Lettre n°64 - Juillet 2017 - disponible sur omc.ceis.eu

Brève du mois

« ***La liberté de circulation des données est une condition nécessaire du marché unique numérique. (…) Nous devons améliorer la confiance et la sécurité. C'est pourquoi il faut nous concentrer également sur des questions de cybersécurité*** »[1] - Juri Ratas, premier ministre estonien. La présidence estonniene de l'Union Européenne, qui a débutée le 1er juillet, est notamment attendue dans le domaine de la cybersécurité .

TABLE DES MATIERES

[1] http://www.la-croix.com/Monde/Europe/LEstonie-joker-tete-lUnion-europeenne-2017-07-02-1200859753

FONDS D'INVESTISSEMENT ET CYBERSÉCURITÉ : QUELLES SONT LES TENDANCES ?

En bourse, le climat s'avère favorable pour la cybersécurité. Aux évolutions règlementaires (directive NIS, règlement européen sur les données personnelles…) s'ajoutent les cyberattaques récentes. Avec le *ransomware* WannaCry, la valeur de Wallix Group, seul acteur spécialisé dans la sécurité informatique côté à la Bourse de Paris, est par exemple passée de 13,09 € le 12 mai à 15,79 € le 15 mai (week-end de l'attaque).

Le secteur de la sécurité informatique a en outre connu des records d'investissement au premier trimestre 2017 (+20% par rapport au précédent) et bénéficie d'une prise de conscience de la part des États, des entreprises et des individus. Déjà marqué par de nombreuses opérations de fusions-acquisitions (dont l'acquisition de LightCyber par Palo Alto Networks en mars), le marché global de la cybersécurité pourrait ainsi atteindre 120 milliards de dollars cette année selon le cabinet Gartner. Une tendance qui devrait être renforcée par l'engouement pour les firmes de l'AssurTech aux États-Unis, la montée en puissance du *Big Data* ou de l'Internet des objets (*IoT*). Le marché européen reste néanmoins bien en-deçà de son voisin outre-Atlantique, avec 10% seulement des investissements des fonds de capital-risque en 2015 et 2016[2].

Quels sont les types d'investissement privilégiés ? Quels sont les domaines bénéficiant des plus importantes levées de fonds ? L'Europe parviendra-t-elle à rattraper son retard sur les États-Unis ?

Réalités américaines vs. Ambitions européennes

Au 25 mai 2016, 4 des 5 plus grandes levées de fonds en cours en matière de cybersécurité concernaient des investisseurs américains. L'année précédente, 4 fonds européens se disputaient 300 millions de dollars quand 20 concurrents outre-Atlantique collectaient 8,1 milliards de dollars[3]. Du reste, en 2015, l'américain Paladin Capital Group créait un fonds cyber (actuellement actif) centré sur la résilience des infrastructures numériques et s'associait, en avril 2017[4], au Fonds européen d'investissement (FEI) et au Luxembourg Future Fund afin de gérer un nouveau fonds cyber européen basé au Luxembourg.

Ce rapide panorama reflète la position dominante des États-Unis sur le secteur, au même titre que ses ambitions financières avec le NASDAQ, marché d'actions américain le plus important après le New-York Stock Exchange[5]. Accel Partners, Kleiner Perkins Caufield & Byers et Sequoia Capital, les 3 fonds d'investissement américains incontournables en 2017 selon *Leaders League*, figurent ainsi dans la catégorie des « investisseurs les plus actifs en capital-risque » dans le « tableau périodique de la cybersécurité »[6]

[2] Rapport Citi (janvier 2017) : « *Digital Disruption – Revisited: What FinTech VC Investments Tell Us About A Changing Industry* »

[3] https://www.lesechos.fr/13/06/2016/LesEchos/22211-125-ECH_investissements-dans-la-cybersecurite---l-europe-distancee-par-les-etats-unis.htm

[4] http://www.paladincapgroup.com/joins-with-eif-lff-to-invest-in-eu-based-cyber-security-firms/

[5] En volume traité

[6] https://www.cbinsights.com/blog/periodic-table-cybersecurity-startups/

élaborée par *CB Insights*. Quant aux spécialistes, on retrouve notamment Francisco Partners, Bessemer Venture Partners et Institutional Venture Partners.

