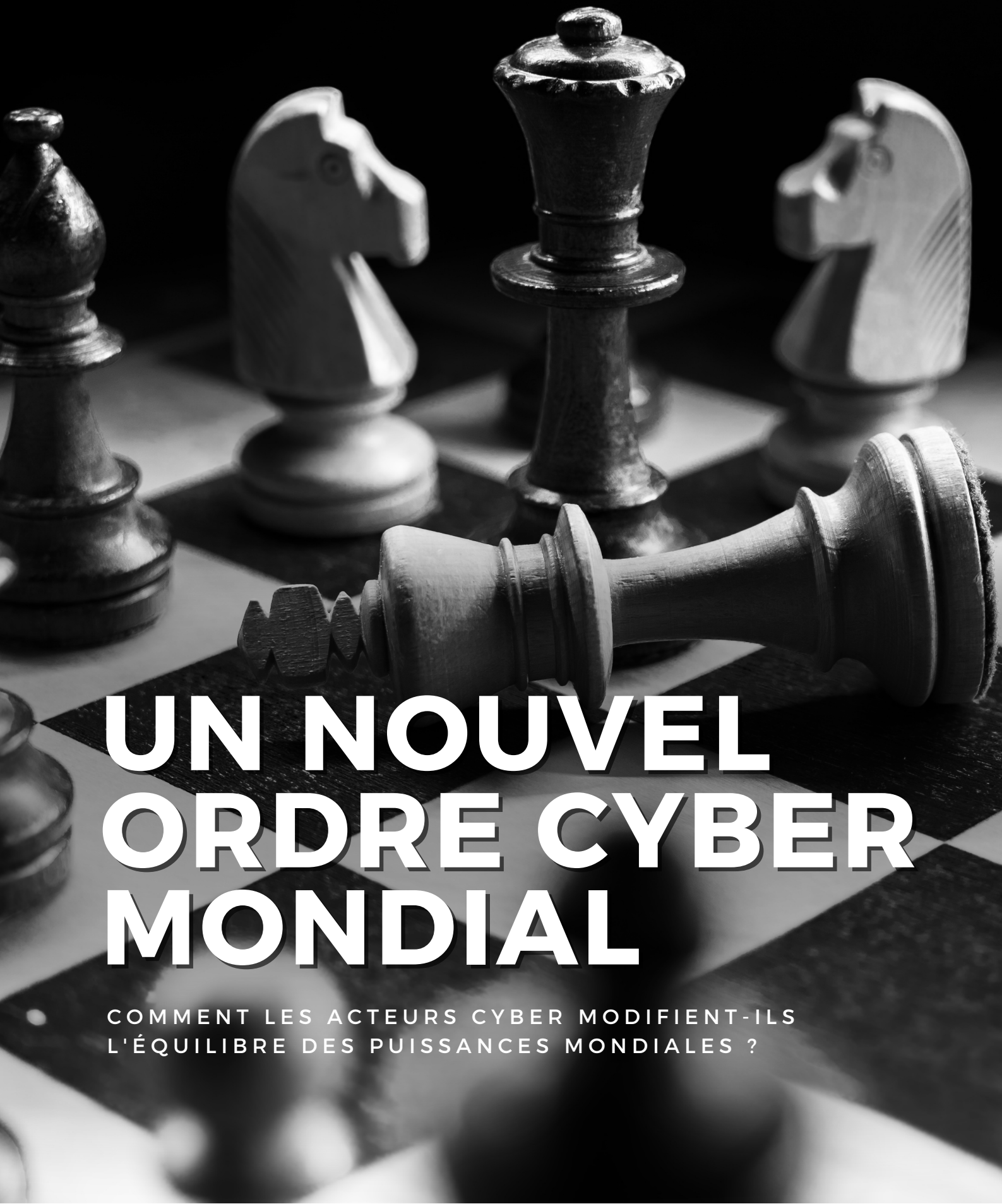
UN ARTICLE UBCOM

EDITION 2023



UN NOUVEL ORDRE CYBER MONDIAL

COMMENT LES ACTEURS CYBER MODIFIENT-ILS L'ÉQUILIBRE DES PUISSANCES MONDIALES ?

COMMENT LES ACTEURS CYBER MODIFIENT-ILS L'ÉQUILIBRE DES PUISSANCES MONDIALES ?

Avec l'avènement du cyberespace, les différentes menaces et attaques cyber prolifèrent désormais dans notre quotidien. Que ce soit à l'encontre des systèmes d'information d'organisations privées (TPE/PME ou grandes entreprises) ou publiques (infrastructures critiques et services d'un État), plusieurs milliards d'attaques cyber ont lieu quotidiennement à travers le monde – y compris dans nos poches, nos voitures, nos télévisions, nos aspirateurs autonomes jusqu'à nos pacemakers. Ces cyberattaques sont une forme d'armes nouvelles totalement dématérialisée, pouvant pourtant avoir un effet létal.
Elles sont au service d'acteurs puissants, étatiques et non étatiques (que l'on peut aussi appeler mafia), face auxquelles les organisations publiques ou privées, nous, citoyens et les États devons apprendre à se prémunir. Depuis la nuit des temps de l'ère numérique, la meilleure technique pour se prémunir des attaques, et c'est bien le paradoxe, réside dans la formation des utilisateurs. Malgré toute l'innovation technologique qui permet beaucoup pour protéger les systèmes, reste que seul l'humain détient les ressources pour garantir l'intégrité des systèmes d'information.

