Anatomie d'une cyber-attaque contre une entreprise : comprendre et prévenir les attaques par déni de service

Par Albert DE MEREUIL
Consultant en intelligence économique
et Annabel-Mauve BONNEFOUS
Professeur associé en leadership et management, responsable du département People and Organisations de NEOMA Business School.

Les cyber-attaques représentent une menace mal connue, mais pourtant bien réelle pour les entreprises, publiques comme privées. Les entreprises qui en ont été victimes peuvent témoigner de pertes financières colossales et d'une dégradation sans précédent de leur réputation. Comment prévenir de telles attaques ? À partir de l'analyse approfondie de 234 attaques par déni de service (DOS) s'étant produites entre septembre 2011 et janvier 2015, cet article met en lumière les profils des cyber-attaquants, leurs motivations et les types d'entreprises qui sont leurs cibles favorites. Sont ensuite discutées diverses pistes d'actions concrètes permettant de prévenir ces cyber-attaques avant que les entreprises ne soient contraintes à en gérer les conséquences - au prix fort.

Introduction

Le Forum économique mondial classe dans son rapport annuel *Global Risks 2014* le risque de cyber-attaque comme le cinquième risque d'ampleur mondiale le plus probable. Selon ce rapport, la connexion de plus en plus d'objets du quotidien démultipliera les points faibles du réseau Internet, et donc les possibilités d'attaques. Dans un monde informatique où il est toujours plus facile d'attaquer que de défendre, le danger est bien réel, car « nous ne pourrions être qu'à une innovation de rupture près de l'acquisition d'un avantage considérable par les attaquants » (p. 40). Une étude publiée en juillet 2013 par le *think-tank* américain *Center For Strategic and International Studies* évalue le coût total de la cybercriminalité à 500 milliards de dollars par an, dont 100 milliards de dollars et la destruction de 508 000 emplois pour les seuls États-Unis.

Le *Security risks survey* du Kaspersky Lab (2014a) confirme ce danger. Il révèle que 94 % des entreprises ont été victimes d'au moins une cyber-attaque au cours de l'année écoulée (sur un échantillon de 3 900 entreprises dans 27 pays) et que 12 % d'entre elles ont été victimes d'attaques ciblées. Le problème est que la fréquence et l'intensité des cyber-attaques contre les entreprises tant publiques que privées ne cessent d'augmenter (HULT et SIVANESAN, 2013).

Cet article est consacré aux attaques DDoS (*distributed denial-of-service*), un type de cyber-attaque que les entreprises subissent très fréquemment. Au cours des quatre dernières années (2011-2015), nous avons répertorié et disséqué 234 attaques DDoS subies par des entreprises privées et publiques de toutes tailles et situées partout dans le monde. Nous restituons ici les fruits de cette recherche en portant à la connaissance des lecteurs les profils des cyber-attaquants, leurs motivations et leurs cibles favorites.

La première partie de l'article sera consacrée à la compréhension du phénomène. Dans une seconde partie, seront présentées les motivations de ses acteurs. Dans les deux dernières parties, seront identifiées les entreprises victimes des cyber-attaques, avant de traiter de la manière dont ces entreprises peuvent prévenir ce type particulier d'attaque.

La cyber-attaque, une notion récente

La notion de « cyber-attaque » n'a pas encore été définie dans les dictionnaires traditionnels. Toutefois, les internautes l'ont eux-mêmes définie sur l'encyclopédie libre Wikipédia comme « un acte malveillant envers un dispositif informatique *via* un réseau cybernétique ». Ils ajoutent : « une cyber-attaque peut émaner de personnes isolées, d'un groupe de pirates ou de vastes organisations ayant des objectifs géopolitiques ».

Cette définition non académique a le mérite de souligner la nature multiple des cyber-attaques aussi bien du point de vue de leurs acteurs que de celui de leurs objectifs. Selon François-Bernard Huyghe (2012), les attaques informatiques peuvent en effet répondre à un grand nombre d'objectifs : mettre à jour ou voler des données confidentielles, prendre le contrôle de machines, mettre en place des stratégies d'influence, de chantage, de manipulation, d'espionnage ou de sabotage.

L'ennemi n°1 : l'attaque par déni de service

Dans cet article, nous traiterons en particulier d'un type spécifique de cyber-attaque, l'attaque par déni de service. Il s'agit d'une attaque qui rend inutilisable un service, un site ou un réseau informatique - pour ses administrateurs et/ou pour ses utilisateurs. Pour cela, l'attaquant perturbe les connexions entre deux machines du réseau, ou bien il bombarde le réseau d'informations jusqu'à ce qu'il sature et se mette hors service.

Lorsqu'un seul ordinateur est utilisé pour lancer une telle attaque, celle-ci est qualifiée de *denial-of-service* (DoS). Si plusieurs ordinateurs sont sollicités pour lancer l'attaque, il s'agit d'un *distributed denial-of-service* (DDoS). Les DDoS peuvent être le fruit d'une collaboration entre plusieurs cyber-pirates, mais il est également possible que ce soit l'œuvre d'un seul individu.

En effet, le cyber-pirate installe un logiciel dans d'autres ordinateurs à l'insu de leurs propriétaires. C'est ce qui risque d'arriver lorsque l'on visite des sites peu fiables et mal protégés, ou lorsque l'on télécharge des fichiers sur Internet sans avoir vérifié tout le contenu de l'installation. Dans le jargon d'Internet, l'ordinateur ainsi infecté devient une « machine zombie ». Le cyber-pirate peut désormais contrôler l'ordinateur à distance et peut activer le logiciel d'attaque quand il le souhaite. Les professionnels des cyber-attaques disposent souvent d'un parc de plusieurs milliers de « machines zombies » qu'ils louent à d'autres cyber-pirates souhaitant réaliser des cyber-attaques ponctuelles.