Autre projet : celui de Techstars, accélérateur américain ayant accompagné plus de 1 000 start-up pour un montant de 3 milliards d'euros. Il s'est allié avec Partech Ventures afin de créer un « city program » à Paris qui bénéficiera de l'appui de partenaires de référence tels que Total, Air Liquide ou Renault. 10 start-up, françaises comme étrangères, intègreront chaque année un programme de 13 semaines – dont le premier démarrera en septembre – et bénéficieront d'un financement de 120 000 $ (Techstars prendra une participation à hauteur de 6% pour chaque start-up).

L'engouement affiché par Washington pour la conquête du marché permet aussi à l'Hexagone de surfer sur une vague d'attractivité, la France étant « *the next big thing* » pour le PDG de Cisco. Parallèlement, les fonds nationaux entendent eux-aussi tirer profit de cette conjoncture favorable et s'intéressent davantage au marché de la cybersécurité. A commencer par ACE Management, spécialisé sur les opérations *small* et *mid-cap*, qui a entamé en 2009 sa 4ème génération de capital-investissement et compte de solides investisseurs industriels, financiers et institutionnels. Du côté des fonds de capital-risque, on retrouve notamment CapHorn Invest[7] qui se veut « Digital & Connecté » et investit pour des tickets compris entre 0,5 et 4 millions d'euros (séries A et B) et Auriga Partners, spécialisé dans les investissements software (amorçage, 1er tour, capital-développement).

La balance tend ainsi à s'équilibrer. A l'échelle de l'Union européenne comme de ses États membres, les initiatives fleurissent, principalement sur des usages finaux exigeant un haut niveau de sécurité comme dans le monde bancaire. En témoigne le lancement du hub européen FinTech Go par Euratechnologies et le Crédit Agricole. L'Intelligence Artificielle, la *blockchain* et la cybersécurité y sont à l'honneur à travers un premier programme d'accélération concernant les jeunes pousses de moins de 3 ans et un second pour des porteurs de projet n'ayant pas encore de produit fini.

Les institutions européennes ont également saisi la mesure des opportunités qu'offre la FinTech pour les services financiers, amenant le vice-président de la Commission européenne chargé de la stabilité financière, des services financiers et de l'Union des marchés de capitaux, à présenter les technologies financières comme ayant « la capacité de faire évoluer positivement le secteur financier et la manière d'accéder aux services financiers »[8] pour les consommateurs. Une partie du Fonds européen de la défense[9] sera par ailleurs consacrée à la recherche sur les produits et technologies de défense, dont des projets de logiciels de chiffrement ou portant sur la robotique.

En outre, dans le contexte règlementaire actuel (directive NIS et GDPR qui entreront en vigueur en 2018), l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) souhaite renforcer sa capacité d'action sous le nouveau mandat juridique que le vice-président de la Commission européenne chargé du Marché unique numérique présentera en septembre. Cette volonté devant se traduire par une

[7] InterCloud et Vekia (Big Data) font notamment partie de son portefeuille

[8] http://www.fusacq.com/buzz/la-reglementation-europeenne-est-elle-adaptee-aux-fintech-a135748.html?from=blog

[9] http://europa.eu/rapid/press-release_IP-17-1508_fr.htm

hausse de son budget ainsi que le renforcement du partenariat public-privé de 450 millions d'euros lancé par la Commission en 2016 et qui a déjà attiré près de 2 milliards d'euros d'investissements à ce jour[10].

Capital-risque américain vs. Capital-investissement européen

Si les investisseurs européens et américains sont de plus en plus nombreux à parier sur les sociétés de cybersécurité, leurs comportements diffèrent quant au type d'investissement privilégié. L'Europe tend à privilégier davantage le capital-investissement, via le financement de sociétés déjà avancées, là où les États-Unis se concentrent sur le capital-risque à destination d'entreprises en phase de démarrage. Plusieurs raisons expliquent cette tendance.

