Lettre n°59-Février 2017-disponible sur omc.ceis.eu

Brève du mois

« Si un candidat estime qu'il fait l'objet d'une attaque susceptible d'affecter le déroulement de sa campagne, il pourrait saisir la Commission [CNCCEP].» a déclaré Jean-Marc Sauvé, président de la Commission nationale de contrôle de la campagne en vue de l'élection présidentielle et du Conseil d'Etat. Jean-Jacques Urvoas, garde des Sceaux, a cependant précisé qu'il revenait aux candidats et aux partis politiques de **« mettre en œuvre les solutions adéquates »** pour y faire face[1].

[1] http://www.lci.fr/elections/presidentielle-la-commission-de-controle-veillera-particulierement-2027429.html

CYBER ATTAQUES : LA RESILIENCE DES DEMOCRATIES EST-ELLE EN DANGER ?

En décembre 2016, le renseignement américain affirmait à travers deux rapports[2;3] que le gouvernement russe avait cherché à favoriser l'élection de Donald Trump et à discréditer la campagne de la candidate démocrate, Hillary Clinton. Le rapport accuse la Fédération de Russie d'être responsable de la cyberattaque dont a été victime le parti démocrate et qui avait notamment donné lieu, par la suite, à la divulgation d'e-mails de plusieurs responsables du Parti démocrate, contenant notamment des informations personnelles et financières sur les donateurs du parti. Si la corrélation entre ces attaques et la défaite d'Hillary Clinton ne peut être prouvée de manière certaine, ces attaques ont le mérite de soulever une question importante : la résilience de nos systèmes démocratiques est-elle menacée par les attaques « cyber », qu'il s'agisse d'attaques informatiques ciblant les réseaux et les systèmes d'information ou d'attaques informationnelles visant à désinformer et tromper une cible déterminée ? Bien que souvent confondus, les deux modes opératoires sont en effet très différents : le premier vise l'infrastructure numérique en tant que telle ; le second cible les contenus circulant dans l'espace numérique.

La cybersécurité, un enjeu devenu incontournable pour la démocratie

Comme le montrent les attaques subies par le site du parti démocrate aux Etats-Unis ou celles subies par le site du mouvement d'Emmanuel Macron, le premier risque reste les attaques informatiques traditionnelles susceptibles de viser les partis politiques, les médias, voire les opérations électorales elles-mêmes. Si la surface d'exposition de ces dernières reste limitée en France où les opérations de vote se déroulent de façon très traditionnelle (des bulletins en papier et des urnes transparentes)[4], les partis politiques restent très exposés, notamment lorsque leurs sites utilisent des *Content Management System* (CMS) rarement mis à jour en termes de sécurité… La divulgation de données personnelles ou d'échanges internes peuvent en effet affecter durablement la crédibilité des candidats et du parti qui les soutient.

Même chose pour les médias dont la légitimité et l'intégrité constituent une donnée essentielle dans la perception de l'information qu'ils diffusent. Si les citoyens n'ont plus confiance en un média, c'est le rôle même de l'organe de presse dans le système démocratique qui s'en trouve dénaturé. Le vol d'une base de données contenant les informations personnelles des sources d'un journaliste pourrait par exemple être utilisé à des faits de décrédibilisation du journaliste et plus largement du média auquel il est affilié. Il en est de même pour les données personnelles des journalistes ou les échanges de mail, qui constituent des données pouvant influencer la perception des citoyens quant au support mais également des idées que celui-ci défend.

---

[2] https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[3] https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[4] On dénombrait 64 communes de plus de 3 500 habitants équipées de machines à voter en 2012. Plus de 1,5 million d'électeurs sont donc concernés par des machines, ce qui n'est pas anodin à l'échelle du corps électoral. Source : http://www.numerama.com/politique/232966-presidentielle-pourquoi-francois-hollande-redoute-des-cyberattaques.html

Les différents attributs des régimes démocratiques, qu'il s'agisse des partis politiques, des médias, des systèmes de vote (machine à voter ou vote en ligne), et plus globalement des « civic tech » constituent ainsi de véritables infrastructures vitales qu'il importe de protéger, au même titre que l'énergie, les transports ou les banques.

