Le cyber espionnage chinois

Julia Frémicourt, Yves Parent, Hichem Sall

Introduction

Le cyber espionnage chinois est mené notamment par les biais des APT “Advanced Persistent Threat” (menace persistante avancée) : un type de piratage informatique furtif et continu, souvent orchestré par des humains ciblant une entité spécifique. Le mode opératoire des APT est de plus en plus structuré pour aboutir des objectifs économiques sans déployer les ressources nécessaires pour les recherches visant certains domaines. Le but est d’affaiblir la concurrence grâce à l’exploitation de leur savoir-faire qui est transformé et intégré dans les entreprises chinoises pour créer un véritable avantage économique. Les cas de cyber espionnage analysés dans ce rapport portent sur les deux dernières années.

1) L’espionnage au service de l’ambition chinoise

L’analyse du modus operandi nous montre que nous sommes confrontés à une culture d’espionnage qui est l’héritage d’une tradition très ancienne. Le but est à la fois d’améliorer notre connaissance du cheminement chinois en matière de cyber espionnage, de comprendre les choix politiques qui ont été effectués pour atteindre les objectifs économiques et comprendre les enjeux des APT (advanced perseistent threats) grâce à l’aide d’études de cas.

La culture de l’espionnage en Chine

La conception que la guerre puisse être gagnée sans affronter directement l'adversaire est ressortie, pour la première fois, sous la plume de Sun Tzu immortalisé par la célèbre formule : la guerre peut être gagnée sans combattre, grâce à l’anéantissement de la volonté de se battre chez l’adversaire[1].Cette stratégie, ainsi subtile que difficile à maitriser, repose sur la priorité accordée à l’information. Il faut connaître les adversaires afin d’y pouvoir comprendre la logique et le mode d’opérer. Il n’est pas anodin que Sun Tzu ait consacré le XIII article de son ouvrage à l’emploi d’espions car “une armée sans agents secrets est un homme sans yeux ni oreilles”. L’espionnage est un moyen qui permet de soumettre l’adversaire et de gagner la guerre sans combattre ; il est la ressource la plus indispensable pour obtenir des avantages stratégiques sur l’adversaire : d’ici l’asymétrie qui imprègne la guerre y compris la guerre économique.

L’espionnage a joué en Chine un rôle essentiel dans les efforts des dynasties pour gérer les relations avec les tribus nomades et barbares, qui dans l'histoire ont constitué la source externe majeure de menaces[2]. Toutefois l’espionnage n’a pas été une caractéristique majeure de l’intelligence chinoise jusqu'à récemment. À la naissance de la République Populaire Chinoise, les activités en matière d’espionnage étaient des actions visant à découvrir les opposants internes à l'hétérodoxie idéologique. C’est l’ouverture sur l'extérieur qui a incité la Chine à collecter des informations sur les activités des autres pays. Les années 2000s ont vu la Chine consacrer de plus en plus à la fois argent et moyens aux activités d’intelligence visant à combler le gap entre la Chine et le monde développé. Afin de combler le fossé entre les capacités technologiques avec l'Ouest, la Chine a développé en 1986 le plan 863[3]. Il était conçu pour enrichir les compétences technologiques chinoises dans le but d’éliminer la dépendance aux technologies étrangères.

[1] Sun Tzu - L’art de la guerre, III Article, p. 12 - décembre 2003.
[2] Jon R. LINDSAY, Tai MING CHEUNG, Derek S. REVERON, China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, avril 2015, p. 30.
[3] Ibid, p 34.

Les carences de la surveillance américaine

Il y a eu un cas très célèbre en l'an 1999. Tandis que l'administration Clinton cherchait d'étendre les relations diplomatiques et commerciales avec la Chine, cette dernière essayait de collecter des infos sur l'appareil nucléaire américain. En 1992, le Laboratoire National de Los Alamos (LANL) a étudié les essais nucléaires chinois et a découvert un avancement soudain dans la miniaturisation des têtes nucléaires chinoises. Les résultats auxquels les Chinois étaient parvenus présentaient une similarité avec les outils américains (notamment avec l'ogive nucléaire W-88) qui ont conduit Robert M. Henson, un concepteur d'armes de Los Alamos, à croire que la seule façon de Pékin pour avoir faite de telles avances était en volant des secrets américains. L'affaire a été remis entre les mains de Notra Trulock, directeur de l'intelligence du Departement of Energy qui a ouvert une enquête en 1995. Compte tenu de l'extrême similarité de l'ogive nucléaire, les enquêteurs ont suivi trois critères pour trouver le responsable de la fuite d'informations : les individus qui avaient voyagé en Chine entre 1984 et 1988 ; les Individus avec le l'autorisation pour travailler avec des données d'armes nucléaires ultrasecrètes, les Individus qui ont traité des délégations de visite de la Chine.
La seule personne à répondre aux trois critères était Wen Ho Lee, un spécialiste du nucléaire. Cependant, la faiblesse des recoupements d'informations obtenues conduit les recherches dans l'impasse jusqu'au 1998. En 1998, un comité spécial, dirigé par Christopher Cox, a tenu des auditions sur le transfert de technologie en Chine, en se concentrant sur l'espionnage nucléaire chinois. Notra Trulock a témoigné devant ce Comité, que le chercheur chinois Wee Ho Lee avait volé le design du W-88. En décembre, le FBI a dit au comité en question que le Chinois sur lequel pesaient les soupçons était toujours à LANL avec ses habilitations de sécurité inchangées. Après enquêtes supplémentaires, l'analyse de son ordinateur et la révélation publique de cette affaire par les biais de New York times, ont abouti à l'arrestation de Wee Ho Lee[4].