Most Active VCs Investing In Cybersecurity 2013 – 2017 YTD (5/15/17)

Rank	Investor	Select Investments
1	New Enterprise Associates	Cyence, illusive networks, HackerOne
1	Bessemer Venture Partners	Virtru, PhsihMe, Autho
3	Accel Partners	SentinelOne, Illumio, CrowdStrike
4	Andreessen Horowitz	Tanium, Illumio, Okta
5	Intel Capital	CoreOS, HyTrust, Vectra Networks
5	Lightspeed Venture Partners	Bromium, Zscaler, Netskope
5	Norwest Venture Partners	Exabeam, Shape Security, Palerra
8	Google Ventures	Anomali, Synack, SecurityScorecard
8	Kleiner Perkins Caufield & Byers	Shape Security, Area 1 Security, Synack
8	Paladin Capital Group	Anomali, Endgame, PhishMe

CB INSIGHTS

Figure 1 : transactions de capital-risque entre 2014 et 2017 (tous les investisseurs sont américains), *CB Insights*

D'une part, l'élection de Donald Trump est venue renforcer l'attention particulière que les États-Unis portent à la prise en compte du facteur risque, ce qui se traduit par un nombre croissant de transactions « *early stage* » (amorçage – série A). D'autre part, les brevets tendent à rassurer les investisseurs européens, estimant que la valeur d'une entreprise peut résider dans ces derniers.

En privilégiant ce type d'investissement, l'Europe a pendant longtemps pris le risque de voir ses jeunes talents tenter leur chance outre-Atlantique. Parallèlement, les entreprises précoces ont toujours été conscientes de l'inégalité des montants en jeu pour financer leur développement. L'Europe semble pourtant vouloir remédier à cette situation pour conserver ses talents et en attirer de nouveaux depuis l'étranger. Elle cherche pour cela à se doter du capital nécessaire. Les investissements dans la Tech sont représentatifs de ce dynamisme. En première ligne : les Britanniques, qui se présentent en chef de file, et excellent dans les FinTech ou l'Intelligence Artificielle. Sur le 4ème trimestre de 2016, le Royaume-Uni a comptabilisé près de 3,6 milliards d'euros de financements dans la Tech quand la France et l'Allemagne se sont partagées respectivement 652 millions d'euros et 1 milliard d'euros[11]. La France entre pourtant bel et bien dans une

[10] http://www.euractiv.fr/section/economie/interview/eu-cybersecurity-agency-seeks-remit-funds-to-police-attacks/

[11] https://www.cbinsights.com/research-french-tech

phase de maturité et séduit tant par ses initiatives (Station F[12], French Tech) que ses start-up innovantes (DataDome, solution contre les *bad bots* ayant récemment levé 1 million d'euros). Le quartier de la Défense pourrait par ailleurs prendre un avantage sur la City si l'on considère l'impact du Brexit comme un facteur déterminant d'un point de vue financier.

La réflexion ne peut cependant se cantonner à l'Hexagone et doit être européenne. Si Paris et Londres entendent être compétitives et attirer les start-up, elles ont aussi compris qu'elles devaient viser tant le national que le régional. Deux fonds français ont placé l'Europe au cœur de leurs actions. Idinvest Partners a financé plus de 130 start-up dans les domaines du digital, de la santé et des Smart Cities depuis 10 ans. Le 15 mai dernier, Omnes Capital a lancé la commercialisation d'un nouveau Fonds Commun de Placement dans l'Innovation (FCPI) dont 80% des actifs seront constitués de PME françaises et européennes. Autre exemple, la levée de fonds en janvier 2016 de 500 K€ finalisée par Difenso[13] auprès d'investisseurs tels que Nestadio Capital (suivi d'un second tour de table de 2 millions d'euros en juin 2017). L'opérateur européen de sécurisation des données dans le Cloud vise ainsi les marchés français et européen. Quant à Pictet Asset Management (Suisse), il revendique un avantage concurrentiel sur la région. Son fonds Pictet-Security[14] a été lancé fin octobre 2006 et a atteint 1,8 milliards d'euros d'encours à la fin de l'année dernière.

