Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

Le Centre de la sécurité des télécommunications Canada (CST) a déterminé que les activités de cybermenace de la République populaire de Chine (RPC) dépassent les cybermenaces de toute autre nation en termes de volume, de sophistication et d'ampleur des cibles visées. Le Centre canadien pour la cybersécurité (ou Centre pour la cybersécurité), qui relève du CST, a constaté des activités de menace à grande échelle provenant de la RPC. Ces activités représentent une grave menace envers des entités canadiennes de différents secteurs et ont ciblé :

- tous les secteurs du gouvernement;
- des organismes non gouvernementaux, le milieu universitaire et de la recherche;
- les infrastructures essentielles;
- l'industrie, y compris le secteur canadien de la recherche et du développement.

Lorsque le Centre pour la cybersécurité identifie des activités de cybermenace qui ciblent des Canadiennes ou Canadiens ou un organisme canadien, il communique cette information au propriétaire du système afin de l'aider à identifier et atténuer la menace et à avertir les utilisatrices et utilisateurs concernés, au besoin.

En janvier 2021, le Centre pour la cybersécurité a signalé aux responsables de la sécurité des TI de la Chambre des communes (CC) des activités de harponnage qui ciblaient les comptes courriel de parlementaires. Ces courriels de harponnage incitaient les destinataires à ouvrir un courriel contenant une image (c.-à-d. un lien de suivi) connecté à un serveur contrôlé par un auteur de menace. Cela permet aux auteurs de menace de confirmer la validité des adresses courriel ciblées et de recueillir des données préliminaires sur les utilisateurs, comme des informations de base sur leurs appareils et réseaux locaux. Ces courriels peuvent être précurseurs d'activités de suivi de la part des auteurs de menace.

De janvier à avril 2021, le Centre pour la cybersécurité et le Service canadien du renseignement de sécurité (SCRS) ont rencontré les responsables de la sécurité des TI de la CC et le CST leur a communiqué au moins 12 rapports afin de leur présenter les indicateurs de compromission techniques touchant les systèmes de TI de la CC. En novembre 2021, le SCRS a remis aux 35 clients du GC un rapport d'analyse classifié traitant de la campagne de liens de suivi menée par l'APT31 contre les membres de l'Alliance interparlementaire sur la Chine (IPAC pour *Inter-Parliamentary Alliance of China*). En juin 2022, le Federal Bureau of Investigation (FBI) a communiqué un rapport au

Chronologie des événements
Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

CST et au SCRS au sujet d'une campagne de lien de suivi de la RPC qui comprenait des activités ciblant la CC.

Vous trouverez ci-dessous la chronologie des mesures prises par le Centre pour la cybersécurité et le SCRS pour signaler les menaces aux responsables de la CC et les appuyer dans leurs efforts de détection et d'atténuation.

Remarque : Le Centre pour la cybersécurité a communiqué avec le CC et le SCRS des rapports sur les liens de suivi qui ciblaient des parlementaires depuis la fin de 2018.

Chronologie des événements

22 janvier 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité envoie un rapport au compte courriel de la Sécurité des TI de la CC dans lequel on indique que des liens de suivi ont été envoyés dans ces courriels aux personnes ayant des adresses courriel se terminant par @parl.gc.ca et @sen.parl.gc.ca.

Seuls les détails techniques associés au trafic réseau étaient disponibles.

25 janvier 2021

L'analyste principal, Sécurité des TI de la CC accuse réception du rapport du 22 janvier.

La CC n'a pas fourni de rétroactions supplémentaires.

29 janvier 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité envoie un courriel à l'adresse de la Sécurité des TI de la CC pour demander des rétroactions au sujet du rapport du 22 janvier.

3 février 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité fait un nouveau suivi pour demander de la rétroaction au sujet du rapport du 22 janvier.

L'analyste principal, Sécurité des TI de la CC répond au responsable du traitement des incidents du Centre pour la cybersécurité que le problème a été réglé à l'interne.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

17 février 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité envoie un deuxième rapport au compte courriel de la Sécurité des TI de la CC dans lequel on indique que des auteurs de menace dotés de moyens sophistiqués menaient des activités de reconnaissance réseau dans les dispositifs connus pour se connecter au réseau privé virtuel (RPV) de la CC.

Le 1er mars, le directeur, Sécurité des TI de la CC a indiqué au responsable du traitement des incidents du Centre pour la cybersécurité qu'au moins une adresse IP était associée au réseau domestique d'un utilisateur non divulgué de la CC et que la CC avait été en mesure d'obtenir deux dispositifs électroniques afin de les analyser.