La Chine se lance dans le cyber-espionnage

Même si la Chine est arrivée relativement tard au cyberspace, elle a su compenser assez vite son retard technologique. Le premier problème qui s'est posé a été la dépendance chinoise aux informations communications technologies (ICT) étrangères, notamment américaines. Ce point de vulnérabilité a été rapidement mis en exergue par les colonels Liang Qiao et Wang Xiangsui qui ont publié le livre *la Guerre hors limites* en 1998. Cet ouvrage s'inscrit dans l'esprit du plan 863. Il place l'emploi d'ICT américaine comme la possibilité pour ces derniers de s'en servir pour obtenir des avantages asymétriques. Le livre a révolutionné le paradigme de la guerre : "la guerre recouvre tous les moyens, dont la force armée ou non armée, militaire ou non militaire et des moyens létaux ou non létaux pour obliger l'ennemi à se soumettre à ses propres intérêts."[5]. Par conséquent, le champ de bataille s'tend désormais à un nouveau domaine, le cyber espace qui est devenu une plate-forme vitale pour la Chine afin de récolter plus informations possibles afin d'établir une asymétrie a son propre avantage.
La littérature ouverte sur le cyber espionnage chinois est très réduite. La recherche est minée par un déficit informationnel qui complique ce que on appelle l'attribution" : c'est à dire l'imputation de responsabilité dans le cas d'un acte de cybercriminalité à une certaine entité qu'elle soit d'origine étatique ou pas. Toutefois, les premières années du XXIè siècle ont été témoin d'une croissance rapide et massive des opérations d'exploitation cyber émanant apparemment de la Chine, qui a visé les systèmes classifiés de gouvernements et des sociétés

[4] Phersion Associates - Wen Ho Lee Case Study, octobre 2008.
[5] Liang QIAO, Wang XIANGSUI - La guerre hors limites, Rivage Poche, mars 2006.

majeures. L'année 2003 marque un tournant historique avec une série d'intrusions sur les réseaux du gouvernement américain et des entrepreneurs majeurs : cette opération est reconnue sous le nom de Titan Rain[6]. Après 2003, plusieurs activités d'espionnage visant à exploiter le cyber espace pour obtenir des informations secrètes des entreprises majeures, ont été découvertes par les gouvernements occidentaux. Encore une fois, le problème d'attribution n'est pas anodin.
On peut identifier trois étapes du processus chinois :

- La première c'est l'acquisition, le but est de soutirer des informations
- La deuxième c'est l'absorption : le transformer en output made in china.
- La troisième c'est l'application : Cette innovation industrielle, obtenue par des moyens illicites vise à instaurer un avantage compétitif sur l'entreprise détentrice du savoir-faire ciblé[7].

Pour ne mentionner qu'un exemple, l'entreprise de téléphonie canadienne Nortel, dans les années 2000 a été victime d'un piratage massive d'origine chinois visant à exploiter les secrets du colosse industriel pour créer des avantages au service de l'étoile montante des télécommunications chinoises : Huawei[8].
Le 13éme plan quinquennal 2016-2020 est un fil conducteur pour aider les observateurs internationaux à tracer la direction vers laquelle la Chine s'est engagée à partir de quelques observations sur certains points du plan.
Le gouvernement chinois a établi un objectif de croissance économique à 6,5%[9] dans le dessein de soustraire les fonds à l'export et les convertir en investissements internes au pays. Les secteurs technologique, biomédical et énergétique sont les trois axes de développement prévus pour l'horizon 2020. Ces domaines d'activités peuvent orienter les activités d'espionnage afin de bénéficier des informations confidentielles tirées de l'observation des entreprises étrangères leaders dans le secteur de référence.

L'organisation de l'espionnage chinois en matière de cyber

Après l'analyse de la logique qui se cache derrière les attaques d'origine chinoise, il faut examiner les acteurs majeurs qui peuvent élaborer et mettre en œuvre des attaques de grandes dimensions, transversales et complexes.
Les cyber-attaques chinoises peuvent potentiellement venir de 3 sources différentes :

- L'armée chinoise.
- Agences de renseignement civil et société de sécurité.

L'armée chinoise

La première source qui nous se présente est l'armée chinoise, responsable de plusieurs *computer network opérations* (CPO) c'est à dire de l'ensemble des opérations qui sont menées sur internet.

Avant la réforme du 2015

Avant la réforme qui a concerné l'Armée Populaire Chinoise (Popular Liberation Army, PLA) en décembre 2015, dans le département d'état-major (DEM), il y avait plusieurs « remparts » qui se concentrent sur les CPO :

[6] James A. LEWIS, Computer Espionage, Titan Rain and China, Center for Strategic and International Studies - Technology and Public Policy Program, décembre 2005.
[7] Jon R. LINDSAY, Tai MING CHEUNG, Derek S. REVERON, China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, avril 2015, pp. 51-80.
[8] CBC - Former Nortel exec warns against working with Huawei – octobre 2012.
[9] Corriereasia - Il 13° piano quinquennale e le nuove prospettive di business in Cina.

- Le deuxième rempart (2/PLA) —> il se concentrait sur l'espionnage humain et sur les opérations d'intelligence (HUMINT)
- Le troisième rempart (3/PLA) —> il se concentrait sur le cyber-espionnage et sur les interceptions électroniques (SIGINT).
- Le quatrième rempart (4/PLA) —> il se concentrait sur la guerre électronique, les interceptions des satellites at les actions d'intelligence dans le domaine électronique (ELINT).

L'action de ces trois départements était synergique, par exemple : un espion du 2/PLA pouvait voler des informations sur un network mais renvoyait vers le 3/PLA qui lançait des attaques versus tel network pour en cacher les traces et s'installer dans le réseau en donnant des données utiles au 4/PLA[10].

Grace à une enquête menée par la compagnie de cybersecurity Mandiant en 2013[11], il a été relevé que le 3/PLA était organisé en 12 bureaux dont le 2éme et le 12éme méritent une attention particulière. Connus sous le nom de Unit 61398 et Unit 61486, les deux bureaux bases à Shanghai ont été deux grands acteurs de cyber espionnage, le cybersecurity Mandiant a attribué à l'Unit 61398 l'exfiltration de térabits des données de 141 entreprises étrangères. L'unit 61486, appelle Putter Panda, cible surtout le target spécifique de la défense et de la technologie[12].

Réforme du 2015

La réforme du 2015, voulue par les leaders chinois, vise à protéger les intérêts du pays au-delà des frontières visibles : l'esprit qui a guidé la réforme, avait pour objet de protéger même les frontières stratégiques du cyber-espace. Le domaine cyber conserve une fonction stratégique soit en temps de guerre soit en temps de paix, pourtant, inévitablement, le contrôle de cette arène publique en temps de guerre accorde à qui le détient un avantage inestimable. C'est pour cela que la création du département du *Strategic Support Force* au sein de la PLA permettait de répondre à ces exigences. Il adopte une mode opératoire encore plus synergique en se concentrant sur trois missions : information support, information warfare et développement des forces[13].