Les attaques DDoS sont particulièrement redoutées : elles ont le triste avantage d'être faciles à mettre en œuvre, d'être peu onéreuses et extrêmement rentables pour les attaquants. Selon Sauter (2013), nul n'est besoin de disposer d'outils et de connaissances sophistiquées pour lancer ce type d'attaque contre une entreprise. En raison de leur simplicité, les DDoS sont d'ailleurs considérées comme des attaques « bas de gamme » par les *hackers* (ce qui ne les empêche pas de les employer très fréquemment).

Photo © Universal History Archive/UIG/Bridgeman Images

« Mille images de l'océan », estampe de Hokusai Katsushika (1760-1849), Paris, Musée Guimet – Musée national des arts asiatiques

« Les professionnels des cyber-attaques disposent souvent d'un parc de plusieurs milliers de « machines zombies » qu'ils louent à d'autres cyber-pirates souhaitant réaliser des cyber-attaques ponctuelles. »

Adam, un cyber-pirate « repenti », expliquait dans une interview postée en mai 2013 sur *whitehatsec.com* que les DDoS représentaient une véritable manne financière : « *Le DDoS n'est pas vraiment un exploit, mais ça peut quant même nous rapporter un « salaire » mensuel, en échange de notre « protection ». (…) Le racket est une grande part de ce commerce : on abat un site pendant une heure, on envoie un* e-mail *aux propriétaires (ou on les appelle) pour leur demander 200 dollars. On leur dit que s'ils ne paient pas, le(ur) site sera abattu pour de bon. Généralement, ils paient... Et s'ils ne le font pas, ils perdent des jours, des semaines, voire des mois de transactions.* »

Le Kaspersky Lab estime que 19 % des entreprises américaines ont été victimes de cyber-attaques en 2013. Notre propre recherche sur les cyber-attaques classe l'attaque DDoS en deuxième position parmi les attaques les plus utilisées contre des entreprises, après l'injection SQL.

Pour les entreprises qui en sont les victimes, une attaque DDoS peut être meurtrière : le magazine *Forbes* (2014) a chiffré les pertes financières des attaques DDoS à un million de dollars par jour en moyenne. Pour le Kaspersky Lab (2014b), une attaque qui dure de une à quelques heures fait perdre en moyenne 52 000 dollars à des TPE/PME, et 444 000 dollars à de grandes entreprises. De plus, les marchés financiers n'apprécient guère cette défaillance passagère des systèmes informatiques des entreprises. Une étude menée par Arundhati et ses confrères (2011) montre que les entreprises victimes de DDoS voient le cours de leurs actions et de leur capitalisation boursière chuter significativement. Leur réputation et leur crédibilité auprès des consommateurs sont également fortement impactées. En interne, il faudra inclure les pertes liées au ralentissement de l'activité de leurs salariés, qui sont momentanément privés de leurs outils de travail, ainsi que les éventuels coûts de réparation des dégâts informatiques occasionnés (D'AMICO, 2000). Assénant le coup de grâce, les études menées par Xuhua Bao, directeur de recherche au NSFocus, révèlent que 42 % des victimes d'une cyber-attaque subissent des attaques analogues à répétition. Il ne s'agit donc pas d'un coup unique pour les attaquants, mais bien un repérage en bonne et due forme des meilleurs payeurs.

L'origine des DDoS

Les attaques par déni de service trouvent leur origine dans la « culture *Hacker* » et le fameux « *Lulz* », il s'agit d'une forme d'amusement partagée par des accros de l'informatique. Elle consiste à importuner d'autres internautes en postant des contenus offensifs, répugnants ou tordus sur des forums de discussion. Dans la continuité du « *Lulz* » sont apparus les « *Trolls* ». En langage Internet, les *Trolls* sont des individus qui sèment le désordre sur la Toile en déclenchant des disputes ou en tourmentant les internautes par des propos incendiaires, exagérés ou hors-sujet. Certains *Trolls* le sont sans en avoir réellement conscience, mais d'autres le font sciemment parce que cela les amuse.

Malheureusement, ces « jeux » en apparence anodins et stupides se sont métamorphosés, pour devenir de véritables armes. C'est le cas de l'outil favori des *Trolls*, le « *flood* », qui consiste à inonder de messages un forum de discussion afin d'empêcher qu'une conversation puisse y suivre son cours normal. Cette pratique est sortie des forums de discussion pour s'étendre aux sites Internet. En effet, en envoyant trop d'informations ou un trop grand nombre de requêtes à un site ou à un serveur, il est possible de le faire saturer et de le mettre ainsi « hors ligne » : il s'agit d'une cyber-attaque par déni de service (DoS).

234 attaques DDoS passées au crible

Comment peut-on prévenir ce genre d'attaque ? Pour aider les entreprises à mieux comprendre le phénomène, nous avons étudié 234 attaques DDoS perpétrées entre septembre 2011 et janvier 2015. Sur cet échantillon, 196 attaques ont été répertoriées grâce à la précieuse contribution du concepteur du site *hackmageddon.com*, que nous avons contacté à cet effet. Cet ingénieur italien recense depuis des années toutes les cyber-attaques ayant visé des entreprises et des gouvernements. Les 38 attaques restantes ont été repérées grâce à une analyse systématique des articles de la presse économique répertoriés dans la base de données Factiva. L'analyse en profondeur de chacune de ces attaques ainsi qu'une revue de littérature sur les cyber-mouvements nous ont permis de reconstituer le profil des attaquants, leurs motivations et leurs cibles favorites. Par la suite, nous avons interrogé des professionnels de la sécurité informatique afin d'envisager avec eux les moyens les plus efficaces de prévenir ce type d'attaque.

Profils et motivations des cyber-pirates

Nous avons pu construire sept profils de cyber-attaquants : les *hackers Black Hat*, les *hackers White Hat*, les *hackers* libertaires, les *trolls*, les cyber-djihadistes, les censeurs et les justiciers géopolitiques.

Nous les passons en revue ci-après.

