Fuite de donnÃ©es au Royaume-Uni
Internet
PostÃ© par : JerryG
PubliÃ©e le : 14/8/2023 13:00:00

La Commission Ã©lectorale britannique, organisme de surveillance des Ã©lections au Royaume-Uni, a publiÃ© une note rÃ©vÃ©lant qu'elle avait Ã©tÃ© victime d'une Â« cyberattaque complexe Â» susceptible d'affecter des millions d'Ã©lecteurs.

La Commission Ã©lectorale a dÃ©clarÃ© que des Â« acteurs hostiles Â», non spÃ©cifiÃ©s, avaient rÃ©ussi Ã accÃ©der Ã des copies de listes Ã©lectorales depuis le mois dâaoÃ»t 2021.

Les registres tels quâau moment de la cyberattaque comprenaient le nom et l'adresse de toute personne inscrite Ã un bureau de vote entre 2014 et 2022 au Royaume-Uni, ainsi que les noms des personnes inscrites en tant qu'Ã©lecteurs Ã©trangers. Les cybercriminels ont Ã©galement pÃ©nÃ©trÃ© dans les e-mails et Â« systÃ¨mes de contrÃ´le Â» de la commission, alors que l'attaque n'a Ã©tÃ© dÃ©couverte qu'en octobre de l'annÃ©e derniÃ¨re.

La commission dÃ©clare qu'il est difficile de prÃ©dire exactement combien de personnes pourraient Ãªtre touchÃ©es, mais elle estime que le registre contient les dÃ©tails d'environ 40 millions dâÃ©lecteurs.

Pour Xavier Daspre, directeur technique de Proofpoint France, Â« La nouvelle selon laquelle la Commission Ã©lectorale britannique aurait exposÃ© les donnÃ©es de millions d'Ã©lecteurs est une violation importante de cybersÃ©curitÃ© Ã laquelle, Ã vrai dire, nous aurions dÃ» nous y attendre.

La fragilitÃ© des systÃ¨mes dâinformation des dÃ©mocraties est devenue de plus en plus Ã©vidente ces derniÃ¨res annÃ©es, il n'est donc pas surprenant de voir un acteur de la menace assez compÃ©tent et furtif, chercher Ã Ã©valuer et potentiellement saper les processus de vote.

Cela n'enlÃ¨ve rien Ã la gravitÃ© de l'Ã©vÃ©nement, et nous avons de la chance que la commission Ã©lectorale du Royaume-Uni affirme que cela â n'a eu d'impact sur aucune Ã©lection, ni sur le statut d'inscription de qui que ce soitâ. Ceci Ã©tant dit, cela reste toujours un incident grave, car saper le processus dÃ©mocratique pourrait conduire Ã des changements sociÃ©taux incontrÃ´lÃ©s et catastrophiques Â».

Les Ã©lections passÃ©es nous ont montrÃ© que les cybercriminels ciblent agressivement les infrastructures critiques du gouvernement pour accÃ©der Ã des informations sensibles et causer des dommages gÃ©nÃ©ralisÃ©s. Cette fuite de donnÃ©es au Royaume-Uni nous rappelle que ce type dâÃ©vÃ¨nements, dâimportance nationale, est tout Ã fait privilÃ©giÃ© par les cybercriminels de tout bord.

Pendant la campagne prÃ©sidentielle franÃ§aise, en 2017, 15 Go de donnÃ©es avaient Ã©tÃ© volÃ©es (dont 21 075 mails), publiÃ©s et relayÃ©s par une armÃ©e de trolls sur les rÃ©seaux sociaux, le hashtag #MacronLeaks faisant son apparition dans prÃ¨s d'un demi-million de tweets en l'espace de vingt-quatre heures (IRSEM).

Le risque est donc avÃ©rÃ©, comme en tÃ©moigne l'inculpation de six officiers du GRU (renseignement militaire russe) par le ministÃ¨re amÃ©ricain de la Justice, pour leur implication

dans une sÃ©rie de cyberattaques mondiales, y compris celles de spear phishing ciblant les Ã©lections prÃ©sidentielles franÃ§aises de 2017, et attribuÃ©es Ã l'officier Anatoliy Sergevich Kovalev. Bien que les candidats n'aient pas abordÃ© publiquement cette question, l'action en justice dÃ©montre que le risque est rÃ©el et omniprÃ©sent.

Au Royaume-Uni, il est Ã©vident que les cybercriminels tiraient pleinement parti de la structure vulnÃ©rable et dÃ©centralisÃ©e du systÃ¨me Ã©lectoral afin d'avoir accÃ¨s Ã autant d'informations que possible.

Xavier Daspre estime que Â« avec l'accÃ¨s Ã cette masse d'informations sur les Ã©lecteurs, les attaquants ont Ã prÃ©sent la possibilitÃ© et les moyens de diffuser subtilement de la dÃ©sinformation aux 40 millions de citoyens de la base de donnÃ©es, ce qui renforce leur vision du monde et amplifie la discorde. Ils peuvent Ã©galement manipuler les informations au sein de ces systÃ¨mes afin de crÃ©er la mÃ©fiance, en remettant en question l'authenticitÃ© et l'exactitude des donnÃ©es des Ã©lecteurs, ou mÃªme, dans le pire des cas, des votes eux-mÃªmes Â».

Selon Proofpoint, bien que nous ne puissions pas Ãªtre certains de leur motif, de ce qu'ils ont appris ou de ce que l'attaquant cherchait vraiment, dans ce cas, Â« les attaquants ont eu accÃ¨s aux systÃ¨mes Ã©lectoraux pendant un certain nombre de mois, ce qui indique qu'ils Ã©taient Ã la recherche d'autre chose que d'un gain financier rapide, motif pourtant le plus courant des attaques. Plus un attaquant reste longtemps, non dÃ©tectÃ©, dans un rÃ©seau, plus il peut causer de dÃ©gÃ¢ts Â».

Cette violation rappelle Ã toutes les organisations publiques et privÃ©es de prendre des mesures rapides pour renforcer leurs cyber-dÃ©fenses, pour rendre plus difficile aux criminels lâ□□accÃ¨s initial dans leurs systÃ¨mes et les dommages collatÃ©raux qui sâ□□en suivent.Â