D'un point de vue opérationnelle, au sein du stratégique support force il y a le *network system département* intégrant les départements de la PLA qui s'occupaient des cyber/network opérations, que nous avons déjà évoqué, en concentrant les efforts pour gagner le défi d'une new era dans une seule structure.

Agence de renseignement civil et société de sécurité

La prise en charge des opérations d'espionnage n'est pas le monopole des remparts du PLA, il y a plusieurs groupes de renseignements privés qui ont ciblé des entreprises étrangères pour en dévoiler les secrets. Entre les plus connus sont les groupes du APT10, connus comme Menupass Team, active depuis le 2009, et le groupe APT3, connu comme UPS Team, les deux

[10] Epoch Times - Enorme network cinese di unità militari segrete sta attaccando gli Usa quotidianamente – Novembre 2014
[11] Paolo Messa, L'era dello sharp power, Università Bocconi Editore, Octobre 2018, chap. 6.
[12] Crowdstrike – Intelligence report Putter Panda.
[13] John Costello, China's Strategic Support Force: A Force for a New Era Testimony to the U.S.-China, Economic and Security Review Commission, février 2018.

ciblent le domaine de l'ingénierie, aérospatiale et des télécommunications dans les États-Unis l'Europe et le Japon[14].
Même s'il n'y a pas une claire relation avec le gouvernement chinois, les enquêtes ne semblent pas en mesure d'exclure une synergie entre les plusieurs entités privées de renseignement et le gouvernement chinois. Après le cyber agreement passé entre la Chine même et les États-Unis, il semblerait que Pékin ait accordé une certaine majeure marge de manœuvre aux agences privées, pour éviter le risque d'une implication directe.

Us/Chine cyber agreement

Après les révélations du cybersecurity Mandiant Mandiant en 2014, le Ministère de la Justice américain a officiellement accusé la Chine. Il a accusé 5 officiers de la PLA de voler des secrets des sociétés américaines pour créer un avantage compétitif chinoise ; la Chine, après l'acte d'accusation a protesté contre les dénonciations américaines. En juillet de la même année, la NSA a délivré un rapport qui révélait les centaines d'infiltration cyber réussies par des hackers chinois contre des infrastructures américaines. Lors d'une visite officielle du président chinois Xi Jinping aux Etats-Unis, le Président Obama a abordé le sujet de l'espionnage. Ce sommet a débouché sur un accord signé par les deux présidents, qui avait pour objectif d'accroître la collaboration e la communication sur la lutte contre le cyber espionnage. Avec cet accord, la Chine semblait avoir adopté la position américaine pour ce qui concerne le vol de la propriété intellectuelle. Toutefois, l'accord manquait d'engagements concrets et véritablement réciproques. La formulation de certains dispositifs pouvait être plus précis. Par exemple si à la place de « l'engagement à non conduire et non promouvoir des opérations de vols de secrets commerciaux », le verbe « tolérer » avait été utilisé, le résultat serait-il changé ? Le pacte manque en réalité d'obligations concrètes. En autre, il s'est posé le problème de l'accord sur la signification de certains mots comme cyber criminalité. Si l'accord a été un premier pas vers le dialogue, il n'est resté qu'un premier pas dont le sens profond est régulièrement remis en cause par les événements de cyber espionnage qui ont caractérisé les années de 2016 à 2018.

2) Les APT

Qu'est-ce qu'une APT ?

Les APT (Advanced Persistent Threat) [Persistantes Avancées Menaces] plus communément les menaces persistantes avancées sont des techniques et stratégies d'attaques discrètes et prolongées dans le temps afin d'exploiter le maximum de données sur leur(s) cible(s).

- Les techniques utilisées sont très sophistiquées et se caractérisent par le terme (Advanced) [Avancées].
- La stratégie de continuité d'injection et d'extraction de données de manière perpétuelle et illégale (à l'insu de la cible) se caractérise par le terme (Persistent) [Persistante].
- Des individus ou groupes aux compétences techniques et de moyens bien structurés aux intentions douteuses constituent une menace d'où la notion de (Threat) [Menace].
- Un Advanced Persistent Threat est souvent l'œuvre d'un groupe ou d'une structure stratégique et non pas un individu isolé.

[14] Fireeye - Advanced Persistent Threat Groups.

Les caractéristiques du terme Advanced

Des logiciels malveillants dans le but de nuire à l'insu de la cible et sur une durée plus ou moins longue en fonction des objectifs visés le caractérisent. Plus connus sous le nom de Malware en anglais, les logiciels malveillants peuvent être répertoriés en fonction de leurs actions sur leurs cibles. La stratégie de Persistent [Persistante] se comprend mieux avec cette nouvelle méthode constatée dans le secteur des bâtiments et travaux publics entre la Chine et les pays d'Afrique.

Le don par la Chine à l'Union africaine d'un nouvel immeuble avec un système informatique compris et entièrement équipé par les Chinois n'a pas laissé indifférent les instances internationales. Les systèmes informatiques ont été livrés clé en main. Et les ingénieurs chinois auraient volontairement laissé une faille par des portes numériques dérobées (« backdoors ») qui donnent un accès discret à l'intégralité des échanges et des productions internes de l'organisation. Même si c'est contesté par la Chine, cette méthode inquiète étant donné la position stratégique de la Chine en Afrique. Il a fallu six longues années de pratique du site de l'Union africaine pour constater les failles informatiques exploitées par la Chine.

L'inauguration le 06 novembre 2018 de l'école nationale de la cybersécurité à vocation régionale de Dakar sur le site de l'ENA (Ecole Nationale d'Administration) n'est pas un acte anodin. La Chine projette d'y installer aussi une bibliothèque chinoise très bientôt sous forme de don à l'Etat sénégalais. Ce mélange d'activités sur des sites communs peut entraîner des conflits entre les trois pays. Le Sénégal et la France doivent tirer les leçons du don de l'immeuble de l'Union africaine par la Chine.