En outre, les investissements des fonds de capital-risque ont été multipliés par 5 depuis 2011 pour atteindre 13 milliards de dollars l'année dernière. En témoigne le lancement le 21 juin dernier d'un fonds dédié aux entreprises de l'économie numérique par Iris Capital, « investisseur en capital risque pan-européen »[15], dont une attention particulière sera portée à l'Internet des objets (IoT), l'Intelligence Artificielle ou encore le Big Data. Plus spécifiquement, dans le secteur de la FinTech, 50 *deals* ont été réalisés au premier trimestre 2017 pour 195 millions d'euros, soit quasiment l'équivalent en montant des deux premiers trimestres 2016 réunis (193 millions d'euros sur 65 *deals*[16]). Comptabilisant 2.3 milliards de dollars, Balderton Capital est à ce jour le plus important fonds britannique de capital-risque axé sur la technologie en Europe. La France semble également vouloir investir davantage à tous les niveaux, de l'amorçage à l'*exit*[17].

---

[12] 1 000 start-up devraient rejoindre début juillet Station F, plus grand campus de start-up au monde et symbole de l'ambition de la France de devenir la capitale européenne pour ces dernières

[13] Solution devant être certifiée dans chacun des pays d'Europe, elle est déjà le 1er Cloud Access Security Broker (CASB) à obtenir la Certification de Sécurité de Premier Niveau (CSPN) de l'ANSSI

[14] Les États-Unis concentrent 66.45% du fonds. L'Europe, Israël et le Japon se partagent le reste

[15] http://www.iriscapital.com/fr/content/iris-capital-lance-son-nouveau-fonds-multi-corporate-irisnext-avec-un-premier-closing-%C3%A0-250m

[16] https://www.cbinsights.com/blog/europe-fintech-funding/

[17] Le bilan annuel d'EY précise que les investissements de capital-risque ont augmenté de 22% en France en 2016. L'Hexagone atteint 20% des montants levés en Europe et se place devant l'Allemagne mais derrière la Grande-Bretagne

Les secteurs privilégiés

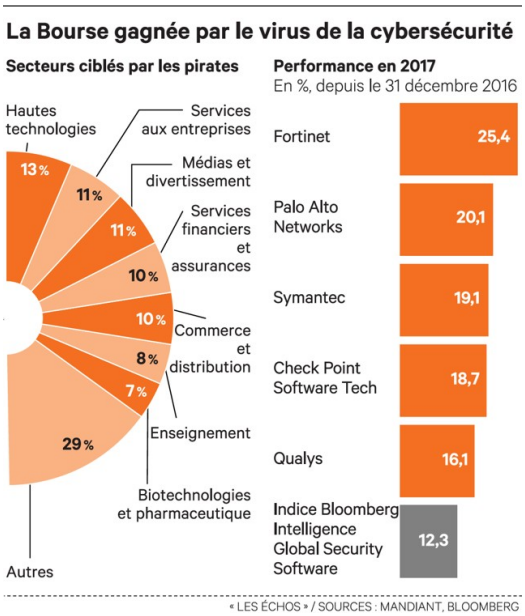

Figure 2 : sources *Les Echos / Mandiant, Bloomberg*

Une typologie des investissements met en lumière deux catégories de sociétés :

- Les entreprises ou grands groupes, pour lesquels les investissements sont moins risqués, mais dont la cybersécurité n'est bien souvent qu'une partie de leurs activités. En témoignent les performances en 2017 d'acteurs comme Fortinet ou Symantec ;
- Les sociétés plus petites, la plupart du temps spécialisées sur un secteur, et bénéficiant d'un intérêt croissant de la part des investisseurs. Les investissements y sont néanmoins plus risqués mais peuvent entraîner des potentiels de croissance non négligeables. Le bond de 14% de la valeur de Wallix Group souligné en introduction en est l'exemple.

Ces deux catégories entendent répondre à la demande grandissante de nombreux secteurs en matière de cybersécurité.