Qui attaque ? Rattacher une attaque à son auteur reste particulièrement complexe. Cependant, il est désormais possible d'identifier l'affiliation d'une attaque. L'affiliation est effectivement importante à établir pour mieux comprendre qui sont les grands acteurs derrière les cyberattaques. La multiplication d'acteurs cyber, qu'ils émanent ou non d'une entité étatique, de différents groupes de cyberattaquants (*hackers*) - organisés ou pas - mène à penser la redistribution du pouvoir dans le cyberespace. Si sur la scène internationale les pays affirment leur puissance grâce à leur poids économique, militaire, diplomatique ou culturel, dans le monde cyber les acteurs sont plus discrets, plus difficiles à identifier et leur multiplicité redistribue les cartes de puissance géopolitique de chaque Etat.

DES GROUPES CYBER TRÈS DIVERS

APT : OBJECTIFS ET AFFILIATION

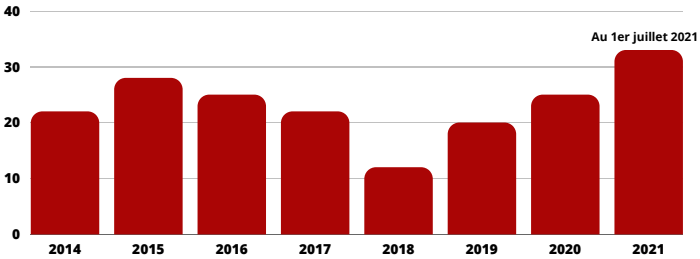
Advanced Persistent Threats ou APT est le nom communément donné aux groupes cybercriminels de premier plan qui sont à l'origine d'attaques cyber destinées à nuire à un État. Certains de ces groupes sont affiliés à des États, mais une telle affiliation n'est pas nécessaire pour qu'un groupe de cyberattaquants soit reconnu et qualifié d'APT - il faut en revanche que les attaques menées soient sophistiquées et persistantes. À ce jour, les organisations mafieuses et terroristes ont les moyens de porter cet acronyme malheureux. Patients et persévérants, ces groupes prennent le temps d'étudier minutieusement leurs cibles et opèrent de manière prolongée et très discrète ; un certain nombre de groupes APT n'ont été détectés que plusieurs années après avoir infiltré un gouvernement étranger ou une organisation. C'est notamment le cas d'APT10, présumé affilié au gouvernement chinois, qui a été actif pendant plus d'une décennie avant d'être officiellement dévoilé en 2016.

Les groupes APT ont en effet pour habitude de s'infiltrer dans les réseaux informatiques de leurs cibles, de collecter et d'exfiltrer un maximum de données et de créer des backdoors qui leur offrent la possibilité d'accéder aux réseaux compromis ultérieurement. Cette porte dérobée constitue une entrée secrète, qui peut être exploitée à volonté sans que personne, ni aucun système, ne puisse la détecter, ou presque. Car il existe quand même, en 2023, des solutions subtiles, bien que peu connues, pour les trouver. Un drôle de jeu de piste en quelque sorte.

La finalité principale de ces groupes est la conduite d'opérations de cyberespionnage, de sabotage, de déstabilisation et/ou de vol de données, le plus souvent sensibles ou classifiées. À ce titre, les entités les plus touchées par des attaques sophistiquées attribuées ou attribuables à des groupes APT, sont les gouvernements, la diplomatie, la défense, les secteurs financiers et énergétiques, ainsi que l'industrie, la santé

et la recherche et développement. Pour résumer, on peut considérer que tout ce qui attrait au régalien les intéresse.

Pour réaliser leurs objectifs, ces groupes ont recours à des méthodes sophistiquées visant à pénétrer les systèmes d'information de leurs cibles. Une première phase peut consister en des techniques classiques d'ingénierie sociale (*phishing*/*spire-phishing*, vol d'identifiants et usurpation d'identité, filature, écoute, interception d'échanges), en l'exploitation de vulnérabilités ou en ayant recours à des méthodes d'attaque *zero-day*[1] . Une fois le réseau de la cible pénétré, les groupes APT procèdent souvent à l'utilisation de malwares spécifiques, voire personnalisés, afin de collecter un maximum de données. Il arrive aussi que le groupe à l'origine de la cyberattaque choisisse de créer une *backdoor* ou un accès à distance, en ayant recours à des réseaux de commande et de contrôle (C&C), dans le but de maintenir un accès au système compromis. Pour faire cela, il faut être doué et bien équipé donc avoir de l'argent et surtout connaitre le gain qui peut en être tiré. La fainéantise des hackers n'est un secret pour personne, de l'indépendant à l'agence d'Etat. Plus vite ils rencontrent des barrières, plus vite ils détournent leur chemin et changent de cible. De plus, aucun n'attaque pour le plaisir. Toute attaque est faite dans une démarche soit cupide et au mieux idéologique. Ce n'est donc jamais gratuit.



Évolution du nombre de vulnérabilités *zéro-day* exploitées de 2014 à Juillet 2021 - Selon Google Tag

Les attaques de ces groupes peuvent avoir de graves conséquences pour les victimes : perte de données sensibles ou classifiées, espionnage industriel, militaire et/ou diplomatique, chantage ou revente de données sur le *darkweb*… Suivant les solutions de cybersécurité mises en place et la résilience de la cible, les coûts liés à une cyberattaque peuvent être plus ou moins conséquents (réparation des systèmes endommagés, récupération des données perdues, perte de confiance des clients et/ou des partenaires, etc.).

