Sécurité : la commission des élections US a (aussi) été hackée

Alors que les Etats-Unis menacent la Russie de représailles en raison de son rôle présumé dans les cyberattaques qui ont émaillé la campagne d'Hillary Clinton, l'agence responsable de la certification des machines à voter (U.S. Election Assistance Commission) de la première démocratie mondiale reconnaît avoir été probablement hackée. Cet aveu fait suite à la découverte de plusieurs preuves de ce piratage par une société en sécurité.

Jeudi, Recorded Future indiquait en effet qu'un hacker mettait en vente sur le Dark Web une vulnérabilité inconnue, de type injection SQL, permettant de s'introduire sur le site Web et sur les systèmes de l'Election Assistance Commission (EAC). Cerise sur le gâteau : le même cybercriminel y ajoutait 100 accès aux systèmes de l'agence qu'il présentait comme compromis. Certains de ces accès ayant un niveau administrateur. De quoi accéder à la base de données de cette commission bipartisane, chargée notamment des tests et de la certification des machines à voter, et y implanter des malwares pouvant contaminer d'autres cibles, selon Recorded Future, qui détaille ses trouvailles dans un billet de blog. La société présente le hacker à l'origine de cette vente comme une personne de langue russe connue sous le pseudonyme 'Rasputin'.

Pas de lien avec le Kremlin… pour l'instant

Les chercheurs en sécurité de Recorded Future précisent avoir détecté la mise en vente des éléments qu'affirme détenir Rasputin le 1er décembre. Et avoir alerté les autorités dans la foulée. Rasputin espère vendre ses données pour une somme comprise entre 2 000 et 5 000 dollars. Se basant sur l'histoire de ce pirate, Recorded Future estime qu'il y a peu de chance qu'il soit soutenu par un service de renseignement.

Dans un communiqué, l'EAC explique « *avoir mis fin à l'accès à l'application (concernée par la faille, NDLR) et avoir commencé à travailler avec les autorités pour déterminer la source de cette activité criminelle* ». Le FBI est sur le pont. En août dernier, ce même FBI recommandait aux responsables de la conduite de l'élection de renforcer la sécurité des systèmes d'enregistrements des votants, après deux failles sur ces systèmes détectés plus tôt au cours de l'été.

Dans un entretien avec nos confrères de *Threapost*, un des dirigeants de Recorded Future explique ne pas croire que la vente de la faille par injection SQL touchant l'EAC soit reliée aux hacking multiples qui ont rythmé la campagne présidentielle américaine, des événements que les services de renseignement US présentent officiellement comme une opération coordonnée de la Russie afin de favoriser l'élection de Donald Trump. Toutefois, Recorded Future ne donne aucune indication sur la date à laquelle cette faille a pu être découverte. De son côté, l'EAC ne précise pour l'heure ni l'exploitation qui a pu en être faite, ni l'étendue du piratage dont il a été victime.

A lire aussi :

Barack Obama en mode cyber-représailles contre la Russie

Donald Trump va-t-il gagner les élections grâce aux pirates russes ?