Premier secteur : celui des **services financiers et assurances**, autrement dit **AssurTech et FinTech**. Parmi les principales banques européennes investissant dans ce dernier, on retrouve Santander, UBS, Deutsche Bank, la Société Générale, BNP Paribas, le Crédit Suisse ou encore HSBC sur des problématiques liées entre autres aux logiciels, aux paiements ou à la *blockchain*.

Côté français, après le Crédit Mutuel Arkéa (investissement risque – 1er tour de 2 millions d'euros de fonds propres le 21 février afin de rejoindre le capital de JiVai) ou encore le groupe BPCE, c'est au tour du Crédit Agricole d'accélérer ses investissements, principalement à destination des jeunes pousses. Deux fonds de 50 millions d'euros ont été créés parallèlement[18] : un premier dédié à la FinTech[19] et un second plus général

[18] http://www.agefi.fr/fintech/actualites/quotidien/20170328/credit-agricole-confie-fonds-fintech-a-breega-214811

de capital-innovation. Autre levée, celle de Truffle Capital qui a annoncé le 20 mai le lancement d'un fonds de 150 millions d'euros. 12 à 15 sociétés devraient se répartir le portefeuille d'ici 5 ans pour un investissement de 10 ans, avec des tickets allant de 5 à 20 millions d'euros. *L'Agefi* précise que « certaines sociétés visées par le fonds pourront intégrer l'incubateur lancé par Truffle Capital en juin 2015 »[20].

Second secteur : celui des **hautes technologies**, marqué par de solides *deals* dans les **technologies de l'information** et par un intérêt croissant pour la **robotique et l'automatisation**.

Dans le premier secteur, on peut notamment citer le rachat progressif du capital de Gfi Informatique par le qatari Manni Corporation, dont la dernière opération de cession a eu lieu le 12 mai dernier et visera un premier bloc de 155 millions d'euros cet été, suivi d'un second de 85 millions d'euros au second semestre 2018. Autre exemple, l'acquisition (à 100%) le 5 avril de vCloud Air, l'activité cloud de l'américain VMWare, par la société roubaisienne OVH, qui illustre la maturité de certaines sociétés françaises et leur capacité à cibler le marché américain.

Dans le second domaine, l'indice Indxx Global Robotics & Artificial Intelligence Thematic a enregistré une augmentation significative de 24,6% en 2017. Deux facteurs permettent d'expliquer ce phénomène. D'une part, la robotique attire les investisseurs conscients de la rapidité des progrès du secteur. D'autre part, l'engouement pour l'Intelligence Artificielle et les avancées qui en découlent sont venus renforcer les capacités de cette technologie toujours plus innovante. Cela s'est traduit par de nombreuses opérations de fusions-acquisitions. En mai 2017, Microsoft a ainsi acquis la solution automatisée de réponse à incidents de Hexadite.

Troisième secteur : **l'aéronautique et la défense.** Le 2 mai 2017, Bpifrance et la Direction générale de l'armement (DGA) ont signé un accord instituant un fonds d'investissement initial de 50 millions d'euros pour les entreprises jugées stratégiques pour le secteur de la défense. Une initiative qui n'est pas sans rappeler le fonds In-Q-Tel de la CIA destiné à l'investissement dans des start-up développant des technologies duales en matière de renseignement et revendiquant plus de 1 500 relations de co-investissement depuis sa création en 1999.

A l'image d'In-Q-Tel, le Mossad vient de lancer son fonds intitulé Libertad[21] pour des projets de R&D lui fournissant des solutions technologiques. La robotique, l'énergie et le chiffrement font notamment partie des domaines prioritaires retenus pour le premier appel à propositions en 2017.