Le cycle de vulnérabilité informationnelle des APT s'appuie sur 4 points de base :

- S'organiser spécifiquement en fonction de la cible pour un objectif singulier.
- Tenter de gagner un équilibre dans l'environnement, la tactique commune inclut le phishing par e-mails, portes dérobées ou backdoors.
- Utiliser les systèmes compromis comme accès dans le réseau de la cible.
- Couvrir les voies afin de maintenir l'accès pour de futures initiatives.

Le cycle APT de l'immeuble de l'Union africaine pourrait se présenter comme suit :

1. Organisations
   Mise en place d'un immeuble administratif à titre gratuit sous forme de don.
2. Stratégies
   Mise en place ou intégration d'un système informatique pour le site et mis à disposition gratuitement par les attaquants
3. Moyens techniques
   Mise en place des failles d'entrées dans le système de manière discrète à l'insu de la cible ou des futurs occupants.
4. Assurer sa couverture
   Mise en place de logiciels malveillants pour injecter (insertion de codes) et extraire des données stratégiques de manière continue sur une longue période.

Les problématiques d'attribution

L'attribution est un processus complexe et critique qui correspond à la recherche de l'acteur supposé d'une intrusion informatique. Les chercheurs en sécurité se basent sur plusieurs éléments techniques pour déterminer la provenance d'une attaque. Ils analysent en profondeur chaque trace laissée par le ou les attaquants afin de récupérer une collection

d'indice. Ces derniers serviront ensuite à assurer avec plus ou moins de certitude qui est à l'origine d'une attaque.

Méthodologie des sociétés de cyber-sécurité

Les différentes informations d'intérêt sont de plusieurs types mais se basent essentiellement sur les habitudes et le comportement des attaquants. Les sociétés de cyber-sécurité analysent avec beaucoup de minutie les différents outils utilisés lors d'une attaque ainsi que le mode opératoire :

- Les codes sources des virus utilisés sont disséqués et analysés afin de les rapprocher d'autre attaques connus.
- Les infrastructures utilisées par les attaquants (serveurs, adresses mail) sont également cartographiées et analysées.

Plus « simplement », l'attribution se base également en partie sur des caractéristiques propres aux créateurs des différents outils utilisés comme la langue ou le fuseau horaire. Il est en effet fréquent que les développeurs laissent des commentaires écrit dans leur langue maternelle dans le code source des virus. Les développeurs réalisent également de manière régulière une action dite de compilation où l'heure (avec le fuseau horaire) est alors inscrite dans le programme. Ces deux éléments permettent ainsi de se faire idée sur la nationalité (ou l'ethnie) de l'attaquant.
Enfin, il est également intéressant de ne pas se limiter au « comment » de l'attaque mais également au « pourquoi ». Ce point sera abordé en profondeur plus tard mais l'actualité géopolitique et les pays ciblés lors d'une attaque servent également d'indice lors d'une attribution.
En résumé, les sociétés de cyber-sécurité utilisent tout un panel d'indice pour effectuer avec une assurance variable l'attribution à un pays ou ensemble de pays. C'est l'ensemble de plusieurs éléments (outils, mode opératoire, langue, fuseau horaire) qui permettent à des chercheurs d'affirmer la provenance d'une attaque.

Limitations, tromperie et communication

Néanmoins, il faut tempérer les attributions et communication qui peuvent être faite par les différents acteurs de ce milieu. La plupart des éléments abordés précédemment peuvent être falsifié et vidé de leur valeur. Il est en effet possible d'acheter sur le darknet des outils créés dans d'autre pays et pouvant servir à détourner l'attention.
Par exemple, lors des JO d'hiver de 2018 en Corée du Sud, les infrastructures informatiques ont subi une attaque informatique de grande ampleur (*Olympic Destroyer*). Les différentes entreprises qui ont pu analyser les outils utilisés n'ont à ce jour pas été capable de fournir une attribution avec certitude définitive. L'attaque a été lancé à partir d'outils précédemment attribués à plusieurs groupes connus d'origines chinoises, russes et nord-coréenne[15].
Il existe également des techniques beaucoup plus simples comme la possibilité de travailler en horaire décalé afin d'inscrire un fuseau horaire différent. Il est également possible d'ajouter des commentaires dans d'autres langues dans les outils développés. La CIA a notamment développé un outil spécifiquement dédié à cette tâche nommé *Marble* et l'utilise depuis plusieurs années[16]. Ce dernier est capable de modifier un virus afin de faire croire aux analystes qu'il a été écrit par des personnes parlant chinois, russes, coréen, arabe ou farsi.

[15] Kasperksy - OlympicDestroyer is here to trick the industry, mars 2018.
[16] NextInpact - Wikileaks publie le code source de Marble, un outil masquant la provenance des attaques, mars 2017.

Il existe néanmoins un moyen efficace mais dangereux pour identifier un attaquant : le *hack-back*. Derrière ce terme se cache des représailles visant spécifiquement les infrastructures utilisées par un attaquant. C'est par exemple ce que fit la société Mandiant dans les années 2010 lorsqu'elle lança une attaque sur les infrastructures du groupe nommé APT1[17]. Elle remonta ainsi jusqu'à l'ordinateur utilisé par un des hackers, le prenant en photo et récupérant également son identité précise et sa localisation (des bureaux de l'armée chinoise). Ce processus reste néanmoins très dangereux et la quasi-totalité des acteurs (états exclus) ne s'adonne pas à ce genre de pratique.
En résumé, il reste très difficile d'assurer avec une certitude élevée l'origine des attaquants. C'est pour cette raison que certains pays ne réalisent pas officiellement d'attribution. C'est le cas notamment de la France et de l'ANSSI dont la politique officielle est de ne pas attribuer les attaques sur lesquelles elle intervient. Néanmoins, certains pays, les Etats Unis en tête, ont à plusieurs reprises annoncées publiquement la responsabilité de certains individus dans des attaques informatiques[18]. En absence de preuve, il reste difficile alors de différencier les inculpations avec un fondement technique (campagne de *hack-back* ?) de celles qui ont un but purement politique. L'objectif de ces dernières pourrait ainsi se limiter à une campagne de communication dans le cadre de négociation.
L'attribution est donc une activité critique qui présente une importance stratégique mais qui reste très risqué. En effet, les moyens mis en place par les sociétés qui interviennent après une attaque peuvent être « pollués » par une manipulation possible de la part des attaquants. Néanmoins, il faut également mettre en avant un principe fondamental dans le panorama des cyber-attaques actuelles : la plupart des attaques émanent d'acteurs ne cherchant pas à réaliser des attaques précises et élaborées[19]. En effet, la quasi-totalité des attaques répertoriées ne sont pas des opérations précises et ne justifient donc pas les techniques de tromperie vues précédemment. Cela concerne notamment la majorité des attaques venant de Chine, de Russie et de Corée du Nord. C'est pour cette raison que nous avons choisie de ne pas aller à contre-courant des conclusions tirés par les différentes sociétés de cyber-sécurité ayant attribuées des attaques à des acteurs parlant chinois.