Les algorithmes des moteurs de recherche en question

A côté des attaques informatiques proprement dites, les opérations de déstabilisation et de manipulation de l'information connaissent un nouvel essor avec l'avènement de l'espace numérique. Permettant de toucher des dizaines de millions de personnes en s'affranchissant des relais traditionnels que sont les médias, Internet constitue une caisse de résonnance formidable mais aussi, potentiellement, un miroir déformant de la réalité.

Dans ce schéma, les moteurs de recherche ont pris une place de premier ordre, ceux-ci constituant souvent la première étape vers l'information. Point le plus critique : les algorithmes utilisés pour classer les résultats de recherche qui sont un facteur déterminant dans l'appréhension et la perception des informations, a fortiori dans un contexte électoral, d'autant qu'ils sont le plus souvent de véritables boites noires. Pendant les élections américaines, une théorie accusant Google de favoriser délibérément Hillary Clinton est ainsi apparue. Même si cette accusation ne peut être vérifiée car Google garde jalousement son algorithme de référencement secret, elle met en exergue le rôle central joué par ces moteurs dans l'orientation des internautes. Rappelons qu'en France, Google est aujourd'hui utilisé par 90% des français lors d'une recherche sur internet.

Deux études scientifiques récentes soulignent d'ailleurs ce rôle clé :

- Une étude parue dans la prestigieuse revue de l'Académie des sciences des Etats-Unis (« *The Search Engine Manipulation Effect [SEME] and Its Possible Impact on the Outcomes of Elections* », de Robert Epstein et Ronald E. Robertson, et Proceedings of the National Academy of Sciences[5]) démontre l'impact du référencement des sites sur un moteur de recherche dans le choix d'un candidat pour un électeur indécis. Les deux scientifiques américains montrent ainsi que ce référencement a une influence indéniable sur le choix des citoyens, ces derniers ayant systématiquement choisi le candidat qui était favorisé par son rang dans le classement du moteur de recherche.
- Dans son ouvrage *Egocratie versus Démocratie,* Alban Martin explique comment les moteurs de recherche tiennent une place croissante dans le fonctionnement démocratique[6]. Sur Internet, les opinions marginales qui n'auraient pas passé le filtre de la presse traditionnelle peuvent en effet gagner une exposition médiatique, et donc de l'influence, si elles sont bien référencées. Or s'il favorise par exemple les sites gouvernementaux parce qu'ils les jugent plus crédibles, en les plaçant en haut des pages de classement, Google joue par là même un rôle politique essentiel, en confortant de fait la communication officielle par rapport aux opinions divergentes. C'est la raison pour laquelle, en Chine, les moteurs de recherche sont considérés comme un élément incontournable de la souveraineté numérique.

[5] http://www.lemonde.fr/idees/article/2016/01/27/de-l-influence-de-google-sur-les-resultats-electoraux_4854577_3232.html

[6] http://www.numerama.com/magazine/16684-google-peut-il-garder-ses-algorithmes-secrets-et-rester-neutre.html

A l'instar des médias traditionnels, les moteurs de recherche ne sont donc pas neutres : ils orientent et filtrent l'information. Mais leur impact est démultiplié compte tenu du nombre de personnes qu'ils permettent de toucher, de leur instantanéité, de leur effet égalisateur et du secret entourant leurs algorithmes.

Ils ont par ailleurs un effet déformant, internet n'étant qu'un reflet déformé de la réalité. Un petit parti politique, qui n'aura pas la même présence médiatique (au sens traditionnel : radio, télé, papier) qu'un parti politique plus important fera par exemple de sa présence sur internet un élément clé de sa campagne. Et s'il y est davantage présent (vidéos Youtube, comptes des réseaux sociaux proactifs, etc.), son référencement sur Google s'en retrouvera favorisé par rapport à des partis politiques qui ont une communication plus traditionnelle. Les réseaux sociaux jouent enfin un rôle clé, notamment dans les algorithmes de Google. Une étude[7] a ainsi montré que les moteurs de recherches utilisaient les réseaux sociaux non pas comme une simple plateforme proposant des liens vers une page web mais comme un moyen d'analyser et de détecter les pages intéressantes qu'il faut faire sortir du lot.