Les hackers Black Hat

Les concepts de « *Black Hat* » et de « *White Hat* » sont couramment utilisés dans le jargon Internet. Les « *Black Hat* » désignent les *hackers* non éthiques faisant usage de leurs talents à des fins personnelles et malveillantes. Ils sont à l'origine de 40 % des attaques DDoS recensées dans notre échantillon. Pour eux, leur technique est une source de revenus efficace fondée sur le chantage et la menace. Adam, le *Black Hat* « repenti », admet disposer de 60 000 à 70 000 ordinateurs zombies pour réaliser des DDoS. Les réseaux zombies peuvent être plus impressionnants encore : ainsi, en avril 2012, le site *UK2.net*, l'un des plus gros hébergeurs du Royaume-Uni, a été attaqué par un réseau composé de plus de 10 millions d'adresses IP.

Adam nous confirme également que ces cybercriminels ne choisissent pas leurs cibles au hasard : « *S'il y a un grand événement sportif, comme le Super Bowl, vous pouvez* être sûr que 95 *% des sites de paris sportifs se sont fait extorquer de l'argent…* ». L'événementiel *online* est le secteur le plus juteux, car les victimes d'attaque sont dans l'impossibilité de refuser la transaction et les sommes en jeu sont très importantes.

Notre étude révèle (hélas) que les *Black Hat* s'intéressent à tous les types d'entreprise, de la TPE à la multinationale. En effet, ils soutirent habituellement entre 200 et 700 dollars par victime. Ce faible montant s'explique par le fait que ces cybercriminels souhaitent être payés très vite et qu'ils réalisent en moyenne une dizaine d'attaques par jour contre différentes entreprises. Ils optent donc pour une stratégie de volume.

Les sites *Web Meetup.com* et *Basecamp.com* ont ainsi été mis hors ligne durant plusieurs jours après avoir refusé de payer une rançon de 300 dollars. De même, une pizzeria de Dallas, Mas Pizza, a été contrainte de fermer son site en pleine opération promotionnelle de pizzas gratuites. En mai 2012, le groupe Voyager Mobile a, quant à lui, été obligé de reporter son inauguration à cause d'une attaque DDoS ayant visé son site principal.

Enfin, Adam nous rappelle à quel point les *Black Hat* sont dépourvus de morale : « *J'ai connu un groupe qui s'en était pris à un site de recherche contre le cancer, juste avant le lancement d'une grande campagne de collecte de fonds. C'est triste à dire, mais ce groupe a eu son argent…* ». On le constate : les *Black Hat* représentent donc une menace permanente pour les entreprises.

Les *hackers White Hat*

À l'extrême opposé des *Black Hat*, on trouve les « *White Hat* ». Ceux-ci sont des *hackers* éthiques qui n'attaquent qu'à la seule fin d'aider leurs cibles, parfois même contre leur volonté. En général, ils préviennent leurs cibles de leurs failles informatiques, et si celles-ci ne réagissent pas, ils divulguent publiquement ces failles pour les forcer à agir. C'est le cas d'*Abu Nazir*, un hacker polonais, qui a lancé une attaque DDoS en février 2012 contre le site de Gram24, une entreprise polonaise de *streaming vidéo*, afin de faire prendre conscience à ses responsables de certaines vulnérabilités susceptibles de mettre en danger les utilisateurs de leur site. Notre échantillon ne comporte que ce seul cas d'attaque par un *White Hat* (un unique cas qui s'explique par le fait que les *White Hat* recourent habituellement à des attaques bien plus complexes que ne le sont les DDoS).

Les *hackers* libertaires

Ces cyber-attaquants sont des représentants de la culture dite « *Hacker* ». Ils se battent pour un Internet ouvert à tous et pour une totale liberté d'expression. Ils sont responsables de 23 % des attaques DDoS que nous avons recensées au cours des quatre dernières années. Selon Vincent Cornalba (2013), ce type de *hacker* serait « le Robin des Bois des temps modernes » faisant plier les puissants sous les coups de ses attaques informatiques. Ainsi, le mouvement Anonymous a perpétré 41 attaques DDoS sur la période étudiée. Leurs cibles étaient extrêmement variées, allant de l'Église de Scientologie à la loi Hadopi (en France), en passant par Sony (avril 2011), ou bien encore Arcelor Mittal ou l'entreprise pétrolière Koch Industries. Ils réagissent avant tout à des mesures de censure ou de restriction de la liberté d'expression sur Internet. Cependant, il leur arrive de s'engager dans d'autres combats, comme nous l'avons vu récemment : après les attentats perpétrés contre le mensuel satirique Charlie Hebdo, le 7 janvier 2015, ils ont décidé de se mobiliser pour détruire le plus grand nombre possible de sites Internet de propagande islamiste.

Les Trolls

D'autres groupes appartenant à la culture « *hacker* » se situent plutôt dans l'esprit « *troll* ». Ils lancent des attaques DDoS juste pour s'amuser. C'est le cas de *TheWikiBoat,* qui a notamment attaqué le groupe KPMG, et du collectif *UGNazi Collective* qui s'en est pris à Twitter, au NASDAQ et à l'entreprise MGM (Metro Goldwyn Mayer). Même s'ils sont minoritaires dans notre échantillon, leurs attaques sont tout aussi destructrices que celles des autres cyber-attaquants.

Les cyber-djihadistes

Le cyberespace est, hélas, devenu un lieu d'expression des luttes religieuses : 21 % des attaques DDoS visant des entreprises leur sont imputables. 48 attaques ont notamment été revendiquées par le groupe d'hacktivistes Izz ad-Din al Qassam Cyber Fighters. En réalité, il s'agit de véritables vagues d'attaques : au cours de ces 48 vagues, 135 attaques DDoS contre 35 banques ont été enregistrées (parmi les banques attaquées, peuvent être citées : Bank of America, JP Morgan Chase, HSBC, American Express). Ces vagues d'attaques sont en lien avec la parution de la vidéo *The Innocence of Muslims* publiée par le pasteur protestant américain Terry Jones. En représailles, le groupe a attaqué les banques supposées être « *la propriété de capitalistes sionistes américains* ». Pour les banques, les pertes financières sont difficiles à estimer. Mike Rogers, membre républicain de la Chambre des Représentants des États-Unis, a déclaré que les pertes, pour l'une d'entre elles (dont il n'a pas souhaité révéler l'identité), s'étaient élevées à cent millions de dollars.

