux procès-verbaux de violation qui incluaient un rapport d'expert;
    - le rapport d'expertise externe commandé par le Conseil;

[5] Le Conseil a tenu compte de ces restrictions lorsqu'il a examiné les mémoires des entreprises et de la personne désignée soumis en réponse à cette lettre et dans son analyse et ses conclusions dans la présente décision.

- les commentaires de la personne désignée sur le rapport d'expertise externe et la réponse des entreprises sur le rapport et les commentaires de la personne désignée.

14. Le dossier a été fermé le 16 février 2021.

15. En vertu de l'article 25 de la LCAP, si une personne présente des observations conformément à un procès-verbal de violation, le Conseil doit décider, selon la prépondérance des probabilités, si la personne a commis la violation et, le cas échéant, si elle doit imposer, réduire, annuler ou suspendre la pénalité, sous réserve des conditions qu'il estime nécessaires pour assurer la conformité.

Question

16. Le Conseil a établi qu'il devait examiner la question suivante dans la présente décision :

    - Le dossier de l'instance étaye-t-il les conclusions des procès-verbaux de violation, selon lesquelles les entreprises ont aidé, en violation de l'article 9 de la LCAP, à commettre des actes contraires au paragraphe 8(1) de la LCAP, à savoir l'installation d'un programme d'ordinateur?

17. Pour que le Conseil puisse parvenir à une conclusion sur toute violation de l'article 9, il doit d'abord déterminer si au moins une des sept installations d'un programme d'ordinateur a eu lieu en contravention au paragraphe 8(1) de la LCAP. Si le Conseil ne parvient pas à conclure, selon la prépondérance des probabilités, qu'un programme d'ordinateur a été installé, il ne serait pas possible de conclure que les entreprises ont violé l'article 9 de la LCAP.

18. De plus, avant de déterminer si un programme d'ordinateur a été installé, le Conseil doit établir si les fichiers Shockwave Flash constituent des « programmes d'ordinateur » au sens du paragraphe 1(1) de la LCAP. Le sens du mot « installation » dans le contexte de l'expression « installation d'un programme d'ordinateur » énoncée au paragraphe 8(1) de la LCAP doit également être déterminé dans les circonstances particulières de la présente instance de révision, puisque la LCAP ne fournit pas de définition pour « installer » ou « installation ».

Programmes d'ordinateurs présumés qui sont identifiés dans les procès-verbaux de violation

19. Le Conseil fait remarquer que l'expression « programme d'ordinateur » est définie au paragraphe 1(1) de la LCAP comme ayant la même signification qu'au paragraphe 342.1(2) du *Code criminel*, qui la définit comme suit :

> ensemble de données informatiques qui représentent des instructions ou des relevés et qui, lorsque traitées par l'ordinateur, lui font exécuter une fonction.

20. De plus, les termes « données » et « ordinateur » que l'on retrouve dans cette définition de programme d'ordinateur sont également définis au paragraphe 1(1) de la LCAP. Plus précisément, le terme « données » est défini comme suit :

> signes, signaux, symboles ou représentations de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur.

21. Quant au terme « ordinateur », la LCAP énonce qu'il a le même sens qu'au paragraphe 342.1(2) du *Code criminel*, qui le définit comme suit :

> dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux : a) contiennent des programmes d'ordinateur ou d'autres données informatiques; b) conformément à des programmes d'ordinateur : (i) exécutent des fonctions logiques et de commande, (ii) peuvent exécuter toute autre fonction.

22. En ce qui concerne les programmes d'ordinateur au cœur de la présente instance, la personne désignée prétend que les entreprises ont aidé à installer des fichiers Shockwave Flash contenant des programmes d'exploitation Flash.

23. Le Conseil fait remarquer que les fichiers Shockwave Flash sont constitués de signes, de symboles et de concepts préparés sous une forme adaptée à une utilisation dans un ordinateur afin de générer des graphiques animés, des vidéos, du son et des interactions avec l'utilisateur sur le Web. Plus précisément, ils sont créés à partir de codes informatiques, qui sont des signes et des symboles représentant des instructions ou des déclarations qui, lorsqu'ils sont interprétés par un module d'extension de navigateur Web ou un autre logiciel compatible tel qu'Adobe Flash Player, affichent le contenu des fichiers Shockwave Flash.