Cet effet déformant pourra encore être accéléré en détournant à des fins malveillantes le fonctionnement d'un moteur de recherche et de leurs algorithmes. C'est par exemple le rôle des *bots* de réseaux sociaux qui permettent de créer et d'animer des milliers de faux-comptes qui peuvent propager une information non vérifiée, contribuer à sa popularité et la placer en tête des résultats de recherche. Qu'elle soit exacte ou fausse, cette information va donc venir perturber la réception de l'information par les citoyens qui, s'ils ne sont pas avertis, vont la placer sur le même plan de véracité qu'un fait vérifié et recoupé.

Des recommandations essentielles

Face à ces risques, la première recommandation à destination des partis politiques et des médias relève de l'hygiène numérique chère à l'ANSSI : éviter d'utiliser les clés USB venant de l'extérieur ou les connections permanentes, vérifier l'émetteur du mail, choisir un mot de passe de 12 à 14 caractères alphanumériques ou encore maintenir à jour ses applications. Mais ces mesures doivent aussi s'inscrire dans une démarche de sécurité plus globale basée sur une analyse des risques. Quelles sont les données sensibles dans un contexte électoral ? Pour un parti politique, citons par exemple les données personnelles et les listings des adhérents, les données financières et les factures ou bien encore la sécurité du vote électronique si celui-ci est utilisé. En matière d'infrastructures, le recours à des hébergeurs spécialisés susceptibles de résister à des attaques DDoS est également essentiel. Notons que l'attaque de janvier 2015 contre la chaîne TV5 Monde a largement contribué à la sensibilisation du secteur.

Au plan informationnel, différentes solutions permettent de détecter des pages frauduleuses ou de faux profils. Exemple : la solution ZeroFox utilisée par le Monde et TV5 Monde qui détecte les pages Facebook usurpant l'identité d'une entreprise ou d'une organisation en reprenant son nom, son logo, sa description, et servent ainsi à légitimer une information erronée. Cette solution permet également de surveiller l'activité sur une page Facebook et de détecter des comportements suspects

[7] http://www.abondance.com/actualites/20110420-8952-de-linfluence-des-reseaux-sociaux-sur-lalgorithme-de-google.html

Le fact-checking : solution miracle ?

Les moteurs de recherche et les réseaux sociaux ont également pris en compte le risque d'une cyberdéstabilisation dans le cadre d'une campagne électorale. Google et Facebook s'allient désormais aux journaux afin de vérifier les informations suspectes.

Intitulée Crosscheck[8], l'initiative est portée par First Draft, start-up financée par le Google News Lab. Collaboratif, le dispositif mis en place par Facebook et Google permettra d'améliorer le signalement par ses utilisateurs d'informations potentiellement erronées, et leur vérification par des journalistes grâce à un partenariat pour l'instant rejoint par huit médias français : l'AFP, BFMTV, L'Express, France Médias Monde, France Télévisions, Libération, Le Monde et 20 Minutes.

Outre cette initiative, Facebook a développé un outil anti « fake news »[9] qu'il teste actuellement en Allemagne[10]. Facebook propose pour sa part une commande qui permet de signaler un contenu comme contenant de fausses informations. Il s'agit en réalité d'une adaptation d'une fonctionnalité existante, puisqu'il était déjà possible de signaler un message comme étant "ennuyeux" ou "indésirable". Le site comptabilisera ces signalements et décidera en fonction de cela, et d'autres critères non précisés, de soumettre le contenu à des vérificateurs spécialisés qui s'appuieront sur les codes du fact-checking de l'Institut de journalisme Poynter. Suite à leur travail, les contenus litigieux seront tagués et indiqués comme "contestés par des vérificateurs indépendants" mais ces contenus ne seront pas censurés ou effacés. Autre conséquence : ces contenus ne pourront plus faire l'objet d'une promotion publicitaire.