Par ailleurs, le hacker saoudien OxOmar, un activiste antisioniste, a été lui aussi très actif durant la période étudiée. Il a notamment réussi à détruire le site Internet d'un artiste danois (l'auteur des caricatures de Mahomet) et à pénétrer dans les serveurs les plus sécurisés au monde, tels ceux de Microsoft, de Kaspersky ou de Kevin Mitnick.

Les censeurs

Cette catégorie de *hackers* regroupe des cyber-attaquants dont l'objectif est de censurer des internautes avec lesquels ils ne sont pas d'accord.

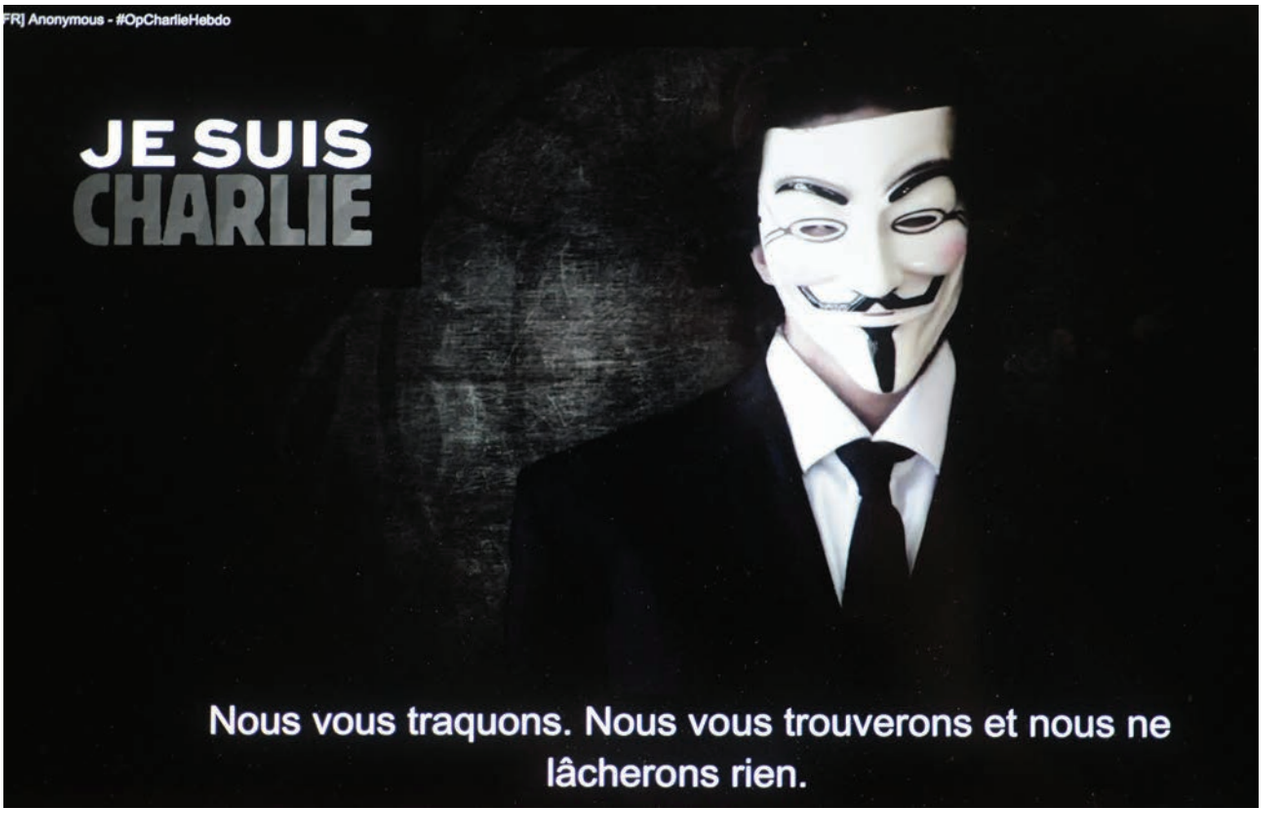

Photo © MAXPPP

« Les *hackers* libertaires réagissent avant tout à des mesures de censure ou de restriction de la liberté d'expression sur Internet. Cependant, il leur arrive de s'engager dans d'autres combats, comme nous l'avons vu récemment : après les attentats perpétrés contre le mensuel satirique Charlie Hebdo, le 7 janvier 2015, ils ont décidé de se mobiliser pour détruire le plus grand nombre possible de sites Internet de propagande islamiste. »

Les États sont souvent soupçonnés de commanditer ces attaques, mais leur responsabilité est difficile à démontrer. 12 % des attaques DDoS sont attribuées à ce profil de cyber-attaquant. En Russie, le *hacker* Hell attaque les blogueurs, les journalistes et les écrivains pro-démocratie. On recense également des attaques non revendiquées (et potentiellement commanditées) contre des médias indépendants, des agences de presse et des opposants politiques (comme celle ayant ciblé Mikhail Khodorkovsky, l'ancien PDG du *trust* pétrolier russe Youkos).

En Ukraine, l'agence de presse prorusse Ruptly, le site de la chaîne télévisée prorusse Channel One et le site de la Bank of Russia ont été mis hors ligne, à la suite du coup de force ayant entraîné l'éviction du président ukrainien Viktor Ianoukovitch. On recense des actions similaires liées au contexte politique dans de nombreux pays : au Mexique, en Chine, en Corée du Nord, ou encore au Zimbabwe. Enfin, aux États-Unis, le collectif Antileaks attaque toutes les entreprises qui soutiennent Julian Assange (le fondateur de Wikileaks) ou qui émettent une opinion positive à son sujet.

