En Marche est la cible d'attaques de phishing des services russes

Dans un document à paraître demain, et qui reprend deux années d'agissements de Pawn Storm (un groupe de hackers masquant probablement les activités des services de renseignement russes), Trend Micro indique qu'En Marche a été victime d'une campagne de phishing orchestrée par cette organisation impliquée notamment dans le piratage du camp démocrate lors de la présidentielle américain. Dans ce rapport de 70 pages, une ligne indique que le groupe de hackers, aussi appelé Fancy Bear, a créé, au moins à partir du 15 mars dernier, un domaine appelé Onedrive-en-marche.fr. Le signe d'une volonté des hackers de cibler l'équipe de campagne du candidat, arrivé en tête au premier tour hier. Objectif de Pawn Storm avec ce lien créé sur l'environnement de stockage de Microsoft : tromper les personnes ciblées par l'opération, en leur faisant croire à un lien officiel, donc de confiance.

Mais, pour Mounir Mahjoubi, responsable de la campagne numérique d'Emmanuel Macron, le ciblage des équipes d'En Marche par des opérations de phishing est plus large que celui décrit par l'éditeur. Et remonte à au moins février dernier. « *Chaque semaine, nous assistons à la résurgence d'une campagne ou à l'apparition d'une nouvelle opération. Les assaillants ont récupéré tous les noms publics ou semi-publics associés à l'équipe d'En Marche et les ont tous ciblé* », explique l'ex-président du Conseil national du numérique. Et ce dernier de préciser qu'il dispose d'une « *très belle collection d'e-mails de phishing, la plupart très bien faits, avec par exemple des certificats HTTPS parfaits. Ces mails sont capables de tromper y compris un œil très averti.* »

Bombarder les URL piégées

En février dernier, Mounir Mahjoubi décrivait déjà dans nos colonnes une opération de phishing sophistiquée. « *Au départ, il s'agit d'un lien RSS qui renvoie vers un site de fake news. Mais si l'onglet reste ouvert, alors il se transforme en fausse page de connexion à Gmail, capable de piéger un utilisateur qui y entrerait ses codes d'accès* », expliquait-il alors. Une technique appelée Tabnabbing qu'affectionne également Pawn Storm, même si, dans ce cas précis, Trend Micro ne donne aucune indication permettant de relier le groupe de hackers russe à la campagne d'Emmanuel Macron.

Mais, selon En Marche, ces assauts répétés se sont révélés infructueux : les pirates n'auraient pas réussi à infiltrer l'organisation d'Emmanuel Macron en prenant le contrôle d'un compte mail interne. Et ce, même si certains membres de l'équipe ont cliqué à l'occasion sur des liens piégés. Probablement aiguillonnée par l'expérience de la campagne présidentielle américaine, l'équipe de campagne d'Emmanuel Macron a mis en place un certain nombre de contre-mesures contre le phishing. A commencer par la formation de tous les utilisateurs. « *Quand tout le monde est sensibilisé, le gros du travail est effectué*, dit Mounir Majhoubi. *Même si cela prend beaucoup de temps.* » S'y ajoute le remplacement des mots de passe en cas de doute, ainsi que le monitoring des accès au système de messagerie. « *Par ailleurs, à chaque fois qu'on a identifié une adresse piège, on a tenté de perturber les assaillants en leur envoyant massivement de faux couples login / mots de passe* », dévoile le responsable de la campagne numérique.

Par ailleurs, là encore à la lumière de l'exploitation des mails piratés lors de la campagne présidentielle américaine, l'équipe d'En Marche a décidé de ne pas trop avoir recours à cette forme de communication pour les échanges sensibles, préférant les messageries chiffrées ou les systèmes d'échange de documents.

Pawn Storm, industriel du phishing

Si le rapport de Trend Micro, que nous avons pu consulter en amont de sa sortie officielle, ne comporte qu'une seule URL reliée au candidat Macron, nos confrères de *l'Express* mentionnent d'autres domaines (comme mail-en-marche.fr, repéré le 12 avril) créés par Pawn Storm pour cibler En Marche. De son côté, Mounir Majhoubi indique avoir identifié quelques URL supplémentaires, non signalées par l'éditeur d'outils de sécurité.

L'environnement One Drive associé à Emmanuel Macron figure parmi une liste de plus de 70 domaines créés spécifiquement par Pawn Storm pour ses opérations de phishing ciblant des organisations étatiques, des partis politiques, des organisations internationales ou des médias. « *Pawn Storm est très actif dans les opérations de phishing visant à collecter les codes d'accès des utilisateurs pour mettre en place un espionnage au long cours de l'entité ciblée. Ceci afin de comprendre les orientations de cette entité, voire d'exfiltrer, puis de révéler certains documents par exemple via un site comme Wikileaks* », explique Loïc Guézo, directeur de la stratégie cyber de Trend Micro pour l'Europe du Sud.

La main du Kremlin ?

Si Trend Micro affiche sa confiance dans le fait que l'opération émane bien de Pawn Storm (via notamment des plages d'IP, le mode d'enregistrement des noms de domaine ou le recours à l'hébergeur britannique M247), il se garde bien de pointer la responsabilité directe de Moscou. « *Nous observons simplement que ce groupe prend pour cible des intérêts liés à la politique du Kremlin* », dit Loïc Guézo. Comme le G20, l'Agence mondiale antidopage, le parti démocrate américain ou encore le bureau d'enquête néerlandais en charge des conclusions sur le crash du vol MH17, abattu en juillet 2014 dans la région de Donetsk. Même prudence du côté de l'équipe d'En Marche ou de l'Anssi (Agence nationale de la sécurité des systèmes d'information), elle aussi avertie des opérations de phishing contre Emmanuel Macron par Trend Micro.

Toutefois, plusieurs sources, notamment américaines, relient directement Pawn Storm (ou Fancy Bear ou APT28) aux services secrets militaires russes (GRU), sans toutefois avoir produit, à ce jour, de preuve irréfutable de ce lien. Quoi qu'il en soit, les opérations de phishing à répétition du groupe de hackers contre celui qui apparaît comme le favori du second tour jettent déjà une ombre sur les futurs rapports entre la France et la Russie de Vladimir Poutine.

A lire aussi :

Piratage des élections U.S. : tout a commencé par du spearphishing

Cybersécurité de la campagne : En marche s'inquiète, l'Anssi mobilisée

Chiffrement : Emmanuel Macron marche en rond

Photo E. Macron : mutualite.fr via Visual Hunt / CC BY-NC

Photo M. Majhoubi : swannyyy via VisualHunt / CC BY-NC