3) Les cyber-attaques chinoises au cours des 2 dernières années

Afin de satisfaire son ambition, la Chine a mis en place un programme d'espionnage informatique de grande ampleur et intégré dans l'appareil d'Etat. A la suite à l'accord signé en septembre 2015 entre la Chine et les Etats-Unis, l'Empire du Milieu a réorienté son dispositif cyber afin de se concentrer, non plus sur les infrastructures du monde occidental, mais aussi sur les pays l'entourant. En effet, le lendemain de la signature de cet accord, les APT chinoise sont devenues silencieuses sur les réseaux américains et anglais[20]. Le cyberespace est donc devenu au cours des deux dernières années un outil majeur de la Chine dans sa quête pour accroitre sa puissance régionale.
La Chine possèderait en effet à ce jour plus de 25 groupes actifs en Eurasie ces deux dernières années[21]. Ces APT sont plus ou moins indépendantes et possèdent chacune une ou des cibles bien particulières. Il est en effet rare de voir deux groupes d'attaquant viser les mêmes entités.

[17] Mandiant – APT1 – Exposing one of China's cyber espionage unit, février 2013.
[18] New York Times - 5 in China Army Face U.S. Charges of Cyberattacks, mai 2014.
[19] Errata Security - How to irregular cyber warfare, octobre 2018.
[20] Kaspersky - Kaspersky Security Analyst Summit, 2016.
[21] Florian Roth – APT Groups and Operations, août 2018.

Nous allons parcourir les différents groupes actifs depuis 2016 en fonction de leur cible, que ce soit un pays, un groupe de pays, des communautés ou une industrie précise.

Le Japon

Le Japon, à cause de son avancée technologique, représente une cible de choix pour l'espionnage économique. Au cours des deux dernières années, deux principaux groupes d'origine chinoise ont été identifiés :

- Stone Panda.
- Bronze butler.

Stone Panda

Derrière ce nom se cache un acteur responsable de plusieurs opérations d'envergure au cours des dernières années. Bien que le domaine de compétences des différentes entités ciblées soient diverses, ces opérations ont en commun un but précis : voler un maximum de données à haute valeur ajoutées pour la Chine. Ce groupe utilise pour cela un arsenal bien spécifique dans le but de pénétrer des institutions académiques, des entreprises de haute technologie (notamment pharmaceutique[22]) et des agences gouvernementales[23]. Ce groupe se fit notamment passer pour des agences publiques japonaises comme le Ministère des Affaires Etrangères dans le but de tromper ses cibles.

Ce groupe se caractérise également par le ciblage spécifique des entreprises mettant à disposition des services numériques (notamment de stockage) à d'autres entreprises[24]. La compromission de tel services permis à cet APT d'exfiltrer une grande quantité de donnée sans être détecter.

Bronze Butler

Actif depuis 2008, ce groupe a, par le passé, ciblé plusieurs pays comme la Russie, Singapour, la Corée du Sud mais se concentre principalement sur le Japon[25]. Cet APT utilise notamment la technique d'hameçonnage ciblé afin de pénétrer les réseaux critiques d'entreprises dans des domaines divers[26]. En effet, les différentes entités concernées opèrent dans le milieu des biotechnologies, de la production industrielle (électronique, chimique) mais également des agences gouvernementales ainsi que l'ingénierie maritime[27]. Ce groupe se concentre sur des entreprises possédant des informations sensibles ou à haute valeur ajoutée[28].

En effet, cet APT réussit à rester invisible à l'intérieur d'infrastructures critiques pendant plusieurs années, aspirant toutes les données de valeurs comme de la propriété intellectuelle, des spécifications de produits mais également des informations commerciales et des comptes rendus de réunion. Le Japon représente une cible de choix et a subi des attaques répétées au cours des dernières années. Ce n'est pas moins de deux groupes, chacun disposant de ses compétences propres et d'un mode opératoire spécifique, qui ont donc la charge de récupérer un maximum d'information pouvant aider la cause chinoise.

---

[22] Paloalto – menuPass returns with new malware and new attacks against Japanese academics and organizations, février 2017.
[23] Trend Micro – ChessMaster makes its move : a look into the campaign's cyberespionage arsenal, juillet 2017.
[24] PWC – Cloud Hopper final report v4, avril 2017.
[25] Trend Micro – Bronze butler's Daserf backdoor now using steganography, novembre 2017.
[26] Secureworks – Bronze Butler targets japanese entreprises,
octobre 2017.
[27] Symantec – Tick cyberespionage group zeros in on Japan – avril 2016.
[28] Paloalto – Tick group continues attacks – juillet 2017.

La Corée du Sud

La Corée du Sud possède une industrie technologique de pointe, notamment dans le domaine de l'électronique. Néanmoins, c'est son industrie du jeux vidéo (la plus développé au monde) qui fut la cible d'attaque ces dernières années de la part d'un groupe nommé *Suckfly*[29].

Ces industries, historiquement peu ciblé par des attaques informatiques, possèdent néanmoins un outil précieux : la capacité de signer des certificats. Derrière ce terme se cache la méthode utilisée dans le monde de l'informatique pour assurer la provenance d'un logiciel via l'utilisation d'un certificat numérique. Cet outil est une pierre angulaire de la sécurité informatique et donc une cible de choix pour des acteurs malveillants.

En effet, si une APT arrive à pénétrer le réseau informatique d'une société éditrice de jeux-vidéo, elle peut également gagner accès à cet outil d'édition de certificat. Une fois sous son contrôle, le groupe peut ainsi, en toute discrétion, signer des virus qui pourront ensuite se propager sans être bloquer par un antivirus. Ce dernier pensera que ce logiciel émane de la société en question et ne relèvera donc pas d'alerte de sécurité.