Les justiciers géopolitiques

Ces *hackers* utilisent les moyens Internet pour intervenir, à l'échelle internationale, dans des conflits géopolitiques. Leurs attaques ne représentent que 4 % de notre échantillon, car, la plupart du temps, ils attaquent directement les gouvernements. Les *hackers* tels que The Jester, patriote américain, et Israel Defense Forces (IDF Team), patriotes israéliens, agissent principalement en riposte. Ainsi, l'IDF Team a riposté aux attaques d'OxOmar. De son côté, The Jester a attaqué une série de sites Internet qu'il qualifie d'ennemis des États-Unis, comme 4chan. Il revendique également l'attaque de l'entreprise Datacell, parce qu'elle avait invité Edward Snowden (un informaticien américain à l'origine de la diffusion de données ultraconfidentielles de la NSA, notamment, à venir en Islande, en 2013.

D'autres « hacktivistes » essaient de faire entendre leur voix sur des sujets spécifiques. C'est le cas de Maxney, un membre du groupe de *hackers* turcs Ajan, qui souhaite que les États reconnaissent les « génocides en cours » en Palestine et au Turkestan oriental. Pour cela, il a attaqué par DDoS plusieurs entreprises prestigieuses, parmi lesquelles McDonald (Thaïlande), Avast (Allemagne), Acer (Inde), Renault (Bulgarie) et Nokia (Taiwan).

Le conflit syrien génère également de nombreuses cyber-attaques, telles celles de la Syrian Electronic Army, qui s'en prend aux médias supposés hostiles à Bashar Al-Assad. En août 2013, ils ont mené une attaque DDoS contre le *Washington Post,* parce

que celui-ci avait dressé un portrait peu élogieux du président syrien.

Quelles sont les victimes privilégiées des cyber-attaques ?

L'analyse des 234 attaques que nous avons recensées révèle que 62 % de celles-ci se sont concentrées sur le secteur de la finance (36 %) et sur celui des « *pure players* » (26 %), c'est-à-dire des entreprises de service travaillant uniquement sur Internet. 25 % des attaques visent le secteur des médias (14 %) et celui du divertissement (11 %). Enfin, les 13 % restants se répartissent entre les secteurs des télécommunications (5 %) et de l'industrie (4 %), ainsi que des autres services (4 %).

Le secteur financier

Le secteur financier est le plus fortement impacté par des attaques de type DDoS, et de très loin. Les banques en sont les premières victimes (83 % des attaques). Viennent ensuite les marchés financiers (11 %) et les sites de transaction de la monnaie virtuelle Bitcoins (6 %). Les opérations malveillantes des *Black Hat* ne représentent que 28 % du total de ces attaques. Selon nous, ce résultat s'explique par la nature des attaques DDoS, lesquelles, sauf à servir de support pour masquer une autre attaque, ne permettent pas de voler de l'argent directement.

71 % du total de ces attaques sont imputables à des groupes divers ayant comme motif principal l'« hacktivisme ». Celui-ci consiste à mettre son expertise informatique au service de ses convictions politiques, éthiques ou religieuses. Pour les hacktivistes, le secteur de la finance est un symbole : il représente le pouvoir en place et la société capitaliste. Cela explique notamment les vagues d'attaques contre les banques perpétrées par les djihadistes d'Izz ad-Din al Qassam Cyber Fighters et l'attaque de la bourse de Tel Aviv par OxOmar.

Pour les Anonymous, qui ont notamment attaqué le site du NYSE lors de l'opération « *OccupyWallStreet* », l'attaque des banques symbolise la lutte entre le peuple et l'élite économique. Sur l'une de leurs vidéos concernant l'opération « *Invade Wall Street* », le collectif de *hackers* explique : « *Nous avons observé les autorités chargées de l'application de la loi punir les 99 % tout en laissant les 1 % échapper à la justice* ». Les actions du collectif visent donc à rétablir la justice et à défendre les opprimés. Dans tous les autres cas étudiés d'hacktivisme, la finance apparaît toujours comme une cible symbolique. Ces attaques sont aussi un excellent moyen de se faire remarquer par les médias.

Les « *pure players* »

Le deuxième secteur le plus attaqué est celui des services Internet (26 % des attaques). 82 % des attaques DDoS dans ce domaine relèvent de la cyber-criminalité. Les *Black Hat* savent que le modèle économique de ces entreprises repose totalement sur la disponibilité de leurs services. Les attaques DDoS sont donc une arme efficace pour les faire chanter. 11 % des attaques relèvent de l'hacktivisme, et notamment du mouvement Anonymous. Enfin, on observe, à la marge, des cas d'attaques purement gratuites, « pour le *lulz* ».

Les cibles privilégiées sont les hébergeurs. Ils représentent en effet des proies de choix pour les pirates, car de nombreux sites Internet reposent sur eux. Attaquer un hébergeur leur permet de mettre hors ligne tous ses clients. Il y a donc de fortes chances pour que celui-ci paie rapidement la rançon. Les hébergeurs intéressent également les hacktivistes et les justiciers géopolitiques : ainsi, par exemple, l'attaque d'un hébergeur israélien a permis de toucher l'ensemble de la société civile israélienne, et ce, grâce à une unique attaque bien ciblée.

Les services de partage de textes, comme Pastebin, sont également très attaqués. Il s'agit de sites habituellement utilisés par les *hackers* et les programmeurs pour partager du code source. Cependant, ces sites sont aussi utilisés par les pirates informatiques pour exprimer leurs revendications, car ils leur garantissent l'anonymat. Ainsi, OxOmar a attaqué Pastebin, car il estimait que ses messages de revendications étaient supprimés, alors que ceux de ses opposants israéliens étaient conservés sur ce même site.