24. Le Conseil souligne également que la personne désignée et les entreprises ont toutes deux reconnu que les fichiers Shockwave Flash sont constitués de données ou de codes informatiques destinés à être exploités ou lus par un module d'extension de navigateur Web ou un autre logiciel compatible, ce qui, selon le Conseil, correspond à la définition de « programme d'ordinateur » énoncée dans la LCAP.

25. Par conséquent, tant les fichiers Shockwave Flash que les programmes d'exploitation Flash (intégrés dans les fichiers Shockwave Flash) constituent, dans le contexte de la présente instance de révision, des programmes d'ordinateur.

Définition du terme « installation » aux fins de la présente instance

26. Comme le Conseil l'a déjà mentionné, la LCAP ne définit pas le terme « installation », ce qui a amené la personne désignée et les entreprises à fournir chacune leur propre définition.

27. Le Conseil fait remarquer que les entreprises ont indiqué qu'il n'existe pas de définition concluante du terme « installer » ou de l'expression « installation de logiciel » dans l'industrie du logiciel, mais que cela signifie généralement rendre un

logiciel prêt à être exécuté. Les entreprises ont également fait valoir que l'installation peut être aussi complexe que l'exécution d'un programme d'installation d'une suite logicielle ou aussi simple que la copie d'un fichier dans la mémoire ou sur le disque dur d'un ordinateur.

28. Le Conseil souligne également que de multiples définitions du terme « installation » peuvent être trouvées dans le rapport d'enquête. Dans l'annexe 1 du rapport, il est défini comme suit :

> l'action de rendre un programme d'ordinateur prêt à être exécuté par un processeur de l'ordinateur. Le processus d'installation peut varier mais, au minimum, l'installation consiste à fournir les instructions du programme à l'ordinateur. Ces instructions se présentent généralement sous la forme d'un code machine qui est copié ou généré. L'installation d'un programme d'ordinateur ne nécessite pas nécessairement un fichier réel stocké de manière persistante sur le disque dur d'un ordinateur. [traduction]

29. Dans l'annexe 9 du rapport d'enquête, il est indiqué que :

> > l'installation peut être effectuée en plaçant silencieusement un code machine sur le disque dur ou la mémoire vive (RAM) d'un ordinateur sans le consentement ou l'avis de l'utilisateur. De là, un programme est ensuite exécuté, par exemple, par le navigateur Web de l'utilisateur. [traduction]

30. Le Conseil fait également remarquer que des éléments communs ont été présentés dans chaque définition et que tant la personne désignée que les entreprises ont reconnu que :

    - l'installation exige que le programme d'ordinateur soit prêt à être exécuté;
    - l'installation d'un programme d'ordinateur peut être effectuée de manière silencieuse en copiant ou en plaçant des fichiers ou des codes sur la mémoire vive (c.-à-d. la mémoire temporaire) ou le disque dur (c.-à-d. la mémoire permanente) d'un ordinateur.

31. En l'absence d'une définition du terme « installation » dans la LCAP, le Conseil estime que ce terme doit être interprété dans son sens grammatical et ordinaire, conformément aux objectifs de la LCAP.

32. Compte tenu des observations et des arguments soumis tant par les entreprises que par la personne désignée, et compte tenu du dossier et des faits propres à l'examen en cause, la définition suivante du terme « installation » doit être utilisée pour déterminer, aux fins de la présente instance, si le dossier démontre, selon la prépondérance des probabilités, qu'un programme d'ordinateur ait été installé :

> rendre un programme d'ordinateur prêt à être exécuté en copiant ou en plaçant des codes informatiques dans la mémoire vive ou le disque dur d'un ordinateur.

33. Le Conseil souligne qu'« ordinateur » et « programme d'ordinateur » dans cette définition ont la même signification que dans la LCAP[6].

