Professeur Yuval Shavitt, DPT chez BGProtect – séance du 20 février 2019, SECU

Je m'appelle Yuval Shavitt, je suis professeur en génie électrique à l'Université de Tel Aviv associée au centre de cyberrecherche interdisciplinaire Blavatnik. Je suis également fondateur et dirigeant principal de la technologie chez BGProtect, une société créée pour défendre les nations et les entreprises contre les attaques de routage, donc de connectivité.

Les attaques relatives au protocole Internet (PI), également appelées attaques de déviation, sont sérieuses car elles ouvrent la porte à de nombreuses variantes d'attaques de l'intercepteur, notamment l'espionnage, la mise à niveau inférieur, le décryptage et l'usurpation d'identité. Ces attaques ciblent principalement les institutions financières compte tenu de leur potentiel lucratif tant pour les organisations criminelles que pour les gouvernements étrangers. Au cours des dernières années, nous avons documenté des attaques de déviation ciblant des organisations financières, qui comprennent de nombreuses banques moyennes et grandes, des bourses, des compagnies d'assurance et des organisations fournissant des renseignements financiers. Les attaques ne se sont pas limitées au détournement de protocole de passerelle frontière, elles ont également compris le réacheminement furtif de trafic aux points d'échange Internet et chez de grands fournisseurs de services Internet. Dans certains cas, il a fallu des semaines avant que les victimes ne se rendent compte de ces attaques.

Que peut-on faire? D'abord et avant tout, le secteur financier devrait exercer une surveillance étroite du routage vers les domaines PI cruciaux, notamment les adresses PI publiques et les serveurs PI comme le courriel, les systèmes d'adressage par domaines (DNS) et les réseaux privés virtuels (RPV). Deuxièmement, une surveillance de l'infrastructure de routage s'imposerait au niveau national pour éviter que des données provenant d'organisations financières ne soient transmises à l'étranger. Enfin, il faudrait mettre sur pied une équipe nationale d'intervention en cas d'urgence informatique (EIUI) – les États-Unis se sont dotés d'un centre de fusion – à qui les organisations financières pourront communiquer des données sur des attaques tout en étant assurées de divers niveaux d'anonymat.

La réglementation fédérale peut également aider à gérer le risque associé aux attaques relatives au protocole Internet (PI). Les lois doivent être mises à jour pour préciser qui peut être autorisé à posséder une infrastructure de communication de données sur un territoire donné. Par exemple, certains fournisseurs Internet internationaux, comme China Telecom, ont des points de présence partout dans le monde, mais la Chine ne permet pas à des fournisseurs Internet étrangers d'être présents sur son territoire. Cette asymétrie donne à China Telecom un avantage indu. Pire encore, même lorsque le coupable est identifié, celui-ci peut très facilement invoquer une erreur de configuration pour éviter les poursuites.

Comme je l'ai mentionné, je suis également dirigeant principal de la technologie chez BGProtect. Cette entreprise est chef de file en matière de détection et d'atténuation des attaques relatives au protocole Internet (PI) et à la couche de données. Notre plateforme et nos services sont actuellement utilisés dans le monde entier par des institutions financières, des gouvernements, des agences de renseignement de sécurité, des fournisseurs de service et des agences de presse internationales. Les récentes attaques ne se limitent pas au protocole de passerelle frontière, elles visent également la couche de données (p. ex. menaces aux routeurs). Notre entreprise offre le seul service capable d'identifier tous les types d'attaques de détournement de données quelle que soit la technique utilisée. Nous avons mis en place des centaines d'agents logiciels sur des serveurs situés partout dans le monde et notre base de données compte plus de 6 000 emplacements d'adresse PI de routeurs qui permettent de fournir des

résultats de mesures en temps réel et d'analyser les réseaux de routes locales et mondiales et de déceler les anomalies au moyen de notre moteur d'intelligence artificielle.

En ce qui concerne la question de Huawei, il importe de noter qu'essentiellement tout l'équipement de réseautage et de télécommunication peut être vulnérable à des attaques, notamment par des portes dissimulées, et que la meilleure façon de réduire et d'atténuer les risques consiste à investir dans de l'équipement de surveillance du trafic. En effet, « mieux vaut prévenir que guérir » comme le veut le dicton.