Une résilience sociétale

En dehors des actions menées directement par les partis politiques et les médias, c'est la société toute entière qui se sensibilise aujourd'hui aux problématiques de cyberdéstabilisation lors d'une campagne électorale.

Le fact-checking en est le meilleur exemple. Si les partis politiques l'utilisent aujourd'hui lors des débats avec des adversaires afin de vérifier et de contrer des arguments, les médias ont désormais compris qu'ils avaient un réel rôle à jouer.

Les principaux médias français ont donc chacun mis en place des équipes dédiés à cette tâche (Désintox[11] pour Libération, Les Décodeurs[12] pour Le Monde, etc.). Mais s'ils sont désormais présents pour vérifier ces informations, c'est qu'il existe aujourd'hui une quantité d'information qui doit être vérifiée. Se retrouvant dans l'incapacité de vérifier chaque information une par une, le journal Le Monde a développé un outil à la portée de chaque internaute : Le Décodex.

Fruit de plus d'un an de travail, le Décodex, lancé début février 2017 par Le Monde, est un outil qui vise à lutter contre la diffusion virale de fausses informations et à aider les internautes à se repérer dans la jungle

---

[8] http://www.latribune.fr/technos-medias/internet/fake-news-facebook-et-google-lancent-de-nouveaux-outils-en-france-636552.html

[9] http://www.francetvinfo.fr/internet/reseaux-sociaux/facebook/signalement-fact-cheking-comment-facebook-veut-lutter-contre-les-fausses-informations_1928867.html

[10] http://www.zdnet.fr/actualites/facebook-commence-a-tester-son-outil-anti-fake-news-en-allemagne-39847194.htm

[11] http://www.liberation.fr/desintox,99721

[12] http://decodeurs.blog.lemonde.fr/

des sites producteurs ou relayeurs d'informations : est-ce un média citant ses sources et vérifiant ses informations, un site fabriquant ou propageant de fausses informations, un site militant ne mentionnant pas son affiliation politique ?

Concrètement, l'outil classe les sites selon différents niveaux de fiabilité, en fonction notamment de leur historique de publication. L'outil existe sous la forme d'un site internet, mais également de plugins de navigateur qui affichent la classification des sites consultés au cours de la navigation.

Ce type d'outil divise. Si l'initiative peut sembler salutaire, il reste contraint par l'affiliation de ses auteurs à leur journal et à sa ligne éditoriale. Ceux-ci se retrouvent effectivement tout à la fois juges et partis.

Cet outil constitue quoiqu'il en soit une prise de conscience et une première réponse de la part d'un média traditionnel, confrontés d'un côté à une perte d'hégémonie sur l'information (consécutif du web 2.0), et de l'autre côté à un phénomène de cyberdéstabilisation dans des contextes électoraux.

QUAND LES CYBERCRIMINELS S'INSPIRENT DES DERNIERES PRATIQUES DU MARCHE DE LA SECURITE INFORMATIQUE

La communauté cybercriminelle ne cesse d'innover. Ingénieux, les cyberattaquants n'hésitent plus à détourner les nouvelles pratiques de la sécurité informatique à des fins malveillantes. Exemple avec le bug bounty et l'ubérisation de la sécurité.

En décembre 2016, un nouveau modus operandi basé sur la gamification, ou ludification, a été identifié sur la plateforme underground turque Surface Defense. Cette nouvelle pratique consiste à rapprocher les sphères hacktiviste et cybercriminelle jusqu'alors relativement indépendantes. Elle se matérialise par le procédé suivant : en dressant une liste de site web d'organisations politiques comme cibles, le groupe garantit aux participants, politiquement motivés, de monnayer leurs succès par des points échangeables contre des outils de fraude en ligne. Selon les chercheurs de Forcepoint[13], cette méthode permettrait d'attirer un nombre critique de pirates vers une cible déterminée afin d'assurer la réussite de l'opération.