34. La définition proposée par la personne désignée utilisait spécifiquement l'expression « codes machine » plutôt que « données informatiques » ou « codes informatiques » sans fournir de justification supplémentaire. Le Conseil fait remarquer que l'expression « codes machine » a une portée limitée, car elle ne s'applique qu'aux fichiers binaires, tels que les fichiers exécutables (.exe) pour Windows, qui sont prêts à être envoyés au processeur de l'ordinateur, ou matériel, par le système d'exploitation. Le Conseil estime que l'utilisation de l'expression « codes informatiques » dans la définition ci-dessus est plus large puisqu'elle englobe les langages de programmation qui sont lus par un logiciel, tel qu'un navigateur Web ou un module d'extension. Cela reflète mieux le libellé général et l'objectif de la LCAP et ne limite pas la définition à un scénario spécifique, comme ce serait le cas si le Conseil utilisait l'expression « codes machine ».

Des programmes d'ordinateur ont-ils été installés, sans consentement exprès, sur les ordinateurs du GC?

35. Le Conseil fait remarquer qu'à la suite de l'analyse des échantillons de fichiers pcap acquis auprès de SPC en réponse à l'avis de communication, la personne désignée a conclu que sept programmes d'ordinateur ont été installés sur des ordinateurs du GC entre le 8 février et le 30 mai 2016. La personne désignée n'a pas prétendu que les entreprises avaient installé les programmes d'ordinateur elles-mêmes, mais qu'elles avaient plutôt aidé des personnes inconnues à installer les sept programmes d'ordinateur sans le consentement exprès du propriétaire de l'ordinateur ou de son utilisateur autorisé.

36. Selon la personne désignée, les preuves numériques ont confirmé que les ordinateurs du GC ont visité des pages de renvoi hébergeant des trousses d'exploit Angler, un type spécifique de trousse d'exploit, qui renvoyaient des programmes d'exploit Flash pour tirer parti de vulnérabilités découvertes dans les versions d'Adobe Flash Player des ordinateurs.

37. Sur la base de l'analyse des preuves numériques figurant dans le dossier, la personne désignée a déterminé que les programmes d'exploitation Flash ont été installés avec succès, ce qui a entraîné le téléchargement ultérieur de deuxièmes programmes par les ordinateurs du GC. Selon la personne désignée, ces deuxièmes programmes constituent la « charge utile »[7] des trousses d'exploit, qui ciblaient le logiciel Adobe Flash Player des ordinateurs.

---

[6]La définition d'ordinateur au paragraphe 342.1(2) du *Code criminel* est large et ne comprend pas seulement des dispositifs individuels, mais aussi un groupe de dispositifs interconnectés ou reliés.

[7] La personne désignée a indiqué que l'expression « charge utile » fait référence au logiciel malveillant dans le cadre de la présente enquête. Toutefois, cette expression fait généralement davantage référence aux données transportées par paquets sur un réseau; ces données ne sont pas nécessairement malveillantes.

38. De plus, pour chaque échantillon de fichiers pcap où l'ordinateur du GC a téléchargé un deuxième programme, la personne désignée a affirmé qu'il était impossible de dire quelle était la charge utile secondaire ou de voir des indicateurs post-infection, car la session pcap capturant le trafic réseau s'est terminée après le téléchargement du deuxième programme.

39. La personne désignée a également fait valoir que les ordinateurs du GC n'étaient pas disponibles pour l'examen des indicateurs post-infection parce que les ordinateurs compromis sont habituellement réimagés (c.-à-d. nettoyés en étant restaurés à un état antérieur) moins de trois jours après l'infection. Il était donc impossible pour la personne désignée d'établir la nature précise de la charge utile.

40. Les entreprises ont argué que le rapport d'enquête n'a pas démontré que des programmes avaient été installés sur les ordinateurs du GC sans son consentement exprès. Elles ont soutenu que les éléments de preuve figurant au dossier concernent le chargement des fichiers Shockwave Flash sur les ordinateurs du GC, et non leur installation.