Quant au secteur aéronautique mondial, sa croissance continue s'accompagne aujourd'hui d'une prise de conscience de la vulnérabilité du transport aérien en matière de cybersécurité. Comme le précise le rapport

[19] Si le Crédit Agricole a annoncé mi-mars assurer la partie expertise financière, la gestion sera quant à elle confiée à Breega Capital, société de capital-risque, notamment actionnaire de Nanocloud

[20] http://www.agefi.fr/fintech/actualites/quotidien/20170321/truffle-capital-profite-l-essor-fintechs-attirer-214067

[21] http://www.libertad.gov.il/eng/index.html

Deloitte[22] présenté à la presse le 9 mars dernier, les cyberattaques pourraient constituer une menace significative. Piratage d'un système de contrôle d'un avion, menace de la sécurité des vols, espionnage des bases aériennes…, autant de risques potentiels pris en considération par l'écosystème français. Calao Finance suit ainsi activement les secteurs sous-marin (robotique) et maritime tout comme ACE Management qui s'est spécialisé dans l'aéronautique (fonds Aerofund I en 2004, Aerofund II en 2008 et Aerofund III en 2013), le maritime (fonds ATALAYA en 2010), la défense et la sécurité (la levée du fonds Brienne III dédié à la sécurité du numérique est en cours de finalisation). Via son fonds Aerofund III, ACE Management est entré en mars 2016 au capital du groupe WeAre Aerospace. Ces deux derniers ont ensuite rejoint en septembre 2016 le capital de 3D Trust, start-up de sécurisation des données relatives aux impressions 3D, à travers une levée de fonds d'1 million d'euros, à laquelle s'ajoute un prêt d'amorçage de Bpifrance.

Plus généralement, les **biens et services industriels** représentent un domaine cible pour les levées de fonds en matière de cybersécurité, notamment à destination des infrastructures critiques. Le 27 janvier 2016, ACE Management et Rhône-Alpes Création[23] investissaient équitablement à hauteur de 2 millions d'euros (risque – 1er tour) sur la solution de sécurisation des réseaux industriels de Sentryo.

Dernier secteur : la **santé**, dont la protection des données est devenue un véritable enjeu à l'heure de l'attaque WannaCry qui a paralysé le National Health Service britannique. Plusieurs start-up ont développé des solutions innovantes allant dans ce sens. C'est notamment le cas de ClearDATA, fournisseur de cloud pour les soins de santé, qui a pu bénéficier d'investisseurs tels qu'Excel Venture Management, et de Health Linkages, utilisant les technologies blockchain et Big Data à destination des établissements de santé et soutenu par le programme IndieBio du fonds de capital-risque SOSVentures.

[22] « *Les grandes tendances 2017 de l'industrie aéronautique et défense* » : https://www2.deloitte.com/fr/fr/pages/manufacturing/articles/grandes-tendances-2017-industrie-aeronautique-defense.html

[23] Le rapprochement de Rhône-Alpes Création et de Banexi Ventures Partners a donné naissance en 2016 à Kreaxi, spécialiste français du capital-risque

HONEYPOTS ET *SINKHOLES*, OUTILS DE DEFENSE ACTIVE

Parmi les mesures défensives à disposition des équipes responsables de la sécurité d'un système d'information, figurent les outils de défense active que sont les *honeypots* et les *sinkholes*. Par leurre ou par détournement transparent de flux réseau, ces outils permettent de ralentir et d'étudier l'attaque de l'adversaire de façon à pouvoir anticiper et contrer les menaces futures.

Dans quelle mesure les *honeypots* et les *sinkholes* sont-ils des outils efficaces face à la recrudescence des attaques informatiques ?

Principes de fonctionnement

Les *honeypots* et *sinkholes* sont des mécanismes de sécurité informatique mis en place pour détecter, observer, voire contrecarrer des tentatives d'intrusions non-autorisées au sein d'un système.

Honeypots

Un *honeypot* est une méthode de défense active qui consiste à attirer, sur des ressources identifiées et prévues à cet effet (serveur, programme ou service) des attaquants, déclarés ou potentiels, de manière à les identifier pour neutraliser, par la ruse en collectant des informations sur leurs méthodes et comportements, les futures attaques sur le réseau de l'entité considérée. Un *honeypot* pourra prendra la forme d'une ou plusieurs[24] machines virtuelles plus ou moins isolées du reste du réseau de l'entreprise. Cette fonction, zone ou base est en fait isolée de toutes données d'importance et sous surveillance permanente, et contiendra des informations ou des ressources de grande valeur apparente pour un attaquant mais mineures pour les intérêts de l'entreprise, voire simplement factices.