Cette nouvelle pratique soulève plusieurs questions : quelles sont les intentions réelles du groupe à l'origine de cette plateforme ? Quelles sont les conséquences de l'éventuelle démocratisation de ce concept ?

Détournement des pratiques tendancielles de la sécurité informatique

La gamification et la pratique du Bug Bounty

Le concept de la gamification, aussi appelé ludification, consiste à transposer les techniques de motivation du jeu dans un domaine non ludique. Parmi ces procédés : la fixation d'objectifs et la mise en place d'un système de récompenses. A titre d'exemple, cette pratique ouvre de nouvelles perspectives dans le monde de l'entreprise (fidéliser les clients, motiver la force de vente, former les employés, récompenser les meilleurs éléments) ou celui de l'enseignement pour favoriser l'apprentissage et stimuler les performances. Le déclenchement de ce processus se matérialise par la combinaison de cinq mécanismes (système de points, de classement, de niveau, de challenge et de badges) qui permettent de stimuler et mobiliser les acteurs autour d'une cause.

Dans le secteur de la sécurité informatique, les acteurs du bug bounty[14] utilisent des techniques de gamification pour attirer, fidéliser et rémunérer pour chaque bug ou vulnérabilité détectée par les hackers éthiques participant à l'opération. L'enjeu premier est de créer un écosystème où les entreprises bénéficient d'une veille active de sécurité en ne payant que pour les vulnérabilités détectées et où la communauté des hackers éthiques est rémunérée et officiellement reconnue. Si son origine remonte à 1995 avec Netscape,

---

[13] https://www.forcepoint.com/sites/default/files/resources/files/infographic_sledgehammer_the_gamification_of_ddos_attacks_en.pdf

[14] Cette pratique consiste pour une entité à faire tester la sécurité de ses applications par la communauté des hackers éthiques.

cette pratique n'a gagné en notoriété qu'au cours des dernières années, incitant le Pentagone à lancer sa propre plateforme de bug bounty en mars 2016.

La gamification du processus constitue l'un des facteurs clé du succès de cette pratique, le bug bounty pouvant s'apparenter à un jeu pour les hackers. Comme en témoigne Yassir Kazar[15], fondateur de la plateforme de bug bounty YOGOSHA, « *La gamification peut être soft ou forte. La première consiste à mettre en place un système basique de points, de niveaux, de classement et de badge, pour motiver les participants. La gamification forte, quant à elle, consiste à retranscrire et transformer tout un processus en jeu. Les plateformes de bug bounty se caractérisent par une gamification soft dans la mesure où seuls le système de points, de classement et de badges y sont utilisés. L'une des principales motivations de ces acteurs provient en effet de l'esprit de compétition que procure cette pratique qui récompense le premier chercheur ayant trouvé une faille de sécurité*. »

La gamification des attaques DDoS

Les attaques DDoS relèvent généralement de deux types : alors que les cybercriminels les emploient à des fins d'extorsions, il s'agit au contraire pour les hacktivistes d'envoyer un message de nature politique à leur cible et au reste du monde.

Ces deux mondes, jusqu'alors distincts, sont aujourd'hui amenés à se rencontrer, avec des plateformes rémunérant des hackers en échange d'un ralliement ponctuel à une cause politique.

Ainsi, en décembre 2016, la société de sécurité informatique Forcepoint Security Lab a identifié une plateforme qui organise des attaques informatiques de type déni de service en utilisant des méthodes de gamification. Ce nouveau mode opératoire s'appuie sur un système qui permet aux hackers de mener des attaques DDoS moyennant une rémunération. Les hackers, principalement turcs, sont recrutés via des sites de piratage underground turcs. Une fois rassemblés, les recruteurs transmettent un programme à télécharger leur permettant de se connecter sur une plateforme conçue à cet effet. Cette dernière sert de lieu de rassemblement pour mener et coordonner les attaques ainsi que pour communiquer entre eux. Dénommée Surface Defense, elle comprend aussi une liste de cible, principalement des sites internet de partis politique turcs et allemands et un classement en temps réel des hackers participant aux opérations d'attaque.