[1] Rapport "Panorama de la menace informatique" - ANSSI, 2021.

En plus de la perte de données et du coût financier résultant d'une cyberattaque, la cible peut par la suite aussi souffrir d'une dévalorisation de son image de marque. En d'autres termes, c'est un cauchemar qui tue une victime sur deux quand il s'agit d'une PME, et deux sur trois quand il s'agit d'une TPE. Et quand il s'agit d'un mineur harcelé sur un réseau social, le résultat est parfois le suicide. Les conséquences ne sont que dramatiques, qu'elles soient humaines, sociales ou économiques.

La force d'attaque des groupes de hackers dépend des moyens financiers et humains dont ils disposent. Ainsi, de manière générale les groupes soutenus par des États, en particulier à des fins de cyberespionnage, sont souvent les plus performants. Diverses agences de renseignement et experts en cybersécurité sont à l'œuvre pour établir des liens entre des groupes de cyberattaquants et les pays auxquels ils se rattachent. Mais ces groupes ayant recours à des pratiques sophistiquées pour masquer leur identité, leur affiliation à une entité étatique ne dépend généralement que de minces faisceaux d'indices concordants. Parmi les indices : les cibles et les méthodes d'un groupe offrent de précieux renseignements aux experts.

L'affiliation exacte d'un groupe doit donc toujours être prise avec précaution. De même, la distinction entre des groupes indépendants et ceux affiliés à un État, ou encore l'affiliation exacte d'un groupe à un service spécifique d'une entité étatique, restent complexes.

Mais qui serait le premier voleur de données de la planète ? La NSA ou l'Agence nationale de sécurité américaine, qui n'est autre qu'un collecteur de données pour les 23 autres agences gouvernementales américaines.
En France, nous comptons 5 agences de renseignement qui, en plus de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), participent à la protection de nos données : La Direction générale de la sécurité intérieure (DGSI), la Direction générale de la sécurité extérieure (DGSE), la Direction du renseignement militaire (DRM), la Direction nationale du renseignement et des enquêtes douanières (DNRED) et la Direction du renseignement et de la sécurité de la défense (DRSD).

Le second voleur de la planète tente de se faire discret mais est gigantesque : la Chine. Depuis 2014, elle produit

des systèmes de collecte de masse envers sa population et au-delà, à travers des technologies qu'elle commercialise ensuite dans le monde entier.

Deux exemples pour illustrer les liens d'un groupe cyber à un État :

>>> APT32 – les cibles comme indices

Le groupe APT32 par exemple, serait parrainé par l'État vietnamien. Parmi les principaux indices ayant poussé les experts à établir une telle affiliation : les cibles. APT32 a principalement pris pour cible des entreprises, des organisations politiques et des gouvernements hostiles ou en compétition avec le Vietnam. Des journalistes et des dissidents vietnamiens auraient également été ciblés. De plus, la sophistication de ces attaques ciblées, laisse penser que le groupe dispose de ressources financières conséquentes et d'un haut niveau d'expertise technique. Cela a conduit les experts à l'associer à l'État vietnamien.

>>> APT39 – une affiliation encore débattue

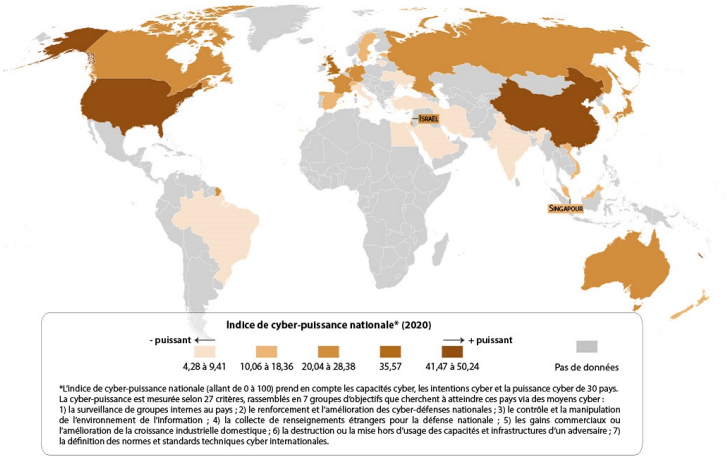
Le groupe APT39 est quant à lui reconnu comme étant affilié à la République islamique d'Iran. Cependant, son affiliation exacte est encore débattue : certains experts considèrent qu'il s'agit d'un service rattaché à l'Organisation de l'énergie atomique de l'Iran (OEAI), tandis que d'autres l'attribuent plutôt au Corps des gardiens de la révolution islamique (*Pasdaran*). Quoi qu'il en soit, l'ADN idéologique de l'attaquant est le même.

4 GRANDES FAMILLES DE CYBERATTAQUANTS, AUX FORCES DE FRAPPE INÉGALES

Si dans les relations internationales il y a une multiplicité d'acteurs (États, ONG, sociétés civiles, groupes terroristes, …), dans l'espace cyber il existe 4 principaux groupes de cyberattaquants :

- les **groupes affiliés à des États**, généralement les plus sophistiqués et disposant des meilleures ressources,
- les **groupes cybercriminels** dont l'essor ces dernières années constituent de véritables défis en matière de cybersécurité,
- ainsi que les **cyberactivistes** qui cherchent à dévoiler des informations au grand public,
- et les **groupes cyberterroristes** procédant principalement à des attaques visant à détruire tout ou partie des données de leur cible.

