Chine : cyber-espionnage et attaques informatiques

La Chine utilise le cyberespace pour maintenir sa croissance économique, par l'intrusion informatique dans des entreprises privées surtout asiatiques, et pour accroître sa puissance régionale par l'espionnage militaire, plutôt à l'encontre des pays occidentaux.

C'est ce qui ressort d'une étude sur le cyber-espionnage chinois (2016-2018), publiée par le Centre de réflexions sur la guerre économique en décembre 2018. Seules les forces armées, des agences de renseignement civil ou des sociétés de sécurité chinoises seraient capables d'élaborer et de mettre en œuvre des intrusions informatiques de grandes dimensions, transversales et complexes.

Retard technologique à combler. La dépendance de la Chine à l'égard des technologies de l'information et de la communication (TIC), notamment américaines, et de sa vulnérabilité militaire ont été mis en exergue dans le livre « La guerre hors limites » des colonels chinois Liang Qiao et Wang Xiangsui, publié en 1998. Les TIC permettent en effet d'obtenir des avantages asymétriques dans une guerre qui recouvre la force, armée ou non, militaire ou non, et des

moyens létaux ou non. Extension du champ de bataille, le cyberespace devient vital pour la Chine afin de récolter le plus d'informations possibles, en vue d'établir une asymétrie à son avantage. Les forces armées chinoises ont porté leurs efforts sur les renseignements d'origines humaine, électromagnétique et satellitaire. En 2013, l'entreprise américaine de cyber-sécurité Mandiant a identifié deux unités militaires de cyber-espionnage, installées à Shanghai. Ainsi la « Unit 61398 » a récupéré des térabits (1.000 milliards d'unités numériques) des données de 141 entreprises étrangères. La « Unit 61486 » a surtout ciblé les secteurs de la défense et de la haute technologie. En 2014, le ministère américain de la Justice a accusé cinq officiers chinois de vols de secrets d'entreprises américaines. En outre, l'agence de renseignement NSA a révélé que des hackers chinois avaient réussi des centaines d'intrusions dans des infrastructures aux Etats-Unis. En 2015, Washington et Pékin ont conclu un accord de collaboration pour lutter contre le cyber-espionnage. Ensuite, les agences privées chinoises auraient bénéficié d'une plus grande marge de manœuvre, pour éviter une implication directe de l'Etat. Les plus connues, « Menupass Team » et « UPS Team », ciblent les entreprises spécialisées dans l'ingénierie, l'espace ou les télécommunications aux Etats-Unis, en Europe et au Japon. Par ailleurs, le 13ème plan quinquennal chinois 2016-2020 fixe un objectif annuel de 6,5 % de croissance économique et transfère des fonds d'aide à l'exportation vers des investissements en Chine même. Il porte aussi sur le développement des secteurs technologique, biomédical et énergétique, orientant l'espionnage vers les entreprises étrangères de référence.

Le Japon. Cible de choix en raison de son avance technologique, le Japon a été attaqué par deux groupes de hackers d'origine chinoise. Le premier, « Stone Panda », a cherché à voler le maximum de données à haute valeur ajoutée. Son arsenal visait les universités, les entreprises de haute technologie, notamment pharmaceutiques, et des agences étatiques. Pour tromper ses cibles, « Stone Panda » s'est fait passer, entre autres, pour le ministère japonais des Affaires étrangères. Il a compromis les services d'entreprises de stockage numérique, afin d'exfiltrer une grande quantité des données sans être détecté. Le second groupe, « Bronze Butler », a pratiqué l'hameçonnage des réseaux critiques dans les milieux des biotechnologies, de l'électronique, de la chimie et de l'ingénierie maritime. Non détecté pendant plusieurs années, il est parvenu à récupérer des informations commerciales et des comptes rendus de réunions ainsi que des données de valeur sur la propriété intellectuelle et les spécifications de produits.

La Corée du Sud. Le groupe des hackers chinois « Stuckfly » a notamment ciblé les entreprises sud-coréennes de jeux vidéo, habilitées à délivrer des certificats numériques garantissant la provenance de logiciels et donc leur sécurité informatique. En possession de l'outil d'édition, « Stuckfly » pourrait signer les certificats de logiciels malveillants, qui ne seraient pas bloqués par les anti-virus. S'il est détecté, la société de jeux vidéo risque de voir tous ses certificats considérés comme malveillants et sa réputation ternie.

L'Asie centrale. Malgré un accord entre Moscou et Pékin, similaire à celui entre Washington et Pékin et signé également en 2015, des APT (logiciel malveillant, *voir encadré*) chinois ont ciblé des institutions bancaires et des entreprises de télécommunications de la Russie et de la Mongolie, pourtant alliées de la Chine. L'APT « Emissary Panda » s'est aussi attaqué à des infrastructures, institutions bancaires et universités turques. Peu avant des réunions importantes, il a visé l'Organisation de coopération de Shanghai (sécurité mutuelle et coopérations politique et militaire), qui regroupe le Kazakhstan, le Kirghizistan, le Tadjikistan, l'Ouzbékistan, la Russie et…la Chine !

L'Asie du Sud-Est. L'APT « Lotus Blossom » a attaqué des institutions gouvernementales, des partis politiques, des universités et des entreprises de télécommunications en Indonésie, à Taïwan, au Viêt Nam, aux Philippines, à Hong Kong, en Malaisie et en Thaïlande. Il a également procédé à des intrusions lors des réunions des ministres de la Défense de l'Association des nations d'Asie du Sud-Est (Indonésie, Malaisie, Philippines, Singapour, Thaïlande, Brunei, Viêt Nam, Laos, Birmanie et Cambodge). L'APT « Platinum » a notamment visé les services diplomatiques et les agences de renseignement et de défense de Malaisie et d'Indonésie. L'APT « Mofang » a participé à une guerre économique en Birmanie. Dans le cadre d'un appel à investissements pour le développement d'infrastructures, il a récupéré des informations sur le concurrent singapourien d'une entreprise publique chinoise…qui n'avait pas été retenue.

Les « cinq poisons » chinois. Des cyberattaques chinoises visent des communautés considérées comme déstabilisatrices : Ouighours ; Tibétains ; secte du Falun Gong ; Mouvement démocratique chinois ; Mouvement pour l'indépendance de Taïwan. Pourtant, elles n'ont pu empêcher, en 2016, l'élection de la première femme présidente de Taïwan, Tsai Ing-wen, confortablement réélue en 2020.

Loïc Salmon

Les « menaces persistantes avancées » (APT) exploitent le maximum de données de leurs cibles par des cyber-attaques discrètes et prolongées, grâce à des groupes aux connaissances techniques pointues et des moyens importants. L'Union africaine a constaté, au bout de six ans, que son immeuble, construit et équipé gratuitement par la Chine, comportait des « backdoors » (portes numériques dérobées) donnant un accès discret aux échanges et à la production interne de l'organisation. Le cycle APT a été le suivant : organisation en fonction de la cible (don de l'immeuble) ; stratégie (hameçonnage par des courriels et backdoors) ; moyens techniques pour accéder à son réseau (systèmes informatiques installés et compromis) ; couverture pour maintenir l'accès pour de futures initiatives (logiciels malveillants sophistiqués).

Chine : montée en puissance régionale et internationale

Intelligence économique et renseignement

Cyber : instrument de la puissance russe en Baltique