Le 5 mars, le responsable du traitement des incidents du Centre pour la cybersécurité a demandé au directeur, Sécurité des TI de la CC d'effectuer une analyse judiciaire des dispositifs pour garantir qu'aucune activité malveillante n'avait eu lieu. La CC n'a pas fourni les dispositifs électroniques au Centre pour la cybersécurité.

17 février 2021

Le directeur, Sécurité des TI de la CC et des représentants du SCRS et du Centre pour la cybersécurité se sont réunis pour discuter d'une collaboration accrue au sujet de cet incident.

Le directeur, Sécurité des TI de la CC a fourni à l'équipe de Gestion des incidents du Centre pour la cybersécurité un document imprimé contenant des exemples de courriels malveillants et les noms de huit parlementaires qui étaient les destinataires ciblés par ces courriels malveillants.

D'après le document, la CC avait évalué à ce moment que les courriels n'étaient pas parvenus jusqu'à leurs cibles au sein de la CC. Toutefois, la CC a indiqué que certains destinataires pourraient avoir reçu des courriels similaires à leur adresse courriel personnelle.

18 février 2021

Une réunion de l'unité de cybertriage (CTU pour *Cyber Triage Unit*) a eu lieu entre le SCRS et le Centre pour la cybersécurité afin de discuter des efforts d'intervention combinés de chaque organisme.

Il avait été décidé que le SCRS collabore avec la CC. L'équipe de Gestion des incidents du Centre pour la cybersécurité a fourni au SCRS une liste de questions techniques afin d'aider à analyser les activités suspectes.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

18 février 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité communique un troisième rapport à la CC dans lequel on avait identifié d'autre trafic préoccupant dans le système de noms de domaine (DNS).

19 février 2021

Le SCRS et le Centre pour la cybersécurité rencontrent le directeur, Sécurité des TI de la CC pour discuter de la portée de l'incident et d'une possible analyse judiciaire.

22 février 2021

Le SCRS et le Centre pour la cybersécurité rencontrent le directeur, Sécurité des TI de la CC pour faire le suivi de la réunion du 19 février.

Le directeur, Sécurité des TI de la CC a indiqué que l'équipe de la CC avait consacré beaucoup de temps à l'étude de l'incident après la réunion du 19 février. Le directeur, Sécurité des TI de la CC a fourni des données d'analyse au SCRS et a autorisé le personnel du Centre pour la cybersécurité à faire une copie, ce qui a été fait à la fin de la réunion.

23 février 2021

Une réunion de la CTU a lieu entre le SCRS et le Centre pour la cybersécurité.

Après la réunion, le responsable du traitement des incidents du Centre pour la cybersécurité a fourni des questions de suivi au SCRS à des fins de diffusion à la CC, afin de soutenir l'enquête en cours.

24 février 2021

Une réunion de CTU a eu lieu entre le SCRS et le Centre pour la cybersécurité pour définir un cadre d'engagements conjoints avec la CC.

Après la réunion, le responsable du traitement des incidents du Centre pour la cybersécurité a présenté (le 23 février) ses questions de suivi à des fins d'enquête au directeur, Sécurité des TI de la CC et a demandé des copies des courriels mentionnés dans la liste. Le directeur, Sécurité des TI de la CC n'a pas fourni les courriels.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

24 février 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a fait parvenir un quatrième rapport au compte courriel de la Sécurité des TI de la CC afin de signaler que des auteurs de menace dotés de moyens sophistiqués scannaient des adresses IP qui pourraient être liées à des dispositifs électroniques de la CC.

Le Centre pour la cybersécurité a communiqué un cinquième rapport à la CC dans lequel on indiquait qu'entre le 23 et le 24 février 2021, le trafic DNS du réseau a été observé se dirigeant vers un domaine précédemment signalé à la CC.

26 février 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a reçu un courriel du directeur, Sécurité des TI de la CC dans lequel il indiquait que plus de courriels et des métadonnées partagées de 41 courriels avaient été envoyés à 13 parlementaires entre le 21 et le 28 janvier 2021. De ce total, 31 avaient été lus ou ouverts par inadvertance.

Sept des 13 parlementaires avaient été aussi nommés dans le rapport partagé par le directeur, Sécurité des TI de la CC lors de la réunion du 17 février; ainsi, on pouvait confirmer qu'un total de 14 parlementaires avaient reçu des courriels malveillants.