Les principales cyber-puissances



Source : European Council on Foreign Relations

Ces 4 grandes familles peuvent suffire à provoquer une révolution, une guerre ou encore un renversement de la doctrine politique d'une nation. Et au-delà de ça, elles peuvent vous convaincre qu'il vaut mieux acheter une marque plutôt qu'une autre, croire les opinions de ce courant de pensée plutôt que les autres.

Une étude réalisée sur une soixantaine de groupes d'attaquants cyber, par le groupe français Thalès et israélien Verint[2], a montré que 49% d'entre eux étaient parrainés par des entités étatiques (gouvernements, agences de renseignement ou forces armées). Encore une fois, il reste complexe de déterminer si un groupe de cyberattaquants a été créé par un État ou s'il n'est que mandaté par ce dernier. Il peut aussi arriver qu'une agence de renseignement monte directement sa propre équipe : c'est le cas aux États-Unis avec *Equation Group*, appartenant à la NSA (*National Security Agency*). Concernant les groupes de *hackers* soutenus par un État, la Russie et la Chine sont les pays les plus représentés et certainement les plus connus du grand public. Mais d'autres États sont aussi connus pour avoir recours à de tels groupes (Iran, Corée du Nord, Israël, Turquie, Ukraine, Thaïlande, Singapour, etc.).

Le vol de données et de propriété intellectuelle, plus communément appelé cyberespionnage ou intelligence économique pour rester diplomate, est l'un des objectifs principaux poursuivis par les cyberattaquants affiliés à des États. En France, ce cyberespionnage constituait le plus grand nombre d'offensives cyber ayant affecté le pays à la fin de la décennie 2010[3].

2 "The CyberThreat Handbook" – Rapport conjoint Thales & Verint, 2019

3 "Revue stratégique de cyberdéfense" – SGDSN, 12 février 2018

Il consiste en l'utilisation de techniques de piratage informatique, dans le but d'accéder à des systèmes d'information préalablement ciblés afin d'en extraire des données confidentielles et autres renseignements stratégiques. Il confère deux avantages majeurs à l'attaquant : ne pas éveiller les soupçons et rester discret. Par l'information captée, l'auteur de cyberespionnage a un coup d'avance en s'imaginant, à tort ou à raison, que son adversaire l'ignore. De manière générale, ce type d'attaques est difficile à détecter et à tracer. En France, c'est l'ANSSI qui, avec le soutien tactique de la DGSI, est chargée de contrer ces opérations. En 2015, des pirates informatiques, probablement affiliés au gouvernement de la République populaire de Chine, ont visé l'OPM (Office of Personnel Management) des États-Unis. Cette attaque, d'une ampleur inédite, a permis aux hackers de voler les informations personnelles d'environ 20 millions d'employés fédéraux.

Source : The CyberThreat Handbook Thales & Verint, 2019

L'autre moitié des cyberattaquants (51%) émanent de trois autres "grandes familles" : 26% sont des "hacktivistes", 20% des cybercriminels et 5% divers groupes cyberterroristes. En fonction de l'origine de la cyberattaque, les motivations ne sont évidemment pas les mêmes.

Ces groupes se caractérisent par la nature de leurs actions :

- **Cyberactivisme** : nuire à l'image de leur cible et dénoncer des faits considérés comme relevant de l'intérêt général.
- **Cybercriminalité** : générer du profit par le vol de données.
- **Cyberterrorisme** : chiffrement (*ransomware* ou rançongiciels) et/ou destruction de données (*malware* ou logiciels malveillants de type *Wiper*[4]).

Si certains groupes cybercriminels, *hacktivistes* ou cyberterroristes peuvent s'avérer particulièrement opérationnels et virulents dans leurs attaques, les groupes cyber disposant de la plus grande capacité d'action restent ceux affiliés à une entité étatique. En effet, de par leur appartenance, ces groupes disposent de moyens humains et financiers plus importants, de compétences techniques supérieures et de capacités de ciblage accrues.

En comparaison, les groupes cyber indépendants ont souvent un nombre de membres plus limité et n'ont pas accès aux ressources et aux technologies utilisées par les agences de renseignement et de défense. Leurs financements sont également moins conséquents et émanent principalement de diverses activités criminelles (vente de données volées, blanchiment d'argent, vol de comptes bancaires en ligne, etc.) et du recours à des rançongiciels (la cible est alors obligée de payer une rançon pour déchiffrer ses données ou empêcher sa divulgation).

Qu'ils soient ou non affiliés à un État, les *hackers* poursuivent de manière générale des objectifs premiers similaires : le cyberespionnage, les trafics illicites, la déstabilisation et/ou le sabotage.[5] Il en va de même pour les moyens utilisés, les cyberattaques déployées dans le but d'accomplir ces objectifs étant majoritairement des attaques par *malware* (logiciels malveillants), *phishing* ou *spire-phishing* (ingénierie sociale),

4 Un Wiper est un logiciel malveillant sophistiqué, conçu pour détruire un maximum de données et les rendre irrécupérables.

5 Revue stratégique de cyberdéfense 2018 - SGDSN

DDoS (*Distributed Denial of Service*) ou dites par déni de service, ainsi que des attaques de type *bruteforce* (aussi appelé "cassage de mot de passe"). Ainsi, si les principales techniques d'attaque sont partagées par divers groupes cyber, l'intensité de l'attaque est adaptée à la robustesse et la résilience de la cible.