En conclusion, ce type d'attaque est particulièrement intéressant car il représente également une atteinte à la réputation des sociétés victimes. En effet, l'attaquant se faisant passer pour une société de jeux-vidéo, cette dernière pourrait voir la totalité de ses certificats étiquetés comme malveillant. Cela créerait alors des erreurs de sécurité chez les utilisateurs de ses produits et mettrai à mal à la réputation de l'éditeur.

L'Asie centrale

A la suite à l'accord entre Pékin et Washington de septembre 2015, une réorientation de plusieurs groupes fut observée en direction de la Russie (et des pays voisins) avec une multiplication par 3 des attaques[30]. Plusieurs groupes ont ainsi attaqué la Russie ces dernières années, violant l'accord passé entre Pékin et Moscou en mai 2015, mais également d'autres pays d'Asie centrale. Les principaux groupes sont :

- TA459
- Emissary Panda
- IronHusky

TA459

Groupe actif depuis 2016, cette APT s'est d'abord illustrée par des attaques visant des entreprises d'armement, des militants des droits de l'homme et groupes pro-démocratie en Russie, Mongolie, Biélorussie entre autres[31]. En 2017, cette dernière s'est concentrée sur les institutions bancaires et de télécommunication de ces pays[32].

Emissary Panda

Actif depuis plusieurs années, cette APT chinoise ciblait historiquement des agences gouvernementales américaines et ses partenaires. Près d'un an après l'arrêt officiel du cyber espionnage entre la Chine et les Etats-Unis, ce groupe fut détecté dans les réseaux d'entreprises occidentales de défense. Néanmoins, cela ne brisa pas l'accord car ce dernier concerne l'espionnage économique et non militaire. Le gouvernement chinois utilise cette

[29] Symantec – Suckfly : Revealing the secret life of your code signing certificates – mars 2016.
[30] Darkreading - Chinese Cyberspies Pivot To Russia In Wake Of Obama-Xi Pact, septembre 2016.
[31] Proofpoint - NetTraveler APT Targets Russian, European Interests, juillet 2016.
[32] Proofpoint - APT Targets Financial Analysts with CVE-2017-0199, avril 2017.

faille pour récupérer des données stratégiques d'entreprises concurrente dans le domaine de la défense. C'est le cas notamment d'une société européenne de drone, concurrente de la société *DaJian Innovation Technology*, le leader chinois du marché mondial. Cette entreprise fut victime d'une attaque à travers un de ses ingénieurs ; ce dernier possédant accès à des brevets et autres données sensibles[33].
Ce groupe se démarqua également lorsqu'il attaqua en 2016 les infrastructures gouvernementales turques ainsi que ses institutions bancaires et académique[34].
En 2018, cette APT s'est principalement concentrée sur la Mongolie qui accueilli plusieurs sommets de dirigeants asiatique[35]. Depuis l'élection en 2017 d'un président pro-russe, le gouvernement mongoliens a rompu avec la politique extérieure historique de neutralité[36]. Ses choix politique et économique représentent donc un intérêt particulier pour la Chine.
Enfin, ce groupe visa également les membres de la *Shangai Cooperation Organization* à l'approche des réunions importantes de cette dernière ; et ce malgré que la Chine soit à l'initiative de cette organisation[37].

IronHusky

Groupe chinois actif depuis le printemps 2017, ce dernier semble suivre l'agenda géopolitique d'Asie centrale et particulièrement celui de la Mongolie. Cette APT a en effet créé des virus spécifiques et visant des acteurs importants. Ce fut notamment le cas lorsque ce groupe s'attaqua à des acteurs participant aux réunions entre la Mongolie et le FMI en janvier 2018[38].
Les pays d'Asie centrale, la Russie et la Mongolie en première ligne, connaissent une vague inédite d'attaque informatique depuis la signature de l'accord entre Pékin et Washington. Bien que ces pays soient des alliés de la Chine, cela n'a pas empêché cette dernière de mettre en place un système d'espionnage avec un panel de cible large. En effet, aussi bien les groupes pro-démocratie que des sociétés ou des organisations gouvernementales furent la cible de ces APT au cours des deux dernières années.
Cependant, il est intéressant de noter que les attaques subies par les pays d'Asie centrale touchent également les pays officiellement alliés avec Pékin. De plus, il semblerait que la Chine n'hésite pas à s'attaquer à un allié possédant également un programme de cyber-espionnage développé comme la Russie. Ceci est particulièrement intéressant alors que ces deux pays avaient également signé un accord du même type que celui entre la Chine et les Etats-Unis.

L'Asie du Sud-Est

Les pays d'Asie du sud-est, bien que ne représentant pas une menace directe pour Pékin et ses ambitions, restent néanmoins victimes de plusieurs campagnes d'attaque informatique. En effet, plusieurs APT d'origine chinoise ont, au cours des dernières années, prisent pour cible spécifiquement des pays d'Asie du Sud-Est à travers leurs institutions ou leurs entreprises.

[33] Threat Connect - ThreatConnect identifies Chinese targeting of two companies. Economic espionage or military intelligence? octobre 2016.
[34] Secureworks - BRONZE UNION Cyberespionage Persists Despite Disclosures, juin 2017.
[35] Kaspersky – APT trends report Q2 2018, juillet 2018.
[36] The Asan forum - As China and Russia Draw Closer, Mongolia Feels the Squeeze, octobre 2018.
[37] Kaspersky - LuckyMouse signs malicious NDISProxy driver with certificate of Chinese IT company, septembre 2018.
[38] Kaspersky - APT Trends report Q1 2018, avril 2018.

Thrip

Ce groupe a mis en place au cours des dernières années une vaste campagne d'espionnage visant les entreprises numériques en Asie du Sud-Est[39]. Ces dernières évoluent dans le domaine des télécommunications, de l'imagerie satellite ou de la défense.
Lors des attaques, cette APT ne se concentrent pas sur les données des clients mais sur l'aspect opérationnel et le savoir-faire de l'entreprise. Par exemple, à la suite à une intrusion dans une société d'imagerie satellite, cet acteur s'est attaqué spécifiquement aux infrastructures hébergeant un logiciel de traitement de données géographiques.
Un point intéressant est le potentiel destructeur des attaques menées. Alors qu'il était possible de sérieusement endommager les infrastructures de télécommunications d'un pays, cet acteur s'est contenté d'extraire des informations à haute valeur ajoutées.