41. Les entreprises ont argué qu'il n'est pas possible de déterminer, sur la base des preuves numériques au dossier, si les fichiers Shockwave Flash ont été exécutés ou s'ils ont entraîné le chargement d'autres programmes sur les ordinateurs du GC, parce que le personnel d'enquête du Conseil n'a pas recueilli les preuves numériques nécessaires pour tirer cette conclusion.

42. La trousse d'exploit Angler se compose d'une série d'étapes, et les entreprises ont fait valoir que les preuves sont insuffisantes pour conclure que toute étape au-delà de la première a été couronnée de succès. Les entreprises ont argué qu'une compromission réussie des ordinateurs du GC, comme le prétendait le rapport d'enquête, impliquait une installation et une exécution réussies des étapes suivantes.

43. Les entreprises ont fait valoir que les preuves au dossier ne prouvent pas que les fichiers Shockwave Flash énumérés dans les procès-verbaux de violation ont été exécutés, ce qui aurait entraîné l'installation de fichiers secondaires. Les entreprises ont plutôt soutenu que les preuves montrent simplement que ces fichiers secondaires ont été demandés pour être téléchargés.

44. Les entreprises ont fait valoir que, puisque le type de données contenues dans certains échantillons n'a pu être confirmé, il est incorrect de qualifier ces données de « programme » ou de « charge utile ».

45. Les entreprises ont fait valoir que la conclusion du rapport d'enquête selon laquelle la compromission a été réussie sur certains ordinateurs du GC n'est pas valide puisque les preuves nécessaires pour déterminer si les étapes ultérieures de la trousse d'exploit ont été installées ou exécutées se trouveraient sur les ordinateurs du GC et que ces ordinateurs n'ont pas été recueillis au cours de l'enquête.

46. Les entreprises ont également fait valoir que le personnel d'enquête du Conseil aurait dû recueillir une copie de la mémoire des ordinateurs du GC alors qu'ils étaient

vraisemblablement infectés, ainsi que des copies-images complètes des disques durs des ordinateurs infectés. Cela aurait permis au personnel d'enquête du Conseil d'obtenir des données essentielles, telles que les paramètres de configuration des ordinateurs susceptibles d'avoir été modifiés par le logiciel malveillant et enregistrés sur le disque dur, l'historique des programmes exécutés, l'historique des sites Web auxquels le navigateur Web s'est connecté et les programmes qui ont envoyé ou reçu des données réseau.

47. Les entreprises ont argué que le personnel d'enquête du Conseil aurait dû recueillir des fichiers pcap complets montrant tout le trafic réseau en provenance et à destination des ordinateurs infectés avant, pendant et après l'infection.

48. Les entreprises ont également soutenu que l'avis de communication adressé à SPC ne demandait pas tout le trafic réseau pertinent. L'avis de communication n'a demandé que des renseignements ou des données, des fichiers pcap et des échantillons de logiciels malveillants liés aux cinq adresses IP appartenant aux entreprises.

49. Le spécialiste externe a fait valoir, en ce qui concerne l'installation de programmes d'ordinateur sur les ordinateurs du GC, qu'il n'était pas possible de conclure que ces programmes d'ordinateur avaient été installés (c.-à-d. qu'ils étaient prêts à être exécutés) ou que des vulnérabilités avaient été exploitées ou que d'autres codes malveillants avaient été récupérés, installés et exécutés, parce que les preuves numériques requises pour les ordinateurs en question n'étaient pas disponibles pour examen, étude et analyse afin de tirer cette conclusion.

50. La personne désignée a contesté certaines des conclusions du spécialiste externe, tout en reconnaissant que la meilleure source de preuves aurait été les ordinateurs compromis. Toutefois, la personne désignée a fait valoir que l'accès à ces ordinateurs n'est pas nécessaire, car les échantillons de fichiers pcap ont démontré que les programmes d'exploitation Flash étaient prêts à être exécutés du simple fait qu'ils avaient été récupérés et transmis aux ordinateurs.