Les motivations diffèrent cependant entre les groupes cyber affiliés à un État et les groupes cybercriminels. Un groupe affilié à un État cherche principalement à accéder à des renseignements stratégiques en pénétrant les systèmes d'information d'un autre État, de services de renseignement étrangers, d'ambassades ou d'entreprises du secteur de la défense. Ces renseignements sont cruciaux pour tout groupe voulant mettre en place un espionnage politique, industriel, une surveillance diplomatique ou une collecte de renseignements militaires. Grâce au vol de ces informations, l'État à l'origine de l'attaque peut accélérer le développement de certaines de ses technologies ou favoriser sa stratégie d'influence. Le rachat de la filiale énergie du groupe Alstom par l'américain General Electric en 2014 témoigne de cette stratégie d'influence que peut exercer un acteur étatique sur un autre. Outre l'utilisation par le *Department of Justice* (DOJ) américain de son processus législatif supranational, ce rachat de la filiale énergie d'Alstom a en partie pu avoir lieu suite à l'enquête du *Federal Bureau of Investigation* (FBI) sur les pratiques de l'entreprise française. L'aspect cyber aurait alors logiquement été mobilisé par les enquêteurs du FBI pour accéder aux informations confidentielles d'Alstom[6].

L'Affaire Crédit Suisse est un autre exemple de ce jeu d'influence exercé par les autorités américaines sur des institutions étrangères. Pendant plus de 15 ans, l'historique banque zurichoise a subi des pressions de la part du DOJ américain à coups d'amendes de plusieurs milliards de dollars, obligeant la banque nationale suisse a lui prêter 50 milliards d'euros en 2020. Mi-mars 2023, après avoir enregistré sa pire séance boursière avec des pertes de 30%, la seconde banque suisse s'est finalement vu rachetée par son concurrent de toujours, la société helvète de services financiers UBS, pour un montant de 3,04 milliards d'euros[7].

C'est ce qu'a réalisé la Chine en 2007 avec l'opération Byzantine Hades par exemple. Réalisée par une unité cyber de l'armée chinoise, cette cyberattaque a visé plusieurs entreprises américaines impliquées dans le développement de technologies d'avions furtifs. Les pirates ont utilisé différentes techniques d'ingénierie sociale ainsi que des logiciels malveillants et ont réussi à pénétrer les réseaux informatiques des entreprises. Ils ont ensuite procédé au vol de documents classifiés, liés au Département de la défense américain (DOD), relatifs aux plans de conception et aux données de tests des avions. Ce vol massif de données a ensuite permis aux autorités chinoises d'accélérer le développement de leurs propres avions furtifs.
A contrario, les groupes cybercriminels non affiliés sont essentiellement motivés par le profit. S'ils cherchent également à pénétrer les systèmes d'information de leurs cibles afin de dérober des documents sensibles, c'est ensuite dans l'optique de monnayer les données qui y sont contenues sur le *darkweb*.[8]

Agissant aussi bien pour un acteur étatique que pour leurs intérêts, les cyberattaquants laissent pour autant des faisceaux d'indices en fonction des cibles et de la sophistication de l'attaque permettant dans certains cas aux experts de remonter à la source de l'attaque.

UNE REDISTRIBUTION DE LA PUISSANCE ?

L'ESSOR DE LA CYBERCRIMINALITÉ

Pour faire un état des lieux de l'essor de la cybercriminalité, il faut rappeler que : Depuis la pandémie en 2019, nous assistons à une véritable explosion du nombre de cyberattaques sur internet : + 600%[9]. En 2020, l'éditeur de logiciel McAfee rapportait également une augmentation moyenne des attaques sur les comptes cloud de l'ordre de 660%.

Un rapport d'information du Sénat français de 2021[10], rapporte que les attaques DDoS sont passées de 15 à 20% lors du confinement en 2020 et constate, la même année, une hausse de plus de 90% du nombre de fuites de données.

6 "Les zones d'ombre de l'affaire Alstom selon Frédéric Pierucci", Portail de l'IE, 17 janvier 2019

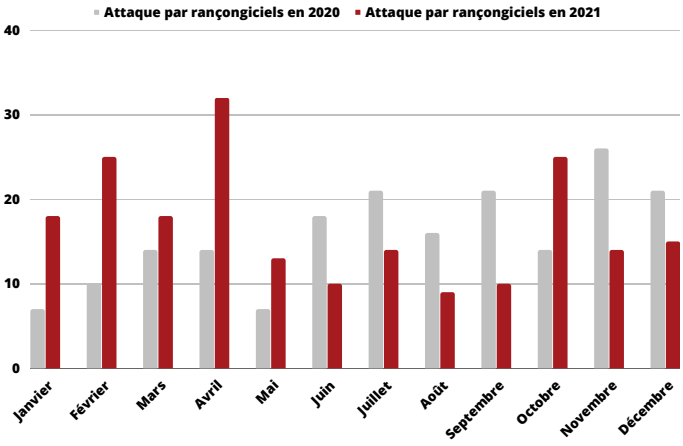
7 "Credit Suisse racheté par UBS : ce qu'il faut savoir sur cet épisode bancaire hors normes", Challenges - 29 mars 2023

8 Défini comme « Internet non indéxé ». Ce sont les serveurs web qui ne sont pas reconnus par les moteurs de recherche comme Google ou Yahoo et ne peuvent donc indexer les contenus.