Lotus blossom

Cette APT est active dans les territoires autour de la mer de Chine du Sud depuis près de 6 ans. Elle a mené plusieurs campagnes d'attaque en visant des organisations gouvernementales, des parties politiques, des universités mais également des entreprises de télécommunication. Les principaux pays visés regroupent l'Indonésie, Taiwan, le Vietnam, les Philippines, Hong Kong, la Malaisie et la Thaïlande[40].
La carte suivante permet de se rendre compte du nombre de pays qui furent, au moins une fois, victime de cet acteur. La fréquence des attaques est indiquée et va du jaune pour les moins touchés au rouge pour les pays les plus touchés.

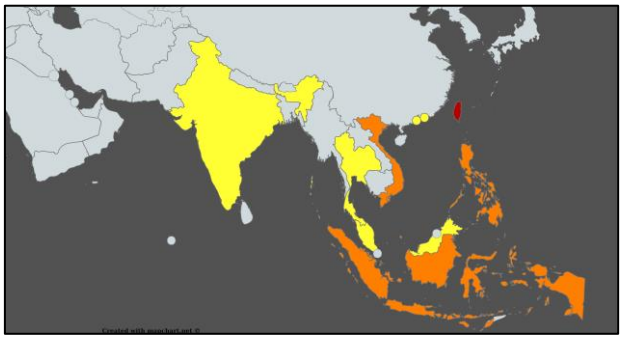

Figure 1: Lotus Blossom targets frequency - Kaspersky

Plus récemment, ce groupe s'est attaqué à l'ASEAN, l'Association des nations de l'Asie du Sud-Est, une organisation politique et économique regroupant dix pays d'Asie du Sud-Est[41]. Les réunions du groupe de défense de l'association (ADMM pour *ASEAN Defence Ministers' Meeting*) furent particulièrement visées lors des dernières campagnes d'intrusion[42].

Platinum

Actif depuis 2009, cet acteur ne semble pas avoir d'agenda spécifique mais est opportuniste dans le choix de ses cibles. Ce groupe change en effet de profile et de région au fil du calendrier géopolitique et s'attaque majoritairement à des pays d'Asie du Sud-Est (notamment la Malaisie et l'Indonésie). Concernant les entreprises visées, les institutions gouvernementales,

[39] Symantec - Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies, juin 2018.
[40] Kaspersky - Spring Dragon – Updated Activity, juillet 2017.
[41] RSA - Lotus Blossom Continues ASEAN Targeting, février 2018.
[42] Accenture – Dragonfish delivers new form of elise malware targetting ASEAN defence ministers' meeting and associates, janvier 2018.

diplomatique ainsi que les agences de renseignement ou de défense restent le choix privilégié de cette APT[43].

DragonOK

APT découverte en 2014, elle s'est d'abord attaquée à des entreprises et individus d'origine japonaises, taiwanaise, tibétaine ou russe[44]. Ces intrusions utilisaient principalement la technique de l'hameçonnage ciblé pour pénétrer des réseaux. Les entités les plus touchées évoluent dans le domaine de la production industrielle, de l'éducation, de l'énergie ou de la technologie.
Depuis le début de l'année 2017, ce groupe a ajouté les parties politiques cambodgien à la liste de ses cibles d'intérêt[45].

Mofang

Mofang est un acteur chinois dont on retrouve la trace sur tous les continents et pays : en Allemagne, au Canada, aux Etats-Unis, en Inde, à Singapour et en Corée du Sud. Néanmoins, c'est la campagne lancée contre la Birmanie qui permet de se rendre compte de l'ambition chinoise et des moyens développés.
Depuis 2009, l'investissement étranger en Birmanie est passé de 300 millions de dollars à plus de 20 milliards de dollars ces dernières années. Cet investissement se concentre au sein de *sezs*, des zones économiques birmane spécifiques où des arrangements ont été réalisés afin d'attirer des entreprises étrangères. La Chine fut un des premiers pays à s'engouffrer dans la brèche, notamment avec la *China National Petroleum Company* qui se positionna pour développement et l'exploitation d'un pipeline de gaz et de pétrole.
Néanmoins, alors que les deux gouvernements avaient signé un accord tacite sous la forme d'un *Memorandum of Understanding (MoM)*, la Birmanie lança un second appel d'offre. Ce dernier avait pour but de trouver l'entreprise qui accompagnerait le gouvernement de la *sezs* dans la future gestion de ses opérations et investissements. Ce fut la société singapourienne *CPG Consultant* qui remporta la mise et qui allait donc accompagner le gouvernement birman dans son développement économique. La première brique fut la création d'un appel d'offre en 2014 pour l'investissement dans les infrastructures de la zone économique. Le gouvernement chinois répondit à cet appel avec la société *CITIC Group*. Cependant, alors que le gouvernement birman tardait à publier les résultats, l'entreprise singapourienne *CPG Consultant* commença à subir des attaques de la part de l'APT Mofang[46]. Nous sommes donc ici dans un cas bien précis où le but n'est pas le vol de données brut mais bien la recherche d'information dans un contexte de guerre économique précis.
L'Asie du Sud-Est subit donc un assaut organisé et dévastateur depuis de nombreuse années de la part d'acteurs d'origine chinoise. Ces derniers s'intéressent à toutes les entités qui pourraient posséder une information de valeur comme des entreprises évoluant dans des domaines stratégiques, des universités ou des partis politiques.
Cependant, c'est la capacité à mettre en place une attaque sur un acteur particulier dans un contexte précis qui est particulièrement intéressante. En effet, contrairement aux attaques « habituelles » dont le mode opératoire est adapté pour toucher un maximum de victime

[43] Microsoft - Digging deep for PLATINUM, avril 2016.
[44] Paloalto - DragonOK Updates Toolset and Targets Multiple Geographic Regions, janvier 2017.
[45] Forcepoint - Trojanized Adobe installer used to install DragonOK's new custom backdoor, mars 2017.
[46] Fox It - Mofang: A politically motivated information stealing adversary, juin 2016.

possible, cette dernière avait un objectif bien précis dans une fenêtre de temps critique et concernait directement les intérêts d'une entreprise nationale chinoise.

