Malgré une diminution des vols de propriété intellectuelle observés ces dernières années, les opérations de cyber espionage chinois continuent de cibler des organisations spécialisées dans des domaines clés de la recherche médicale. Les révélations relatives au groupe APT le plus récent identifié par FireEye — APT41 —, prouvent que les organisations du secteur pharmaceutique et médical sont des cibles de choix. Actif depuis 2012, ce groupe a réalisé des intrusions dans de nombreux autres secteurs d'activités, dont les jeux video, les télécommnuications et l'enseignement supérieur.

L'interêt du secteur medical est illustré par exemple à travers une intrusion dans une organisation de biotechnologie en 2015, lors de laquelle APT41 a dérobé des informations extrêmement sensibles concernant les activités de l'entreprise, incluant les résultats d'essais cliniques sur des médicaments en cours de développement, des données académiques ou encore des données sur le financement du budget de leurs équipes de recherche et développement.

Toutefois, APT41 n'est pas le seul groupe d'espionnage chinois à conduire de telles opérations.

Dès l'année 2014, FireEye a identifié de multiples groupes de cyber espionnage en lien avec la Chine ciblant des centres de recherche médicale, des fabricants de matériel medical, des firmes pharmaceutiques et d'autres organisations liées à la recherche médicale. Ces opérations se sont étendues aux Etats Unis et ciblent souvent des organisations concentrées sur un domaine de recherche particulier: le cancer. Par exemple, plus tôt cette année des acteurs de menaces chinois ont lancé une opération de 'spear phishing' (harponnage) visant un centre de recherche académique spécialisé sur le cancer. Ce même centre a également été ciblé par APT41 à la fin de l'année 2018. En 2017, APT10 a appâté ses victimes en s'appuyant sur deux conférences japonaises sur le cancer. Des tactiques et des cibles similaires ont été rattachées à d'autres groupes de menaces chinois réalisant des campagnes de cyber espionnage dans le monde entier.

Pourquoi cet intérêt particulier pour les centres de recherche contre le cancer? Confronté à une multiplication des cas de cancer et au vieillissement de sa population, le gouvernement chinois a mis l'accent dans ses programmes futurs tels que Made in China 2025 sur le développement de l'industrie pharmaceutique nationale. Même s'il est difficile d'évaluer précisément leur ampleur, les années de vols de données d'essais cliniques pourraient commencer à produire des résultats, des entreprises chinoises produisant désormais des médicaments contre le cancer à un coût inférieur à celui des firmes occidentales. Au delà de la lutte contre le cancer, la Chine a pour objectif de devenir un centre mondial d'innovation dans la biotechnologie, et à ce titre nous n'avons sans doute pas une vision complète de l'impact des cyber intrusions observées dans des centres de recherche médicale pour supporter cet objectif.

De toute évidence, la menace liée au vol de données de recherche médicale n'est pas simplement un problème de cyber sécurité. Plus tôt cette année, plusieurs chercheurs ont été licenciés par le centre de recherche MD Anderson en raison de liens suspectés avec le gouvernement chinois, et le National Institute of Health (NIH) américain a publiquement accru la surveillance concernant des liens potentiels avec l'étranger au sein de centres de recherche. Bien que des opérations d'espionnage traditionnelles via des agents infiltrés puissent jouer un rôle dans le vol de données, des cyber intrusions peuvent permettre de récupérer des informations sur une grande échelle à moindre coût. En raison de la nature des cibles, il est probable que la motivation pour cette activité au sein d'institutions de recherche est différente de celle relative aux opérations d'espionnage chinois contre des assureurs santé ces dernières années. Ces dernières actions peuvent avoir eu pour objectif principal la collecte de larges bases de données en support de futures opérations de renseignement.

L'approche adoptée par les groupes d'espionnage chinois pour cibler des centres de recherche médicale est similaire en de nombreux points à d'autres campagnes visant d'autres domaines importants de recherche. APT40, un autre groupe de menace chinois, a ciblé de

multiples organisations liées à la recherche maritime , dont des universités. Si certaines entités sont perçues comme des cibles moins importantes dans un secteur industriel donné, mais si elles peuvent donner accès aux mêmes données – les acteurs de menaces les attaqueront souvent. Des centres de recherche médicale moins importants pourront en particulier être considérés comme des cibles comparativement plus faciles à compromettre.

L'importance des innovations dans les secteurs de la santé et des biothechnologies pour le développement économique national et la création d'emploi est clair. Adresser la menace contre la domination des Etats Unis dans le domaine de la recherche médicale nécessitera une approche globale impliquant tous les intervenants – administrations publiques, centres de recherche et entreprises. Les organisations dans ce secteur doivent addresser la menace posée par les campagnes de cyber espionage chinois en y intégrant leurs fournisseurs, car même des entreprises dotées de solides fonctions de sécurité peuvent courrir des risques dans l'avenir si certains de leurs partenaires ayant accès à leurs données sont compromis. Garantir la compétitivité future de notre recherche médicale nous imposera d'en faire plus pour sécuriser l'ensemble de l'écosystème.

Luke McNamara, Principal Analyst chez FireEye