9 "Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report", Forbes, 16 mars 2022

10 "Rapport d'information fait au nom de la délégation aux entreprises, relatif à la cybersécurité des entreprises", Rapport du Sénat, 2021

Dans son rapport "État de la menace liée au numérique" en 2019, le ministère de l'Intérieur français précisait qu'en 2018, 80% des entreprises déclaraient avoir subi une cyberattaque, dont une majorité d'attaques par rançongiciel. D'après l'ANSSI, en 2020, les attaques par rançongiciel ont quadruplé. À travers le monde, on recensait en 2021 une attaque par rançongiciel toutes les 11 secondes, contre une toutes les 40 secondes en 2016.[11]



Statistique concernant les attaques par rançongiciels en 2020 et 2021 - Source: Panorama de la menace informatique 2021 - ANSSI.

Néanmoins, ces statistiques sont à nuancer. En effet, de nombreuses entreprises attaquées l'ont bien été mais sans effet car leurs systèmes de protection ont fonctionné. Tandis que d'autres attaques ne sont pas comptées car ne sont tout simplement pas rendues publiques et restent dans l'ombre. Et comment leur en vouloir ? Quand on sait que ne pas rendre publique une cyberattaque peut permettre aux organisations victimes de s'affranchir d'une éventuelle amende administrative de la Commission nationale de l'informatique et des libertés (CNIL). Sans compter l'atteinte portée à la réputation, si durement gagnée de leurs partenaires et clients…

Si en 2015 les coûts liés à la cybercriminalité représentaient entre 3000 et 4500 milliards de dollars par an, tous secteurs confondus, ils représentent le double aujourd'hui (aux alentours de 6000 milliards de dollars par an) et les experts s'accordent à dire qu'elle pourrait coûter environ 10 500 milliards de dollars par an d'ici à 2025[12]. La cybercriminalité rapporterait donc 2 fois plus que le trafic de drogue et autant que la vente d'armes qui à elle seule représente 30 % du PIB mondial.

Toutes ces statistiques permettent de ne plus nier l'explosion de la cybercriminalité. Ce nouveau format de crime, plus difficile à réguler et à sanctionner, permet d'affirmer que nous devons mieux comprendre et agir au sein même du cyberespace.

Dès le début de la décennie 2010, les cryptomonnaies telles que le BTC (Bitcoin), ETH (Ethereum), BNB (Binance Coin), USDC (USD Coin), ont fait leur apparition sur le *darkweb*. Ces monnaies n'appartiennent à aucune banque et sont décentralisées. Elles reposent sur la technologie *blockchain*. Celle-ci consiste à stocker des données de manière décentralisée au sein de blocs, où un certain nombre de transactions y sont inscrites. Les blocs s'ajoutent les uns aux autres et forment une chaîne : c'est donc une chaîne de blocs : *blockchain*. En résumé, c'est un registre d'enregistrement de transactions qui est ordonné chronologiquement, distribué sur tous les ordinateurs du réseau et sécurisé.[13]
Cette technologie permet donc aux utilisateurs de réaliser des transactions intraçables. Aussitôt, divers groupes cybercriminels se sont intéressés à ces cryptomonnaies intégrant alors un système de blanchiment automatique, le rêve pour tout mafieux qui se respecte !

Rapidement, ces dernières ont facilité l'achat et la vente en ligne de données volées ou de produits illégaux. Les *hackers* affiliés à des groupes cybercriminels y ont ainsi vu une opportunité d'accroître leurs profits. Une augmentation significative des vols de données sur internet a depuis lors été recensée. Autrement dit, la courbe de croissance de l'usage du Bitcoin corrobore avec le vol de données (*dataleak*).

Ces groupes cybercriminels ciblent aussi bien des entreprises que des banques ou des particuliers. Ils peuvent décider soit de récupérer de l'argent directement, en accédant à des informations bancaires, en réalisant des virements frauduleux, soit de voler des données personnelles, sensibles ou classifiées, qu'ils revendront ensuite sur le *darkweb* afin de générer des bénéfices colossaux. Cette activité particulièrement lucrative pousse les cybercriminels à réaliser des vols de données à grande échelle.

11 "2023 Must-Know Cyber Attack Statistics and Trends", Embrocker, 6 mars 2023
12 Rapport Sénat 2021 & article Embroker - *ibid.*
13 "Mieux comprendre le principe de la technologie Blockchain", Crypto week, 4 janvier 2022

En voici quelques exemples :

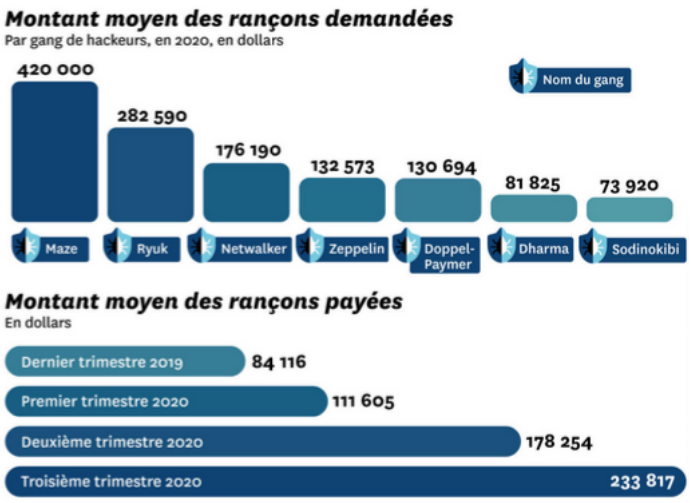
- *Yahoo!* – 2013 : Annoncé en 2016, il s'agit de l'une des plus importantes cyberattaques de l'histoire. L'entreprise avait initialement annoncé qu'un milliard de comptes avaient été compromis, avant finalement d'avouer en 2017 qu'il s'agissait de l'ensemble de ses 3 milliards de comptes qui étaient concernés.