On peut distinguer deux types de *honeypots* :

- Les *honeypots* de production : principalement utilisés par les entreprises, ils ont une capacité d'interaction limitée. Leur objectif n'est pas tant de récupérer un maximum d'information sur l'attaquant (mode opératoire, données techniques, etc.) que de repérer les attaques, afin de pouvoir gagner un précieux temps de réaction avant que l'attaquant ne réalise le subterfuge et ne s'attaque aux cibles réelles. Un pirate s'intéresse généralement au *honeypot* en premier lieu car il semble être une cible plus facile d'accès et/ou de plus grande valeur ;
- Les *honeypots* « de recherche » : plus complexes, et donc plus coûteux à paramétrer/opérer, ils visent à obtenir un maximum d'information sur l'attaquant. Ces informations pourront être mises à profit pour protéger, de façon plus ou moins proactive, le reste du système d'information. Ces mesures proactives peuvent notamment inclure des *sinkholes*.

[24] Plusieurs *honeypots* forment un *honeynet* (réseau de *honeypots*).

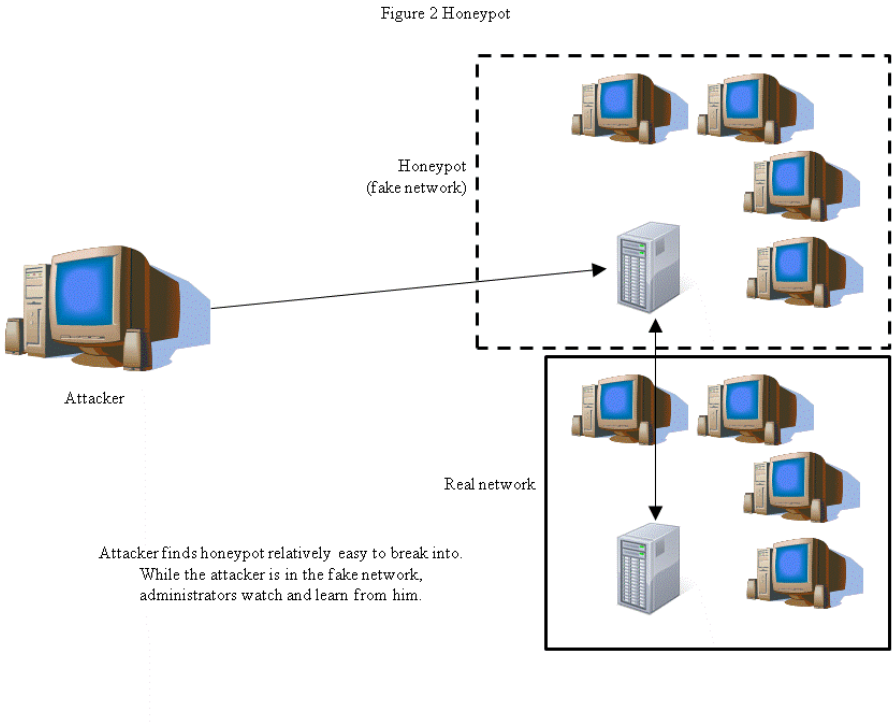

Figure 3 : schéma simplifié du principe d'un honeypot (Source : Washington University)

Les *honeypots* permettent donc :

- De ralentir les attaquants, en leur offrant des cibles d'intérêt réel faible ou inexistant[25] ;
- D'être alerté de tentatives d'intrusion en amont des intrusions des machines d'intérêt réel, ce qui offre un temps de préparation à la défense ;
- D'obtenir des informations nécessaires au déploiement de contre-mesures : failles exploitées, malware employés, mode opératoire, noms de domaines et/ou IP des machines utilisées par les attaquants, etc.

En contrepartie :

- Leur gestion peut s'avérer plus ou moins difficile. Ceci dépend surtout du niveau d'interaction souhaitée (et donc de l'objectif visé) ;
- Ils peuvent être source de vulnérabilité. Un mauvais confinement des *honeypots* et un défaut de surveillance peuvent être dangereux.