Les cinq poisons

Derrière ce terme issu du folklore chinois se cache cinq communautés qui ne représentent pas une menace directe envers l'économie chinoise mais qui possèdent un pouvoir de déstabilisation important. Ces 5 poisons sont :

- *Les Ouïghours,*
- *Les Tibétains,*
- *Les adeptes du Falun Gong,*
- *Les membres du mouvement démocratique chinois,*
- *Les membres du mouvement pour l'indépendance de Taïwan.*

Ce n'est donc pas seulement dans un contexte d'espionnage économique que des acteurs chinois se sont intéressé à des entités appartenant à ces différents peuples ou mouvements.
Un groupe fut responsable d'attaques contre les membres du parlement tibétains (la plus haute organisation politique du gouvernement en exile)[47]. Ces intrusions suivaient un agenda bien précis comme des protestations ou des démolitions d'école bouddhiste. Un autre groupe visa spécifiquement des acteurs hongkongais participants à des évènement pro-démocratie[48].
Enfin, un 3ème groupe prit pour cible uniquement les activistes des communautés tibétaines et Ouïghours[49].
Enfin, une APT portant le nom de « *The Four Element Sword* » est active depuis plusieurs années et s'attaque uniquement à des entités tibétaines, hongkongaises ou taiwanaises. Ce groupe s'est attaqué à de multiples reprises à des communautés tibétaines ainsi qu'à des journalistes originaires de Taiwan ou Hong-Kong[50]. Cette APT semble se consacrer entièrement à des groupes émanant de la société civile et dont la cause commune est la démocratie[51]. Cet acteur fut notamment actif lors de l'élection, en janvier 2016, de la première femme présidente de Taiwan[52].

L'ingénierie maritime

Là où les APT décrites jusqu'à présent choisissaient leurs cibles géographiquement, un groupe du nom de *Leviathan* ne s'attaque qu'à des entreprises travaillant dans le domaine de l'ingénierie maritime.
Cette APT, active depuis 5 ans, a en effet pris pour cible tout ce qui touche de près ou de loin à l'ingénierie maritime[53][54] : industrie navale, prestataire de défense évoluant dans le domaine maritime, institut de recherche mais également des sociétés de transport. De plus, ce groupe ne se contente pas d'une région géographique et est actif en Amérique du Nord, en Europe et en Asie du Sud-Est.

[47] Citizen Lab - It's Parliamentary KeyBoy and the targeting of the Tibetan Community, novembre 2016.
[48] Palo alto - New Poison Ivy RAT Variant Targets Hong Kong Pro-Democracy Activists, juin 2016.
[49] Palo alto - Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists, janvier 2016.
[50] Asert - The Four Element Sword Engagement, mars 2016.
[51] Citizen Lab - Between Hong Kong and Burma, mars 2016.
[52] PWC - Taiwan Presidential Election: A Case Study on Thematic Targeting, mars 2016.
[53] Proofpoint - Leviathan: Espionage actor spearphishes maritime and defense targets, octobre 2017.
[54] Fireeye - Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries, mars 2018.

Les Etats-Unis

Après la signature d'un accord sur l'espionnage économique entre les Etats-Unis et la Chine, une recrudescence des attaques de cette dernière a été observé par la majorité des sociétés de cyber-sécurité. Néanmoins, cet accord ne concernait pas l'espionnage à des fins militaires. En effet, bien que l'espionnage économique envers les Etats-Unis ait diminué, cela ne signifie pas que Washington n'est plus la cible de groupe d'hacker d'origine chinoise. Pas moins de deux APT historiques (*UPS* et *Mirage*) se sont attaquées à des organisations ou entreprises occidentales. *Mirage* s'attaqua au cours des deux dernières années à des prestataire du gouvernement anglais à la recherche de données militaires confidentielles[55] tandis que *UPS* s'attaqua à des prestataires de la marine américaine[56]. Néanmoins, en ce qui concerne le groupe dénommé UPS, ce dernier semblerait avoir changé de cible et consacrerait majoritairement à des organisations et mouvement politique hongkongais[57].

A la suite de l'accord entre Pékin et Washington, une réorientation des différentes APT chinoise a été observé. Visant historiquement les pays occidentaux, ces groupes se concentrent à présent en majorité sur l'Asie.

Au cours des deux dernières années, a quasi-totalité des pays entourant la Chine ont subi une ou plusieurs attaques de la part d'acteurs malveillants d'origine chinoise. Bien qu'il soit impossible d'assurer que le gouvernement chinois est à l'initiative de ces attaques, les entreprises visées et parfois le timing des intrusions ne laissent que peu de doute pour certains cas sur les motivations des attaquants.

En effet, bien que certaines campagnes aient eu pour objectif la surveillance (*5 poisons*), la quasi-totalité des intrusions avaient clairement un objectif d'espionnage économique. De plus, les entreprises visées évoluaient dans la majorité des cas dans des domaines d'intérêt identifiés dans le 13ème plan quinquennal chinois.

Outre les activités de cyber-espionnage économique, plusieurs points d'intérêts ont été observés. Le premier est l'association d'une intrusion informatique avec une attaque contre la réputation d'une entreprise comme ce qui a été réalisé à l'encontre des sociétés de jeux-vidéo sud-coréenne. Le second est la capacité d'entités chinoises à s'attaquer à des alliés de Pékin qui ont la particularité de pouvoir répondre sur le champ du cyberespace, comme la Russie. On peut également citer les intrusions estampillées espionnage militaire en fonction des entreprises visées, mais dont les documents extraits ne présentaient un intérêt que pour une société civile chinoise concurrente de l'entreprise victime.

De plus, certaines cibles déviaient du profil type habituel. C'est le cas notamment des groupes s'attaquant aux communautés appartenant aux « cinq poisons » ou celui spécialisé dans les sociétés d'ingénierie maritime. Enfin, bien que les Etats-Unis ne soient officiellement plus une cible pour l'espionnage économique, des APT restent actives dans un contexte d'espionnage militaire.

[55] NCC Group - APT15 is alive and strong: An analysis of RoyalCli and RoyalDNS, mars 2018.

[56] Washington Post - China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare, juin 2018.

[57] Symantec - Buckeye cyberespionage group shifts gaze from US to Hong Kong, septembre 2018.