Les entreprises du secteur de la sécurité Internet sont globalement peu attaquées de cette manière : nous n'avons recensé que quatre attaques sur la période étudiée. Trois attaques semblent d'origine cybercriminelle, avec notamment la spectaculaire attaque de Spamhaus (le 27 février 2013). Spamhaus est un fournisseur de protection en temps réel contre les spams et les pourriels. L'ampleur de l'attaque fut telle qu'elle a ralenti l'ensemble du trafic Internet mondial de manière perceptible par un internaute « lambda » et qu'elle a permis la propagation de milliards de spams sur l'ensemble des continents.

Enfin, les réseaux sociaux sont également assez peu attaqués. Les sites *Reddit.com*, *Meetup.com*, *soup.io*, *pof.com* et *Twitter* n'ont fait l'objet que d'une seule attaque chacun.

Le secteur des médias

Le secteur des médias a été victime de 14 % des attaques DDoS de la période considérée. L'hacktivisme est le premier motif d'attaque visant des médias. Les médias diffusant des informations de nature politique sont particulièrement exposés. Les hacktivistes les prennent donc pour cibles pour se faire connaître ou pour contester des informations diffusées par lesdits médias. Très attaqués par les Anonymous (21 % des attaques) qui, paradoxalement, défendent la liberté d'expression, les médias sont surtout la cible favorite des censeurs (49 %), tels qu'Hell et Antileaks, ou d'autres *hackers* anonymes, dont les liens n'ont pas été clairement établis. Enfin, 18 % des attaques attribuables aux *Black Hat* semblent être d'origine cybercriminelle.

Le secteur du divertissement

Ce secteur est une cible symbolique pour les *hackers* libertaires (plus de 50 % des attaques). Loin de la politique, cette cyber-guerre est économique et s'articule autour des droits de propriété et de la gratuité sur Internet. Les *hackers* libertaires veulent libérer Internet, alors que l'industrie du divertissement est partisane des droits d'auteur et des politiques sécuritaires. Les attaques les plus retentissantes ont eu lieu en janvier et en avril 2012 après la fermeture de *Megaupload* et l'interdiction de *The Pirate Bay*, deux sites majeurs de téléchargement illégal.

Anonymous et les groupes qui lui sont rattachés ont également attaqué l'industrie du sport pour des raisons politiques. Il s'agit de revendications politiques ponctuelles, telles que la défense des droits de l'Homme au Bahreïn (qui a motivé l'attaque des sites des grands prix de Formule 1 dans le cadre de l'opération #OpBahreïn), la protection des animaux en Ukraine (80 000 chiens auraient été tués à Kiev en lien avec l'Euro 2012) ou la condamnation de la guerre civile syrienne (pour laquelle une cible très visible comme la World Wrestling Entertainment a été choisie).

Par ailleurs, 31 % des attaques sont liées aux *Black Hat* et ciblent principalement les serveurs de jeux vidéo en ligne. La sortie d'un nouveau jeu vidéo est souvent propice à un déferlement d'attaques DDoS d'origine cybercriminelle. Ces entreprises sont aussi les cibles d'opérations de « *lulz* » de la part de *trolls*. Cependant, ces « *lulz* » sont mal perçus par les *hackers* et les internautes, du fait qu'ils affectent un secteur qui est particulièrement apprécié des accros de l'informatique.

Le secteur des télécommunications

Ce secteur représente seulement 4 % des attaques ciblées DDoS de la période considérée. Celles-ci sont surtout perpétrées par des *Black Hat* (67 % des attaques). Les seuls cas d'hacktivisme recensés (22 %) concernent des entreprises qui ont soutenu ou collaboré avec des gouvernements pratiquant la censure (comme l'Inde) ou ayant déposé des projets de lois liberticides, comme le projet de loi CISPA (*Cyber Intelligence Sharing and Protection Act*), aux États-Unis. Les opérateurs de réseaux de téléphonie mobile sont touchés à hauteur des 56 % et les fournisseurs d'accès à Internet représentent 44 % des victimes.

Le secteur de l'industrie

Nous avons recensé neuf entreprises industrielles ayant été attaquées par DDoS. Sept de ces entreprises ont fait les frais de l'hacktivisme des *hackers* libertaires et des justiciers géopolitiques. Ainsi, par exemple, l'opération #OpDefense (des Anonymous) punissant les entreprises ayant soutenu la loi CISPA a frappé Boeing et les associations d'entreprises technologiques National Cable and Telecommunication Association et Tech America. Les Anonymous ont également attaqué Microsoft Japon dans le cadre de #OpKillingBay afin de sensibiliser le public au massacre des dauphins. Les deux autres entreprises, Glencore et Videolan, ont respectivement été attaquées pour le « *lulz* » et à des fins de racket cybercriminel.

Autres services et e-commerce

Les autres services concernent 5 % des attaques DDoS de l'échantillon. Les entreprises de l'e-commerce sont à 100 % victimes de la cybercriminalité. Il ne s'agit cependant que de trois cas d'attaque sur les 234 composant l'échantillon. Ce très faible nombre d'attaques tiendrait au fait que les entreprises de l'e-commerce sont bien équipées en moyens de lutte contre le DDoS.

Par ailleurs, des universités américaines ont également fait l'objet d'attaques DDoS dans le cadre de l'hacktivisme : il s'agit notamment de Harvard University, de la North-side Independent School District et du M.I.T. À chaque fois, il s'agit d'un cas très précis, aucune généralisation n'est donc possible. Harvard University a été attaquée pour son soutien à Julian Assange, le fondateur et rédacteur en chef de WikiLeaks. La North-side Independent School District en a été la victime suite à sa décision de géo-localiser ses élèves à l'aide de badges. Enfin, le M.I.T a été attaqué par les Anonymous en représailles au suicide du chercheur Aaron Swartz. Ce dernier avait été poursuivi en justice pour avoir utilisé frauduleusement la base de données documentaires (articles de presse de plus de 3 000 quotidiens et périodiques) payante JSTOR. Il était passible de plusieurs milliers de dollars d'amende.

Comment prévenir, plutôt que guérir ?