Concernant les outils d'attaque, le groupe turc met à disposition des recrues son propre outil, Sledgehammer, spécialement conçu pour mener des attaques DDoS. A l'instar du célèbre LOIc, très utilisé par la nébuleuse Anonymous, ce dernier est un programme préconfiguré pour mener des attaques par déni de service contre les sites cibles. En contrepartie, les participants reçoivent un point pour chaque tranche de dix minutes d'attaque réalisée contre l'un de ces sites. Le modèle économique de cette plateforme repose sur l'échange de point gagnés contre une version déverrouillée du Sledgehammer, ainsi que des logiciels de « fraude au clic »[16].

---

[15] Entretien réalisé dans le cadre de cet article avec Yassir Kezar, fondateur de la plateforme de bug bounty Yogosha.

[16] Fraude au clic : « clics issus de pratiques frauduleuses ou malveillantes », généralement pratiquée dans le secteur de la publicité en ligne.

Ce mode opératoire, largement inspiré du concept de gamification, a permis une meilleure communication sur l'outil développé par les recruteurs et mis à disposition des participants, mais aussi de fédérer une communauté d'individus, facteur clé de réussite d'une attaque DDoS puissante et efficace.

Concept	Mécanismes	Applications aux attaques DDoS
La gratification matérielle	Les points échangeables	Les participants obtiennent 1 point pour chaque 10 minutes d'attaque
La gratification sociale	Le classement	Les résultats des participants sont publiés sur la plateforme sous forme de classement général en temps réel
La gratification morale	Aspect politique	Echo médiatique des attaques
La compétition	Les classements	Se traduit par le nombre de sites web ciblés
Le challenge	Objectifs quantifiables	Les challenges sont les sites cibles à attaquer. Ils sont fixés par le commanditaire de l'attaque

L'application du procédé de gamification aux attaques DDoS

L'opération Sledgehammer : un pont entre l'hacktivisme et la cybercriminalité ?

La rémunération de l'engagement politique des hackers

La campagne de communication menée par les recruteurs sur les sites underground turcs a été fortement teintée de politique. En effet, l'ensemble des 24 sites internet désignés comme cibles sont des sites d'organisations politiques[17]. Cette liste comprend des sites kurdes telles que celui du Parti des travailleurs du Kurdistan (PKK) ou de la Force de défense populaire (HPG), les sites Web des groupes de hackers kurdes, les stations de radio et de télévision kurdes, le site du Parti démocrate-chrétien allemand, un site web traitant la question du génocide arménien ou encore plusieurs sites web israéliens[18]. Le nom de cette opération « Sledgehammer » fait d'ailleurs référence au supposé coup d'état turc de 2003[19].

En règle générale, seule la motivation politique anime les activistes menant ce type d'opération ciblée. Dans ce cas de figure, il s'agit en réalité de combiner deux éléments : le nationalisme turc et la rémunération,

[17] https://www.bleepingcomputer.com/news/security/turkish-hackers-are-playing-a-ddos-for-points-game/

[18] https://www.bleepingcomputer.com/news/security/turkish-hackers-are-playing-a-ddos-for-points-game/

[19] https://intelnews.org/2015/04/07/01-1673/

spécificité des cybercriminels. L'argument politique, utilisé comme outil marketing pour recruter de nouveaux pirates, se révèle ainsi très efficace pour élargir la base des participants :

- En convaincant les pirates pour lesquels l'une ou l'autre des motivations prises individuellement (argent ou cause politique) étaient insuffisantes pour sauter le pas ;
- En payant à moindre coût des pirates mercenaires, dont la faible rémunération se trouve compensée par un aspect ludique et par l'intégration de l'individu au sein d'un combat politique susceptible de le valoriser et de donner un sens à son action ;
- En entretenant l'esprit de compétition des uns et des autres par la mise en place d'un système de classement en temps réel.