- *Uber* – 2016 : Les informations personnelles de plus de 57 millions d'utilisateurs ainsi qu'une liste de noms et de numéros de permis de conduire de plus d'un demi-million de chauffeurs partenaires ont été volés par deux cyberattaquants. Uber a caché le vol de ces données à ses clients, préférant offrir 100.000$ aux pirates en échange de leur silence et de la suppression des données.

- *Facebook* – 2019 : C'est seulement en 2021 que les données volées de plus de 530 millions d'utilisateurs ont été divulguées sur un forum de pirates informatiques. Noms et prénoms, dates de naissance, numéros de téléphone et parfois aussi adresses e-mail ont été récupérés par une attaque cyber qui a touché le réseau social en 2019.

- *Zoom* – 2020 : Suite aux confinements liés à la pandémie de Covid-19, Zoom a connu une très forte augmentation du nombre de ses utilisateurs entre 2019 et 2021. En 2020 cependant, une cyberattaque d'ampleur a conduit au vol de 500 millions de comptes.

En plus du vol et de la revente de données, les attaques par rançongiciels se sont multipliées depuis 2018[14]. Il s'agit pour les groupes cybercriminels de la deuxième forme d'attaques la plus lucrative. L'opération consiste à chiffrer toutes les données de la cible, afin de paralyser l'ensemble de ses systèmes d'information. Les postes informatiques deviennent inaccessibles et un message proposant aux victimes de payer une rançon apparaît. En échange du paiement de la rançon, les victimes obtiennent la clef de chiffrement, permettant le déblocage du matériel et des données.



Source : Coverware / Sophoslabs / Corriere Della Sera

Les rançons s'élèvent parfois à quelques centaines d'euros, mais peuvent aussi atteindre des sommes astronomiques de plusieurs dizaines de milliers d'euros. Monter de telles opérations peut donc s'avérer particulièrement avantageux pour les cybercriminels.

L'essor de cette cybercriminalité passe aussi par le développement de services d'hébergement bulletproof. Il s'agit d'infrastructures privées, plus souples, qui ferment les yeux sur le contenu que contiennent leurs serveurs et qui assurent à leurs utilisateurs une plus grande confidentialité. Ces hébergements *bulletproof* sont connus pour ne pas désactiver les contenus criminels qu'ils abritent malgré les demandes des autorités, et sont en outre difficilement traçables. Ils permettent ainsi aux pirates d'échapper à la surveillance des services de sécurité.

Finalement, le développement de la cybercriminalité pose de véritables défis en matière de sécurité informatique mais aussi de formation, tant pour les entreprises privées et les particuliers que pour le secteur public. En 2018 déjà, le Secrétariat Général de la Défense et de la Sécurité National (SGDSN) alertait sur la porosité de la frontière entre la lutte contre la cybercriminalité et les objectifs de cyberdéfense. Celle-ci s'explique notamment à travers l'augmentation du niveau de violence des attaques cybercriminelles. Suivant son intensité, une cyberattaque peut avoir de sévères répercussions : si particulièrement violente, elle pourrait techniquement être capable de paralyser des infrastructures critiques et constituerait alors "une menace en matière de sécurité nationale".[15]

14 "Attaques par rançongiciels, tous concernés", Rapport de l'ANSSI, août 2020
15 "Revue stratégique de cyberdéfense", Rapport du SGDSN, février 2018

LES GRANDES PUISSANCE ÉTATIQUES, BOULEVERSÉES PAR DES PUISSANCES ÉMERGENTES NON ÉTATIQUES

Force est de constater que de plus en plus d'attaques cyber sont le fait de groupes cybercriminels indépendants, ayant pour principal objectif de générer du profit. Ces gains sont ensuite partiellement réinvestis, afin d'élargir les équipes et d'acquérir du matériel plus performant, ce qui contribue à la montée en puissance de ces groupes cybercriminels. L'accroissement du poids d'acteurs non étatiques dans le monde cyber vient rebattre les cartes d'un monopole de la puissance, disputé dans le monde réel entre quelques États forts.

Dans le cyberespace, les règles ne sont donc plus les mêmes : un petit groupe, qu'il soit indépendant ou affilié à un État, même de second plan sur la scène internationale – comme le Vietnam, par exemple ; s'il est bien équipé, dispose de machines et d'algorithmes puissants, pourrait venir concurrencer les plus grandes agences de renseignements occidentales, pirater des serveurs de grandes entreprises, voire compromettre la sécurité d'infrastructures critiques, portant de fait atteinte à la sécurité nationale d'un pays. En décembre 2010, le printemps arabe se soulève grâce à un clavier fabriqué en Chine et une souris américaine au travers de Tweeter. Depuis la Tunisie tente de se reconstruire, en vain.

Les groupes cyber affiliés à des États (tels que certains APT, comme évoqués précédemment) restent les mieux financés et a priori les plus performants. Logiquement, leurs objectifs se concentrent en majorité sur des pays ennemis dont la force de frappe leur est opposable. En recherche d'un rapport de force entre puissances égales, la Chine s'attaque aux États-Unis et inversement les États-Unis s'attaquent à la Chine.