Nous avons interviewé plusieurs professionnels de la sécurité, une fois notre étude réalisée. Il ressort de ces entretiens que les solutions pour prévenir les attaques DDoS ne sont pas exclusivement techniques. Nous synthétisons ici le fruit de nos réflexions en la matière afin d'orienter les entreprises dans le dédale des pistes d'actions stratégiques à entreprendre.

Le juste prix de la protection technique

Pour l'ensemble des secteurs d'activité concernés, la première réaction est de se protéger techniquement contre les attaques DDoS. Cependant, les protections anti-DDoS complètes sont coûteuses. Il faut donc trouver un juste équilibre et protéger le site à hauteur des risques qu'il encourt. Les sites des *pure players* et les sites de l'e-commerce sont ceux qui devront investir le plus dans cette protection. Les professionnels leur recommandent d'ailleurs d'effectuer un audit et un test pour évaluer l'ampleur de leurs failles informatiques.

Pour les entreprises qui présentent un risque modéré d'attaque cybercriminelle, le *Black Hat* repenti Adam préconise d'investir dans le système Cloudflare, qui coûte 200 dollars par mois et qui constitue, selon lui, « *un obstacle notable* » aux attaques DDoS. Cet investissement est rentabilisé dès la première attaque subie.

Pour les petites et très petites entreprises (PME/TPE), dont le modèle commercial ne repose pas essentiellement sur leur site Internet, les professionnels interrogés

recommandent de créer une architecture des systèmes d'information qui soit très décentralisée et qui permette, de ce fait, de remettre sur pied tout leur système informatique très rapidement, après avoir subi une attaque.

Enfin, la majorité des attaques ont lieu lors d'événements importants pour les entreprises, comme des opérations promotionnelles, des inaugurations, la sortie de nouveaux produits ou à l'approche d'événements culturels et sportifs auxquels elles sont associées. Les PME sont particulièrement touchées par ce type de racket. Il est donc indispensable pour elles de relever les barrières de leur sécurité informatique avant la date de l'événementiel et de maintenir ce niveau de vigilance supérieur jusqu'à la fin de l'opération. Cet ajustement ponctuel permet de prévenir les attaques DDoS et de rendre la tâche plus difficile aux cyber-attaquants.

La mise en place d'une stratégie préventive

Une étude menée par Chalamon, Chouk et Guiot (2012) sur la cyber-résistance des consommateurs présente trois types de stratégie : la stratégie répressive, la stratégie préventive et, enfin, la stratégie collaborative. La stratégie préventive consiste à réaliser une veille avec prévention des failles informatiques et à anticiper les consommateurs mécontents. Pour les secteurs les plus touchés par l'hacktivisme, comme ceux de la finance, de l'industrie et des médias, la mise en place d'une cellule de veille est d'importance stratégique. En effet, nous avons constaté que la majorité des victimes d'hacktivisme de notre échantillon avaient été prévenues de l'imminence de l'attaque *via* des plateformes comme Pastebin. Une veille efficace permettrait de savoir comment relever les barrières de protection dès qu'une attaque se profilerait et de mettre en place une politique de relations publiques pour être à même d'anticiper les problèmes à venir.

Évaluer son capital symbolique

Le caractère symbolique des attaques des hacktivistes devrait amener les entreprises à réfléchir à l'image qu'elles véhiculent parfois sans le vouloir. Les entreprises évoluant dans le monde de la finance notamment présentent un capital symbolique élevé pour les justiciers géopolitiques. Il en va de même en ce qui concerne les grandes entreprises du secteur du divertissement et pour celles qui relèvent de certains types d'industrie. Plus l'imaginaire collectif les associe au pouvoir, à la suprématie et à la domination capitaliste, et plus ces entreprises sont susceptibles d'être victimes de ce genre d'attaque.

Par ailleurs, les entreprises les plus connues mondialement sont des cibles de choix pour les hacktivistes. Ils considèrent en effet qu'ils seront mieux entendus s'ils s'attaquent à des entreprises prestigieuses. Il est intéressant, pour ces entreprises, de réaliser des études sur la manière dont elles sont perçues par le grand public, car notre étude montre que plus leur capital symbolique est élevé, et plus la probabilité qu'elles soient attaquées est élevée.

Choisir ses combats et faire preuve de prudence dans ses prises de positions publiques ou sociétales

Quel que soit le secteur d'activité, il est essentiel que l'entreprise soit vigilante sur ses prises de positions politiques ou sociétales. Pour rappel, plusieurs entreprises, comme Bambuser, ont subi des attaques massives des Anonymous après avoir soutenu les projets de lois américaines SOPA (*Stop Online Piracy Act*) et PIPA (*Protect intellectual property Act*). La discrétion de l'entreprise et de ses dirigeants sur leurs positions politiques ou sociétales reste la meilleure manière d'éviter des cyber-attaques de type DDoS. De la même manière, tous les sujets en rapport avec la liberté d'expression, la surveillance et la régulation d'Internet sont susceptibles d'entraîner une réaction violente de la part des *hackers* libertaires.

Soigner sa e-réputation

Dans le secteur du divertissement, l'image de l'entreprise est particulièrement importante. Il s'agit en particulier de s'adresser aux *hackers* libertaires, qui sont des consommateurs assidus de ce type de produit. Pour cela, une stratégie collaborative semble être la plus appropriée. D'après Chalamon, Chouk et Guiot (2012), cette stratégie consiste à mettre en œuvre des outils de gestion de l'e-réputation et à créer une relation avec les internautes par l'intermédiaire d'un *Community manager*, l'idée étant de prendre en compte les réactions des internautes afin d'améliorer sans cesse la réponse de l'entreprise.

Un *community manager* bien formé interagissant sur les réseaux sociaux avec les clients peut être efficace. Il faut expliquer les prises de position de l'entreprise, notamment vis-à-vis des droits d'auteur et inciter les internautes à donner leur avis et à participer à l'évolution du modèle économique. Par ailleurs, l'attention portée à l'e-réputation est un levier pour gérer au quotidien le capital symbolique de l'entreprise.