51. Dans leur réponse au rapport d'expertise externe, les entreprises étaient en accord avec la majorité des commentaires, des constatations d'ordre technique et des conclusions de l'évaluation externe. Les entreprises ont fait valoir que le rapport d'expertise externe confirme que les preuves numériques étaient à la fois défectueuses et incomplètes et que le rapport d'enquête ne fournit pas d'éléments suffisants pour prouver qu'un quelconque programme a été installé. Les entreprises ont également ajouté que, dans le meilleur des cas, les preuves techniques contenues dans le rapport d'enquête montrent qu'une partie inconnue a pu tenter d'installer un logiciel malveillant.

Résultats de l’analyse du Conseil

52. Le paragraphe 8(1) de la LCAP indique ceci :

> Il est interdit, dans le cadre d’activités commerciales, d’installer ou de faire installer un programme d’ordinateur dans l’ordinateur d’une autre personne […] sauf si la personne qui accomplit l’acte en question : a) soit le fait avec le consentement exprès du propriétaire ou de l’utilisateur autorisé de l’ordinateur et se conforme au paragraphe 11(5); b) soit le fait en vertu d’une ordonnance judiciaire.

53. Le Conseil fait remarquer que le paragraphe 8(1) de la LCAP fait référence à l’installation d’un programme d’ordinateur, et non à la tentative d’en installer un. Si l’intention du législateur en rédigeant la LCAP avait été de couvrir les tentatives d’installation, il aurait probablement inclus ce langage dans le paragraphe 8(1) de la LCAP. En outre, contrairement à certains arguments avancés dans le dossier, la question ne concerne pas nécessairement l’infection ou la compromission d’un ordinateur, puisque ces actions ou conséquences ne sont pas mentionnées dans la LCAP. La question est de savoir s’il existe suffisamment de preuves dans le dossier de l’instance pour conclure, selon la prépondérance des probabilités, que les fichiers Shockwave Flash énumérés dans les procès-verbaux de violation ont été installés.

54. De l’avis du Conseil, l’accès à une copie de la mémoire des ordinateurs du GC au moment où l’on pense qu’ils ont été infectés aurait aidé à démontrer que les fichiers Shockwave Flash ont été copiés ou placés sur la mémoire vive ou le disque dur de l’ordinateur. Dans ses commentaires sur le rapport d’expertise externe, la personne désignée a reconnu que les ordinateurs physiques auraient constitué la meilleure source de preuves. L’expert des entreprises et le spécialiste externe sont également arrivés à une conclusion similaire à celle de la personne désignée.

55. Bien qu’il n’y ait aucune indication dans le dossier qu’une demande ait été faite à SPC pendant l’enquête pour accéder aux ordinateurs qui auraient pu être compromis, le Conseil est conscient qu’il n’est pas toujours possible ou pratique d’obtenir un accès physique aux ordinateurs quelques jours, voire quelques semaines, après qu’ils aient pu être compromis. Cela est particulièrement vrai lorsque les ordinateurs peuvent être réimagés après un certain temps. Le Conseil ne suggère pas que sans l’accès à de telles preuves, il serait impossible de prouver les violations du paragraphe 8(1) de la LCAP.

56. Cependant, en raison de l’absence d’accès aux ordinateurs, l’élément central des conclusions du rapport d’enquête concernant l’installation des fichiers Shockwave Flash était principalement le résultat de l’analyse technique des échantillons de fichiers pcap fournis par SPC, qui, dans ce cas, ne font que démontrer ce qui s’est passé pendant une période donnée sur une partie spécifique du trafic réseau du GC. Par conséquent, les conclusions que l’on peut tirer de l’analyse de ces échantillons de fichiers pcap sont indirectes et ne précisent pas si, ou où, les programmes d’ordinateur ont été installés.

57. Étant un portrait des paquets de données qui circulent sur une période donnée, les échantillons de fichiers pcap permettent d'observer et d'analyser les données qui circulent sur un réseau entre les hôtes. Cependant, un échantillon de fichiers pcap ne montre pas ce qui se passe au niveau du point d'extrémité. Le Conseil fait remarquer que cette observation a été soutenue par l'expert des entreprises, ainsi que par le spécialiste externe, qui ont tous deux indiqué que les preuves numériques fournies à l'appui des procès-verbaux de violation sont insuffisantes pour prouver que l'installation a effectivement eu lieu.