Une partie de ces groupes cyber cherchent depuis longtemps à déstabiliser les pays occidentaux. Ainsi, la République populaire de Chine, la Fédération de Russie ainsi que la République islamique d'Iran, sont trois des principaux pourvoyeurs mondiaux de groupes cybercriminels en lien avec une ou plusieurs de leurs entités étatiques. Si chaque groupe cyber poursuit ses propres missions, les objectifs convergent souvent vers le cyberespionnage dans le but d'améliorer des technologies, en particulier dans le secteur de la défense, ou encore vers la déstabilisation politique, principalement de démocraties occidentales.

L'exemple flagrant survient lors des élections présidentielles de 2016 aux États-Unis, lorsque des pirates russes ont interféré dans la campagne pour les intérêts du Kremlin[16]. Les États-Unis sont d'ailleurs le premier pays le plus touché par des cyberattaques ayant causé des pertes supérieures à 1 million de dollars[17] : 156 cyberattaques majeures, entre 2006 et 2020. De manière générale, les principales victimes de cyberattaques sont les 12 pays au plus fort PIB (parmi lesquels de nombreux pays occidentaux). Ces actes de déstabilisation et de vol de données participent grandement du bouleversement que vivent les grandes puissances étatiques, atteintes par des acteurs cyber.

Comme précités, les principaux secteurs visés par des cyberattaques sont les gouvernements, la santé, les finances, l'industrie et la défense, l'éducation et les médias. Si des cyberattaques par rançongiciels sont menées sur plusieurs secteurs simultanément, cela peut mettre à mal l'économie de tout un pays. C'est précisément ce qui est arrivé au Costa Rica : en avril 2022 le pays a dû déclarer l'état d'urgence suite à une série de cyberattaques par rançongiciels. Les sommes demandées par les cybercriminels étaient supérieures à la moitié du PIB costaricain. Ainsi, des cyberattaques coordonnées par un groupe peuvent constituer des menaces sévères, déstabiliser, voire paralyser entièrement un pays. C'est de cette manière que les cybercriminels réussissent à défier une autorité étatique souveraine, a priori plus puissante, mais dans les faits incapable de réagir face à des attaques de cette envergure.

Les outils à disposition des cyberattaquants sont un autre élément essentiel à prendre en compte dans l'analyse de la redistribution de la puissance, en particulier au profit d'entités cyber non étatiques. En effet, leur montée en puissance est directement en lien avec le fait qu'ils ont recours à des outils de plus en plus performants. Certains de ces outils, développés par des agences de renseignements, dont la NSA, sont particulièrement sophistiqués.

16 "[…] Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election." (…) "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, […] In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016." Rapport du directeur du renseignement national (DNI) des États-Unis, "Assessing Russian Activities and Intentions in Recent US Elections", 2017

17 "Les pays les plus touchés par des cyberattaques majeures", site du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, consulté le 28 mars 2023

Se pose alors la question de savoir comment ces groupes de cybercriminels ont pu avoir accès à de tels outils ?
La réponse est simple : suite à des cyberattaques sur des services de renseignement, certaines données ont fuité avant d'être mises en ligne.

C'est ce qui est arrivé en 2017 aux États-Unis. Suite à une cyberattaque massive sur la NSA, l'exploit "*EternalBlue*"[18] a pu être récupéré par les cyberattaquants puis mis en ligne. De tels outils sont très prisés par de nombreux groupes cybercriminels, car ils leur permettent d'augmenter leur capacité d'action et leur puissance. Ils sont donc récupérés par divers groupes de cyberattaquants et utilisés pour de nouvelles attaques cyber.[19]

Ces fuites de données et d'outils développés par les services de renseignement sont très préoccupantes et participent grandement à la redistribution de la puissance. Les agences de renseignement perdent, en plus d'un outil confidentiel, sophistiqué et virulent, leur avantage, tandis que les groupes cybercriminels gagnent en puissance en ayant recours à ce nouvel outil.

De plus, ces agences, qui ont parfois investi des efforts humains et financiers colossaux pour le développement de tels outils, ne peuvent finalement plus en faire usage. Pour les groupes cybercriminels, c'est un gain considérable qui leur permet de se renforcer et qui peut également leur fournir de nouvelles idées à l'amélioration de programmes d'attaques cyber.

Le bilan est sans appel : à l'heure où le cyberespace cannibalise la société humaine en dématérialisant les échanges et les services, l'équilibre mondial de la puissance se voit aujourd'hui bouleversé. Ce sont en premier lieu les États qui en sont affectés et indirectement les citoyens. Jusque-là, les Etats incarnaient à eux seuls les grands pôles de puissance mondiale. Mais l'émergence et la montée en puissance spectaculaire de groupes de hackers, soutenus ou non par une entité étatique, vient rebattre les cartes de la puissance. Si pour beaucoup, le cyberespace semble être un monde parallèle, ses conséquences sur le monde réel peuvent être particulièrement violentes. De petits groupes, qui auraient jusque-là pu être considérés comme inoffensifs de par leur taille, peuvent désormais prétendre rivaliser avec les pays les plus puissants du monde et décider de changer nos vies.

19 Un exploit ou code d'exploitation est un élément de programme, en l'occurrence *EternalBlue* développé par la NSA, permettant l'exploitation des failles de sécurité d'un système informatique

20 "Cyberattacks in 12 nations said to use leaked NSA hacking tool", CNBC, 12 mai 2017

Rédaction par Antoine Ilan Kercher et Frans Imbert-Vier
Édition 2023


UBCOM SWISS INTELLIGENCE AGENCY
CYBER PROTECTION AND SOVEREIGNTY