LA QUINZAINE
ZOOM

Chine contre États-Unis : la nouvelle guerre numérique

Cinq militaires chinois, experts en cyberattaques, sont accusés par Washington d'espionnage industriel sur des groupes américains. Un autre épisode de la cyberguerre que se livrent les deux géants.

UglyGorilla, WinXYHappy, KandyGoo... Derrière ces pseudos se cachent des cyberpirates chinois, accusés d'avoir pénétré par effraction les systèmes informatiques d'entreprises américaines. Le 19 mai, le FBI a ainsi publié les noms et les photos des cinq accusés, assortis d'une bannière rouge Wanted. Les cinq hommes sont inculpés par le ministère de la Justice américain de piratage informatique et d'espionnage industriel.

Les victimes ? Des grands groupes américains comme le producteur d'acier US Steel ou le spécialiste du nucléaire Westinghouse qui s'est fait dérober les plans d'une centrale de nouvelle génération. Pékin s'est immédiatement offusqué de ces "soi-disant" accusations, les considérant "infondées" et "absurdes". L'événement a pris une tournure diplomatique inédite avec la convocation de l'ambassadeur américain et la promesse de représailles. "On peut s'attendre à ce que la Chine riposte en inculpant quelques militaires américains pour des faits similaires", analyse Yves Tiberghien, directeur de l'Institut de recherche asiatique à l'université UBC de Vancouver.

Guerre sans merci entre les présidents américain et chinois Barack Obama (à droite) et Hu Jintao, le premier accusant le second d'espionnage industriel.

Des attaques en masse. Les pirates, déjà connus des services de renseignement américains, sont affiliés à l'unité 61398, une équipe de cybermilitaires. Les autorités chinoises nient son existence, mais elle a fait l'objet l'an dernier d'un rapport très précis de la société américaine de sécurité informatique Mandiant. Sans équivoque, celui-ci retrace, entre 2006 et 2013, des attaques sur 141 entreprises souvent nord-américaines et le vol de "centaines de téraoctets de données" : plans industriels, informations liées à des projets de fusions-acquisitions, etc.

La firme Mandiant, qui entretient des liens étroits avec l'armée américaine, est parvenue à trouver l'origine géographique des attaques. Un bâtiment de 12 étages situé avenue Datong, dans une zone militaire de Shanghai. Des centaines de hackers y travailleraient et plus de 1000 serveurs tourneraient en permanence.

Leur technique d'approche n'a rien de révolutionnaire. "Ils exploitent le spearfishing, qui repose sur l'envoi d'e-mails piégés aux salariés", explique Emmanuel Fleury, expert en sécurité informatique à l'université de Bordeaux I. Lorsque la personne bernée clique sur le lien, un programme de type JavaScript installe un logiciel sur son disque dur. Dès lors, le pirate peut contrôler le poste de travail à son insu.

Long à la détente. Détournant la boîte mail du PDG de US Steel, Wang Dong a ainsi convoqué des cadres du groupe à une fausse réunion. Ceux-ci devaient cliquer sur un lien qui infectait leur machine... "Dans certaines firmes, ces Chinois ont réussi à accéder à l'intégralité des postes de travail ! souligne Gérôme Billois, expert en cybersécurité chez Solucom et au Cercle européen de la sécurité. Or elles mettent environ deux cent cinquante jours pour détecter une intrusion." De quoi affoler les directeurs informatiques...

Cela dit, les hackers de l'unité 61398 ne brillent pas par leur discrétion. Ainsi, Wang Dong laissait son empreinte UglyGorilla sur les programmes qu'il installait dans les serveurs de ses victimes. Or il utilisait le même pseudo dans sa vie privée pour aller sur les forums d'achats de véhicules. "Ces méthodes sont caractéristiques des pirates d'Asie du Sud-Est : elles sont massives et visent un grand nombre de données. Et ils ont un grand sentiment d'impunité", conclut Gérôme Billois. Interrogés sur cette affaire, les officiels chinois se contentent de hausser les épaules : "Tous les grands pays ont des cyberespions"... ■ THOMAS LESTAVEL

REUTERS – DR

Les cinq cyberpirates recherchés par le FBI sont des militaires expérimentés, tous gradés de l'Armée populaire de libération chinoise.