Dans le même courriel, le directeur, Sécurité des TI de la CC indiquait que le 10 février 2021, le Sénat avait fourni des informations au sujet d'un courriel malveillant (aucune autre information supplémentaire).

1er mars 2021

En réponse à la demande de clarification du Centre pour la cybersécurité au sujet du nombre d'utilisatrices et d'utilisateurs du Sénat ayant reçu ces courriels, le directeur, Sécurité des TI de la CC a indiqué qu'on avait identifié deux courriels suspects qui avaient été envoyés à ses clients du Sénat.

Après avoir reçu une notification de la CC, le Sénat a fourni un exemple de courriel en indiquant que « les courriels reçus avaient été supprimés de façon permanente par nos clients vigilants qui les avaient reçus ».

3 mars 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité communique un sixième rapport à la CC contenant des adresses IP suspectes qui s'étaient connectées aux serveurs de courriel de la CC.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

9 mars 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a envoyé un septième rapport à l'adresse courriel de la Sécurité des TI de la CC dans lequel on indiquait que l'infrastructure utilisée par les auteurs de menace dotés de moyens sophistiqués s'était connectée aux serveurs de courriel appartenant au Sénat et à la CC.

17 mars 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a fait parvenir un huitième rapport au compte courriel de la Sécurité des TI de la CC dans lequel on indiquait que le 11 mars 2021, un dispositif de trouvant à la CC s'était connecté à une infrastructure de commande et de contrôle (C2) malveillante.

L'analyste de la Sécurité des TI de la CC a répondu que le dispositif concerné était un dispositif personnel dans une partie du réseau de la CC destiné aux appareils personnels, et que l'appareil n'avait pas été détecté à l'intérieur du réseau du bureau.

Le 29 mars, le responsable du traitement des incidents du Centre pour la cybersécurité a demandé à l'analyse, Sécurité des TI de la CC de lui fournir plus d'informations techniques et contextuelles afin de pouvoir mieux évaluer la situation. L'analyste de la Sécurité des TI de la CC a accusé réception de la demande, mais n'a jamais fourni les informations demandées, malgré un suivi renouvelé de la part du responsable du traitement des incidents du Centre pour la cybersécurité le 8 avril.

23 mars 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a envoyé un neuvième rapport au compte courriel de la Sécurité des TI de la CC dans lequel on indiquait que le Centre pour la cybersécurité avait détecté des connexions suspectes aux portails Web de la CC.

La CC a accusé réception du message le jour même.

30 mars 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a envoyé un dixième rapport à la CC dans lequel on identifiait des activités malveillantes dans les réseaux de la CC.

La CC a accusé réception du message le jour même.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

19 avril 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a envoyé un onzième rapport au compte courriel de la Sécurité des TI de la CC dans lequel on indiquait que le Centre pour la cybersécurité avait détecté de nouvelles activités, c.-à-d. que de nombreuses adresses IP se connectaient au portail Web de la CC.

La CC a accusé réception du rapport le jour même et a demandé des renseignements supplémentaires sur le contexte qui ont été fournis le 20 avril par le Centre pour la cybersécurité.

22 avril 2021

Le responsable du traitement des incidents du Centre pour la cybersécurité a communiqué un douzième rapport au compte courriel de la Sécurité des TI de la CC dans lequel on indiquait suspecter que le même dispositif identifié dans le rapport au 17 mars 2021 avait été infecté par un maliciel et qu'il se connectait à ce que l'on suspectait être une infrastructure C2 malveillante.

La CC a confirmé avoir reçu le rapport et a indiqué qu'elle enquêtait sur le sujet; cela dit, aucune autre rétroaction n'a été reçue par le Centre pour la cybersécurité.

29 avril 2021

Le SCRS rencontre le directeur, Sécurité des TI de la CC et lui fournit un moyen d'identifier d'autres cibles possibles des courriels de suivi.

3 juin 2021

Le SCRS rencontre le directeur, Sécurité des TI de la CC. Le SCRS précise que les parlementaires ciblés étaient tous membres de l'IPAC et remet au directeur, Sécurité des TI de la CC une liste complète des parlementaires canadiennes et canadiens qui étaient membres de l'IPAC.

La CC a accepté de poursuivre les recherches pour trouver des noms additionnels dans les journaux de la CC et relever de plus amples preuves de ciblage. Le directeur, Sécurité des TI de la CC a réitéré le fait qu'il serait impossible d'acheminer de tels courriels de liens de suivi par l'entremise du réseau de la CC.