58. Si les échantillons de fichiers pcap examinés par le personnel d'enquête du Conseil confirment que des paquets contenant des fichiers Shockwave Flash ont transité par le réseau du GC à un moment donné, ils ne confirment pas que les fichiers Shockwave Flash présents dans les paquets ont finalement été installés (c.-à-d. copiés ou placés sur la mémoire vive ou les disques durs des ordinateurs du GC).

59. Le Conseil estime que s'il est vraisemblablement possible qu'un échantillon de fichiers pcap contienne suffisamment d'information pour démontrer l'échange et la réception de données entre ordinateurs, les échantillons de fichiers pcap spécifiques figurant dans le dossier de l'instance ne fournissaient pas ce niveau d'information détaillée. Plus précisément, il semble que le filtrage[8] de ces échantillons de fichiers pcap ait limité la quantité de renseignements fournis, y compris les renseignements nécessaires pour démontrer que toutes les étapes permettant de récupérer un programme, et par conséquent de l'installer, ont bien été effectuées.

60. Le Conseil fait remarquer que les commentaires de la personne désignée sur le rapport d'expertise externe abordent la question des conclusions limitées que l'on peut tirer de l'analyse des échantillons de fichiers pcap. La personne désignée a fait valoir que le code d'état « 200 OK » dans les échantillons de fichiers pcap était une preuve suffisante que les programmes d'exploitation Flash étaient installés lorsqu'ils ont été téléchargés et reçus, même s'ils n'étaient pas encore exécutés.

61. Toutefois, le Conseil souligne que la réponse « 200 OK » du serveur indique que la demande du navigateur Web a été reçue avec succès et qu'une réponse est en cours de transmission. Il n'indique pas que les données ou le programme d'ordinateur lui-même ont été reçus avec succès (c.-à-d. installés, mais pas encore exécutés) par le navigateur Web.

62. La réponse du protocole de transfert hypertexte (HTTP) de l'ordinateur client qui aurait indiqué que le programme d'ordinateur a bien été reçu aurait pris la forme d'une réponse d'accusé de réception (ACK) au serveur, par opposition à la réponse « 200 OK » du serveur. Toutefois, le rapport d'enquête et les commentaires de la personne désignée sur le rapport d'expertise externe ne précisent pas si l'ordinateur client a accusé réception du programme d'ordinateur par une réponse ACK. En l'absence d'une telle réponse ACK, il apparaît au Conseil que l'installation du programme d'exploitation Flash a été déduite par la personne désignée et n'est pas nécessairement étayée par des preuves claires dans le dossier.

---

[8] Divers filtres peuvent être utilisés lors de la capture de paquets de données sur les réseaux informatiques, comme des filtres IP.

63. Le Conseil fait remarquer que le rapport d'enquête tente de démontrer davantage l'installation des fichiers Shockwave Flash en affirmant, sur la base de l'analyse des échantillons de fichiers pcap, qu'ils ont été exécutés sur les ordinateurs du GC.

64. Selon le rapport d'enquête, la preuve que ces fichiers Shockwave Flash n'étaient pas seulement prêts à être exécutés, mais qu'ils ont été effectivement exécutés (et donc clairement installés) réside dans le fait qu'un deuxième programme aurait été vraisemblablement récupéré, ce que la personne désignée appelle la charge utile ou le logiciel malveillant dans le rapport d'enquête.

65. Le Conseil estime que cette conclusion pose plusieurs problèmes, notamment le fait que deux des sept échantillons de fichiers pcap ne démontrent pas qu'un deuxième programme a été téléchargé. Plus précisément, dans un cas, le téléchargement d'un deuxième programme a été tenté sans succès, alors qu'un autre échantillon de fichiers pcap démontre qu'il n'y a pas eu de tentative de téléchargement d'un deuxième programme.

