Microsoft s'oppose à des hackers « liés » à la Corée du Nord

Microsoft a confirmé cette semaine s'opposer à de présumés pirates informatiques liés à un État. Le groupe, que l'éditeur nomme « Thallium », opérerait depuis la Corée du Nord. L'affaire a été portée devant la cour de district des États-Unis pour le district Est de Virgine.

Les arguments du Microsoft Threat Intelligence Center (MSTIC) et du Digital Crimes Unit (DCU) de la firme de Redmond ont été versés au dossier.

Thallium aurait exploité un réseau de dizaines de sites web, de domaines et d'ordinateurs connectés à Internet. « Ce réseau a été utilisé pour cibler les victimes, puis compromettre leurs comptes en ligne, infecter leurs ordinateurs, mettre en péril la sécurité de leurs réseaux et voler des informations sensibles », a déclaré Microsoft dans un billet de blog.

Le groupe de hackers aurait ciblé des organisations et des individus travaillant depuis les États-Unis, le Japon ou la Corée du Sud sur la prolifération nucléaire, pour la plupart. Parmi eux se trouvent des agents fédéraux, des universitaires et des groupes de réflexion.

Plusieurs ont été « harponnés ».

Harponnage et malwares

Thallium aurait utilisé des techniques éprouvées d'harponnage (spear phishing) pour cibler des profils spécifiques et tromper leur vigilance à l'aide de courriels personnalisés. Ces derniers semblaient assez légitimes et crédibles pour tromper des chercheurs.

Ces messages contenaient en fait des liens frauduleux qui, une fois cliqués, s'ouvraient sur une page web demandant aux internautes des informations d'identification. Certains ont ainsi transmis, à leur insu, leurs identifiants à des hackers. Thallium utilisait également des logiciels malveillants (malwares) pour compromettre les systèmes et exfiltrer des données.

Après « Barium » (qui opérait depuis la Chine, selon Microsoft), « Strontium » (Russie) et « Phosphorus » (Iran), « Thallium » (Corée du Nord) est le quatrième groupe de hackers soutenu par un État-nation contre lequel Microsoft dit s'être opposé en justice.

Les autorités américaines, de leur côté, ont désigné deux des sponsors présumés de hackers – la Corée du Nord et l'Iran – comme des « États soutenant le terrorisme ». Elles sont aussi en conflit commercial avec la Chine et elles entretiennent des relations ambiguës avec la Russie.

(crédit photo © shutterstock)