29 juillet 2021

Le SCRS rencontre le directeur, Sécurité des TI de la CC pour discuter de l'analyse judiciaire préalablement divulguée et lui remettre l'analyse qu'il avait faite de l'information fournie par la CC.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

19 novembre 2021

Le SCRS remet aux 35 clients du GC un rapport d'analyse classifié traitant de la campagne de liens de suivi menée par l'APT31 contre les membres de l'IPAC.

29 juin 2022

Le Centre pour la cybersécurité et le SCRS ont reçu un rapport du FBI décrivant la campagne de liens de suivi de la RPC que le FBI attribuait à APT31 et qui a ciblé 406 adresses courriel uniques de personnes de partout dans le monde, y compris des personnes qui s'étaient exprimées publiquement sur les activités du Parti communiste chinois.

Le rapport comprenait 20 adresses courriel qu'on croyait avoir été ciblées en janvier 2022, dont 19 adresses courriel se terminant par @parl.gc.ca ou @sen.parl.gc.ca.

Sur ces 19 adresses courriel, 14 avaient été divulguées au Centre pour la cybersécurité par le directeur, Sécurité des TI de la CC les 17 et 26 février 2021.

30 juin 2022

Le responsable du traitement des incidents du Centre pour la cybersécurité communique les détails du rapport du FBI au compte courriel de la Sécurité des TI de la CC après en avoir fait l'harmonisation avec le SCRS.

Le Centre pour la cybersécurité avait indiqué que l'activité était associée à un auteur de menace doté de moyens sophistiqués et comprenait la description de techniques utilisées, des indicateurs d'activités malveillantes, les noms des parlementaires et membres du Sénat, et des conseils techniques d'atténuation.

Le 4 juillet 2022, l'analyste, Sécurité des TI de la CC a répondu au responsable du traitement des incidents du Centre pour la cybersécurité et a indiqué que les seules activités qu'ils avaient trouvées dataient de janvier 2021.

Le 21 juillet 2022, le FBI a confirmé à l'équipe de Gestion des incidents du Centre pour la cybersécurité que l'activité mentionnée dans son rapport de juin 2022 avait eu lieu en janvier 2021. Cela permettait de conclure que le rapport du FBI décrivait la même activité signalée dans les rapports du SCRS et du Centre pour la cybersécurité et qui avait été communiquée à la CC en janvier 2021.

14 juillet 2022

Le Centre pour la cybersécurité publie une évaluation des menaces classifiée intitulée *Revisiting PRC Email Operations against Canadian Parliamentarians* (en anglais seulement).

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

14 juillet 2022 — Le Centre pour la cybersécurité publie une évaluation des menaces classifiée intitulée *Revisiting PRC Email Operations against Canadian Parliamentarians* (en anglais seulement).

20 juillet 2022 — Le Centre pour la cybersécurité publie une évaluation des menaces classifiée traitant de l'activité menée par l'APT31 contre le gouvernement entre juin et septembre 2021.

22 juillet 2022 — Le Centre pour la cybersécurité publie une évaluation des menaces classifiée qui porte sur les difficultés de se protéger contre le nombre très élevé d'activités de cyberespionnage menées par la RPC.

19 décembre 2022 — Le Centre pour la cybersécurité publie une évaluation des menaces classifiée intitulée *PRC Email Operations against Canadians* (en anglais seulement).

25 août 2023 — Le SCRS remet aux clients du GC concernés une évaluation du renseignement qui porte sur la campagne de liens de suivi menée par l'APT31 contre les membres de l'IPAC.

Chronologie des événements

Campagne de liens de suivi des courriels ciblant des parlementaires canadiennes et canadiens

Outils de cyberdéfense du CST à l'intention des systèmes de la CC

2016 Début des discussions entre le CST et la CC au sujet d'un ensemble complet d'outils spécialisés de cyberdéfense que le CST offre aux ministères et organismes du gouvernement du Canada.

2018 La CC adopte les moyens de protection basés sur réseau du Centre pour la cybersécurité.

2020 La CC met en œuvre l'ensemble complet des outils du Centre pour la cybersécurité.

Ces outils étaient et sont toujours un élément essentiel de la protection des systèmes de TI du gouvernement du Canada.

2022 En octobre, la CC étend la couverture de l'ensemble des outils du Centre pour la cybersécurité.