66. Le Conseil souligne également qu'une partie du raisonnement de la personne désignée est que les fichiers Shockwave Flash doivent avoir été installés puisque ces fichiers Shockwave Flash ont récupéré ce que la personne désignée appelle une charge utile. Cependant, le dossier ne contient aucune analyse approfondie de logiciels malveillants démontrant que les fichiers Shockwave Flash contenaient des codes malveillants (c.-à-d. des instructions) ou que ces instructions ont été exécutées afin de récupérer un deuxième programme.

67. Le Conseil estime en outre qu'il est plus probable que ce soit le navigateur Web, plutôt que les fichiers Shockwave Flash, qui ait provoqué la récupération du deuxième programme. Le Conseil fait remarquer que la pratique courante consiste, pour les navigateurs Web, à récupérer des données pour toute ressource qu'une page Web indique comme étant nécessaire au bon affichage de la page (comme des images, du code, etc.). Ces types de demandes ne proviennent pas automatiquement des fichiers Shockwave Flash. Enfin, si ces deuxièmes programmes ont été identifiés comme des logiciels malveillants dans le rapport d'enquête, cette affirmation n'a été étayée par aucune analyse des logiciels malveillants des deuxièmes programmes.

68. Le Conseil aurait été plus enclin à tenir compte de l'analyse des échantillons de fichiers pcap figurant dans le dossier pour déduire qu'une installation a eu lieu, comme l'a fait la personne désignée, si cette déduction avait été étayée par d'autres preuves. Par exemple, un rapport d'incident de sécurité aurait pu être soumis pour démontrer que le dispositif en matière de sécurité de la technologie de l'information (TI) du GC n'a pas arrêté les programmes d'ordinateur avant qu'ils ne soient installés, ou une déclaration sous serment d'employés de SPC aurait pu être soumise pour confirmer que les fichiers Shockwave Flash avaient été trouvés sur les disques durs, et que, par conséquent, les disques durs devaient être réimagés.

69. L’absence de telles preuves ouvre la porte à d’autres explications plausibles et concevables quant à ce qui est arrivé aux programmes d’ordinateur. Par exemple, les programmes d’ordinateur auraient pu être détectés par le dispositif en matière de sécurité TI du GC. Étant donné que le dossier indique que les ordinateurs du GC disposent d’un dispositif de sécurité informatique renforcé, le Conseil fait remarquer qu’il est plausible que les fichiers Shockwave Flash aient été bloqués avant d’atteindre la mémoire vive ou les disques durs des ordinateurs du GC et d’avoir la possibilité de s’y installer.

Conclusion

70. Le Conseil est conscient du niveau de complexité de l’enquête qui a abouti à la délivrance de procès-verbaux de violation aux entreprises. Le Conseil ne remet pas non plus en cause la décision du personnel d’enquête du Conseil d’ouvrir une enquête sur les adresses IP liées aux entreprises. Le Conseil ne suggère pas non plus que le point de vue de la personne désignée sur l’installation éventuelle de fichiers Shockwave Flash sur les ordinateurs du GC est sans aucun fondement.

71. Toutefois, le Conseil conclut que les éléments de preuve dans le dossier ne sont pas suffisants pour prouver, selon la prépondérance des probabilités, que les sept fichiers Shockwave Flash ont été installés sur la mémoire vive ou le disque dur des ordinateurs du GC. De telles installations auraient été en contradiction avec le paragraphe 8(1) de la LCAP.

72. Compte tenu de ces conclusions, il n’est pas nécessaire d’examiner si le dossier démontre que les entreprises ont commis des violations de l’article 9 de la LCAP.

73. Par conséquent, le Conseil détermine que les entreprises n’ont pas commis de violation de l’article 9 de la LCAP en aidant à commettre un acte contraire au paragraphe 8(1) de la LCAP, à savoir l’installation d’un programme d’ordinateur. Par conséquent, les sanctions administratives pécuniaires établies dans les procès-verbaux de violation ne seront pas imposées.

Secrétaire général