Cette rémunération de l'hacktivisme a dès lors permis de fédérer rapidement une cybercommunauté nationaliste et de mener efficacement une opération ciblée. Pour qu'une attaque DDoS soit efficace, il faut en effet réunir un nombre critique de machines participantes. Plus ce nombre de machines est important, plus l'amplitude de l'attaque sera grande et sa distribution géographique potentiellement diversifiée, et plus il sera complexe pour les cibles de s'en prémunir.

Dans une vidéo publiée en décembre 2016[20], l'expert italien Luca Mairani, ingénieur chez ForcePoint souligne que la récente gamification des attaques DDoS présente des similitudes avec le projet Chanology, série d'attaques menées en janvier 2008 par le collectif des Anonymous contre l'Église de scientologie. Les deux opérations se différencient toutefois à travers le mode de rémunération des participants. Comme l'explique Vincent Lavergne, spécialiste des attaques DDoS chez F5 Networks : « *Pour composer son réseau de machines sources, plusieurs techniques sont utilisées par les Hackers. Anonymous a longtemps fonctionné sur un modèle de participation volontaire[21], en se basant sur la motivation "politique" / activiste et donc non rémunérée, au contraire de l'alternative qui consiste à créer un botnet au travers de l'infection d'un grand nombre de machines à l'insu de leur propriétaire. Ici, le groupe de pirates turcs vise un enrôlement volontaire des participants - invitation sur des forums - et les rétribue avec une sorte de programme de fidélité pour hackers. Le cybercrime étant devenu un business à la demande, il n'est pas étonnant que les hackers s'organisent et commencent à partager les gains de ce service lucratif tout en recrutant de nouveaux hackers.* »

L'outil mis à disposition des participants contenait une porte dérobée

Ce mode opératoire a permis aux recruteurs d'attirer plusieurs pirates vers leur plateforme Surface Defense et ainsi de mieux communiquer autour de leur outil d'attaque. Dans le rapport publié par la société Forcepoint, l'analyse de l'outil de DDoS mis à disposition des participants a également permis de découvrir la présence d'une porte dérobée permettant ainsi aux concepteurs d'avoir un accès à l'ensemble des machines ayant participé au jeu d'attaques. Une découverte qui soulève des doutes quant aux véritables motivations des recruteurs turcs, qui semblent beaucoup moins évidentes à la lumière de ce nouvel élément. Sont-ils réellement fidèles à la cause qu'ils prétendent défendre ? Cherchent-ils au contraire à identifier et à surveiller ses sympathisants ? Ont-ils seulement pêché par cupidité, en souhaitant, au-delà de la campagne, s'enrichir des outils de leurs recrues ? Ou était-ce justement l'objectif ?

---

[20] https://www.youtube.com/watch?v=sNUQyT_z9xU

[21] « Opt in botnets »

Conclusion

Au-delà de la question de la motivation qui a présidé à la mise en place de cette plateforme, se pose la question des conséquences d'un tel concept s'il se diffusait.

Le premier impact serait l'augmentation conséquente des capacités offensives des groupements hacktivistes, qui bénéficieraient en outre d'un bassin de compétences beaucoup plus large. De telles plateformes constitueraient en effet des outils de mobilisation précieux à destination de pirates d'abord attirés par la rémunération.

La démocratisation de cette pratique pourrait ainsi augmenter les impacts des attaques visant les cibles usuelles des activistes, parmi lesquelles figurent notamment les sociétés privées. Avec des conséquences financières significatives : coût d'interruption d'un service générateur de revenus, pénalités sur les SLA (l'engagement de niveau de service), perte d'image, perte de clientèle, etc.

Enfin, ce phénomène pourrait être employé par des acteurs, notamment étatiques, afin d'agir en évitant d'exposer ses cyber-forces régulières. A l'inverse, il pourrait aussi s'agir pour une agence de renseignement de piéger, grâce à cet outil, ses adversaires, qui plus en est en désignant des cibles factices ou de faible intérêt réel.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com