Éviter les stratégies répressives

La stratégie répressive évoquée par Chalamon, Chouk et Guiot (2012) consiste à utiliser des moyens juridiques pour sanctionner les agissements frauduleux des *hackers*. Outre le fait qu'elle soit difficile à mettre en œuvre comme le soulignent les auteurs précités, notre étude tend à montrer que cette stratégie est plutôt contre-productive. En effet, une stratégie très répressive envers un *hacker* peut entraîner le soutien massif d'autres *hackers* qui s'empresseront de le défendre en attaquant sa victime par DDoS. Cela fut le cas en janvier 2013, suite au suicide du chercheur Aaron Swartz, ou encore en mars 2013, en ce qui concerne Gary McKinnon, un programmeur de l'entreprise Sendmail qui avait été renvoyé injustement. Les actions répressives doivent donc être mûrement réfléchies, car elles peuvent s'avérer contreproductives en attirant en retour les foudres de la communauté des *hackers*.

Photo © PANORAMIC

Piratage de la chaîne TV5 Monde – Capture d'écran du 9 avril 2015.

« À l'heure où nous écrivons ces dernières lignes, la chaîne TV5Monde vient de subir une cyber-attaque de grande ampleur, qui a été revendiquée par l'État islamique. »

Conclusion

Cette analyse des cyber-attaques de type DDoS nous a permis de mettre au jour plusieurs variables qui peuvent potentiellement prédire la survenue d'attaques ciblées à l'encontre d'entreprises privées ou publiques. Cette mise au jour est essentielle, car le nombre des attaques DDoS augmente d'année en année. Nous pensons d'ailleurs que, dans notre échantillon, les attaques des cybercriminels sont sous-représentées par rapport à la réalité. En effet, les cybercriminels comme leurs victimes restent souvent discrets à ce sujet. Les attaques recensées sont celles qui ont laissé des traces, parce qu'elles ont impacté la réputation des entreprises et qu'elles ont été relayées dans la presse spécialisée ou sur Internet.

Le milieu de la cyber-sécurité est tout aussi peu enclin à la diffusion d'informations. Au cours de nos entretiens, nous avons bien senti que certaines portes demeuraient fermées. La raison principale invoquée est que les détails techniques ne peuvent être révélés, de peur de faciliter la tâche aux cyber-attaquants. Des travaux de recherche dans ce domaine sont donc difficiles à réaliser.

Cependant, cette difficulté d'accès au terrain ne doit pas décourager les jeunes chercheurs en sciences de gestion de s'intéresser à ce domaine encore peu exploré. En effet, l'imbrication de plus en plus étroite entre le monde économique et le cyberespace oblige les entreprises à intégrer cette dimension informatique dans leurs réflexions managériales et leurs outils de gestion. Elles ont besoin d'éclairages empiriques et théoriques pour mieux comprendre ces nouveaux risques. Il existe une grande variété de cyber-attaques, et il serait donc intéressant de poursuivre des recherches similaires sur d'autres types d'attaque afin de comparer les profils et les motivations des cyber-pirates. À l'heure où nous écrivons ces dernières lignes, la chaîne TV5Monde vient de subir une cyber-attaque de grande ampleur, qui a été revendiquée par l'État islamique. Des recherches dans ce domaine semblent donc absolument indispensables pour protéger les entreprises privées et publiques. Nous sommes aujourd'hui à l'aube de la structuration, dans le domaine des sciences de gestion, d'un champ de recherche appliquée à part entière dédié à la gestion des cyber-attaques.

Bibliographie

D'AMICO (A.), *What Does a Computer Security Breach Really Cost?,*The Sans Institute, 2000.

ARUNDHATI (R.), MOHAMED (W.) & WILLIAMS (J. L.), "Intraday Study of the Market Reaction to Distributed Denial of Service (Dos) Attacks on Internet Firms", *Academy of Accounting and Financial Studies Journal*, 15(2), 2011.

CHALAMON (I.), CHOUK (I.) & GIUOT (D.), « La cyber-résistance du consommateur : quels enjeux pour les entreprises ? », *Décisions marketing*, 68, octobre-décembre, pp. 83-88, 2012.

HULT (F.) & SIVANESAN (G.), "Introducing cyber", *Journal of Business Continuity & Emergency Planning*, 7(2), pp. 97-102, 2013.

Group-XP-OxOmar (2012), Pastebin [consulté le 12 janvier 2015], http://pastebin.com/DWi5MW6x

HUYGHE (F-B.), « Stratégie dans le cyberespace », *Médium,* 2(31), pp.129-146, 2012.

KASPERSKY Lab. (2013), *Kaspersky Security Bulletin 2013,* http://media.kaspersky.com/pdf/KSB_2013_EN.pdf

Mcafee, Center for Strategic and International (2013), *The Economic Impact of Cybercrime and Cyber Espionage*, http://csis.org/files/publication/60396rpt_cyber-crime-cost_0713_ph4_0.pdf

OxOmar (2012), Pastebin, [consulté le 12 janvier 2015], http://pastebin.com/u/0xOmar

Hackmageddon.com, http://www.hackmageddon.com/

QassamCyberFighters (2012), Pastebin, [consulté le 10 janvier 2015], http://pastebin.com/u/QassamCyberFighters

SAUTER (M.), "LOIC Will Tear Us Apart: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks", *American Behavioral Scientist,* march 15, pp. 983-1007, 2013.

White Hat Security (2013) [consulté le 10 janvier 2015], https://blog.whitehatsec.com/interview-with-a-blackhat-part-1/

Wikipedia [consulté le 10 décembre 2014], https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service

Wikipedia [consulté le 10 décembre 2014], https://fr.wikipedia.org/wiki/Hacker_%28s%C3%A9curit%C3%A9_informatique%29

World Economic Forum (2014), *Global Risks 2014 Ninth Edition,* http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf