Des gazoducs ciblés par des cyberpirates prorusses - La Presse+

Des gazoducs ciblés par des cyberpirates prorusses

Dan Bilefsky The New York Times

Selon des documents du Pentagone ayant fait l'objet d'une fuite, un groupe de pirates informatiques, sous la direction du Service fédéral de sécurité russe, pourrait avoir compromis l'adresse IP d'une société canadienne de gazoducs en février et causé des dommages à son infrastructure.

Si l'attaque du groupe cybercriminel Zarya réussit, le rapport des services de renseignement indique que « ce serait la première fois » que la communauté des services de renseignement américains « observe un groupe de pirates informatiques prorusse exécuter une attaque perturbatrice contre des systèmes de contrôle industriel occidentaux ».

Le *New York Times* n'a pas été en mesure de vérifier l'évaluation du renseignement américain de manière indépendante, et l'agence nationale canadienne responsable du renseignement d'origine électromagnétique et de la cybersécurité, le Centre de la sécurité des télécommunications, a déclaré qu'elle ne commentait pas les épisodes spécifiques de cybersécurité.

Deux cyberattaques en dix jours

Selon l'évaluation du Pentagone, le 15 février, Zarya a partagé des captures d'écran avec le Service fédéral de sécurité – la principale agence succédant au KGB, connue sous ses initiales russes, FSB – qui auraient montré que l'attaquant avait la capacité

d’augmenter la pression des vannes, de désactiver les alarmes et de procéder à des arrêts d’urgence d’une station de distribution de gaz non spécifiée au Canada.

« Les agents du FSB s’attendaient à ce qu’une opération réussie provoque une explosion à la station de distribution de gaz, et surveillaient les informations canadiennes à la recherche d’indices d’une explosion. »

– Extrait du rapport du Pentagone

Le 25 février, des cyberacteurs situés en Russie ont compromis l’adresse IP canadienne d’une société de gazoducs dont le nom n’a pas été révélé et ont prétendu que les dommages étaient suffisants pour saper les bénéfices de la société, selon l’évaluation, citant des renseignements d’origine électromagnétique. Selon le rapport, les cyberacteurs ne cherchaient pas à « causer des pertes humaines », mais des dommages économiques. Le 27 février, le groupe avait conservé l’accès à l’adresse IP et se tenait prêt à donner d’autres instructions.

Les adresses IP sont des séquences uniques de numéros attribués à chaque site web, ordinateur, console de jeu ou téléphone intelligent connecté à l’internet.

L’agence canadienne de sécurité des technologies de l’information a refusé de commenter la fuite de renseignements, mais elle a indiqué dans un courriel qu’une récente évaluation nationale de la menace cybernétique avait exprimé des inquiétudes quant à la perturbation potentielle des infrastructures essentielles, en particulier des technologies opérationnelles connectées à l’internet « qui sous-tendent les processus industriels ».

Un précédent américain

Le Canada a été l’un des plus fervents critiques de l’invasion de l’Ukraine par la Russie, imposant des sanctions à plus de 2400 personnes et entités russes.

L’agence fédérale de cyberprotection du Canada avait déjà averti que les pipelines pourraient être touchés par le même type d’attaque numérique audacieuse que celle qui avait visé un important pipeline américain en mai 2021.

À l'époque, l'un des plus grands oléoducs des États-Unis, qui transporte de l'essence raffinée et du kérosène du Texas jusqu'à New York en passant par la côte Est, avait été contraint de fermer après avoir été touché par un rançongiciel, ce qui avait démontré de manière éclatante la vulnérabilité des infrastructures énergétiques aux cyberattaques.

Le rançongiciel est une sorte de piratage moderne qui a pris pour cible des entreprises, des administrations locales et des hôpitaux. Dans certains cas, les victimes reçoivent des courriels avec des liens ou des pièces jointes contenant un logiciel qui crypte les fichiers de leur ordinateur et les retient en otage jusqu'à ce qu'une rançon soit versée.

Les experts affirment que des groupes criminels ayant des liens plus ou moins étroits avec des services de renseignement étrangers sont connus pour agir en leur nom dans le cadre de ces attaques.

Les attaques contre les infrastructures critiques constituent une préoccupation majeure depuis une décennie, mais elles se sont accélérées ces dernières années aux États-Unis et au-delà, à la suite de brèches. Parmi celles-ci, on peut citer l'intrusion de SolarWinds par l'une des agences de renseignement russes, et une autre contre certains types de systèmes conçus par Microsoft, qui a été attribuée à des pirates chinois.

Cet article a été publié à l'origine dans le *New York Times*.

Lisez l'article original du *New York Times* (en anglais, abonnement requis)