[25] A ce titre, on peut imaginer toute sorte d'*honeypots*. L'équipe digitale de la campagne En Marche aurait par exemple procédé à la création de faux comptes emails hébergeant de fausses informations de façon à ralentir les pirates (avec le piratage des dits comptes, mais surtout avec la lecture de faux documents).
https://arstechnica.co.uk/information-technology/2017/05/emmanuel-macron-russian-hacking-defence

Sinkholes

Un *sinkhole* ou littéralement « puisard » correspond à un détournement de trafic au sein d'un réseau, volontairement paramétré par son ou ses administrateurs. Il s'agira le plus souvent de détourner le trafic issu de machines infectées à destination d'un serveur malveillant (le serveur de *Command & Control*), de telle sorte à analyser et/ou détruire les flux de données considérés. La méthode de détournement repose généralement sur la personnalisation de tables *DNS* (non utilisation des tables standard). On parle alors de *DNS sinkholing.*

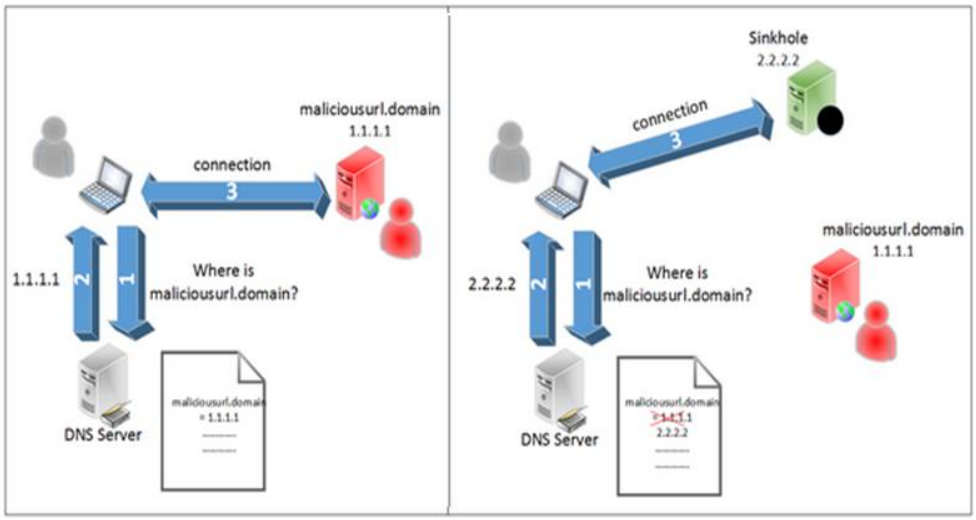

Figure 4 : schéma simplifié du principe d'un *sinkhole* paramétré par serveur DNS local (source : SANS Institute)

Le *DNS Sinkholing*, mis en œuvre par les FAI[26], les hébergeurs, les sociétés de sécurité informatique et les entreprises sur leur propre réseau, permet donc :

- D'identifier les machines compromises qui chercheraient à contacter les domaines malicieux redirigés[27] ;
- D'analyser le trafic malicieux afin d'obtenir des informations sur les attaquants et sur le fonctionnement du malware employé. Il s'agit également de déterminer la portée de l'attaque. Le trafic peut d'ailleurs être redirigé vers le serveur de destination initial, afin de ne pas éveiller les soupçons des attaquants ;
- De soustraire les machines infectées du contrôle des attaquants. En détournant le trafic, le *botnet*[28] perd de sa « puissance » en passant sous le contrôle des administrateurs à l'origine de sa mise en œuvre. A ce titre, on relève deux principales méthodes :

[26] Fournisseur d'accès à Internet.

[27] https://www.paloaltonetworks.com/documentation/60/pan-os/newfeaturesguide/content-inspection-features/dns-sinkholing

[28] Un botnet est un réseau de bots automatiques. Ces bots sont généralement des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour exécuter certaines tâches (envoi de spam, de virus informatiques voire pour mener des attaques par déni de service).

- Le *blackholing*[29] : le trafic est détruit ;
- La prise de contrôle de tout ou partie du réseau de machines infectées, via la mise en place d'un serveur de substitution au serveur *C&C* malicieux.

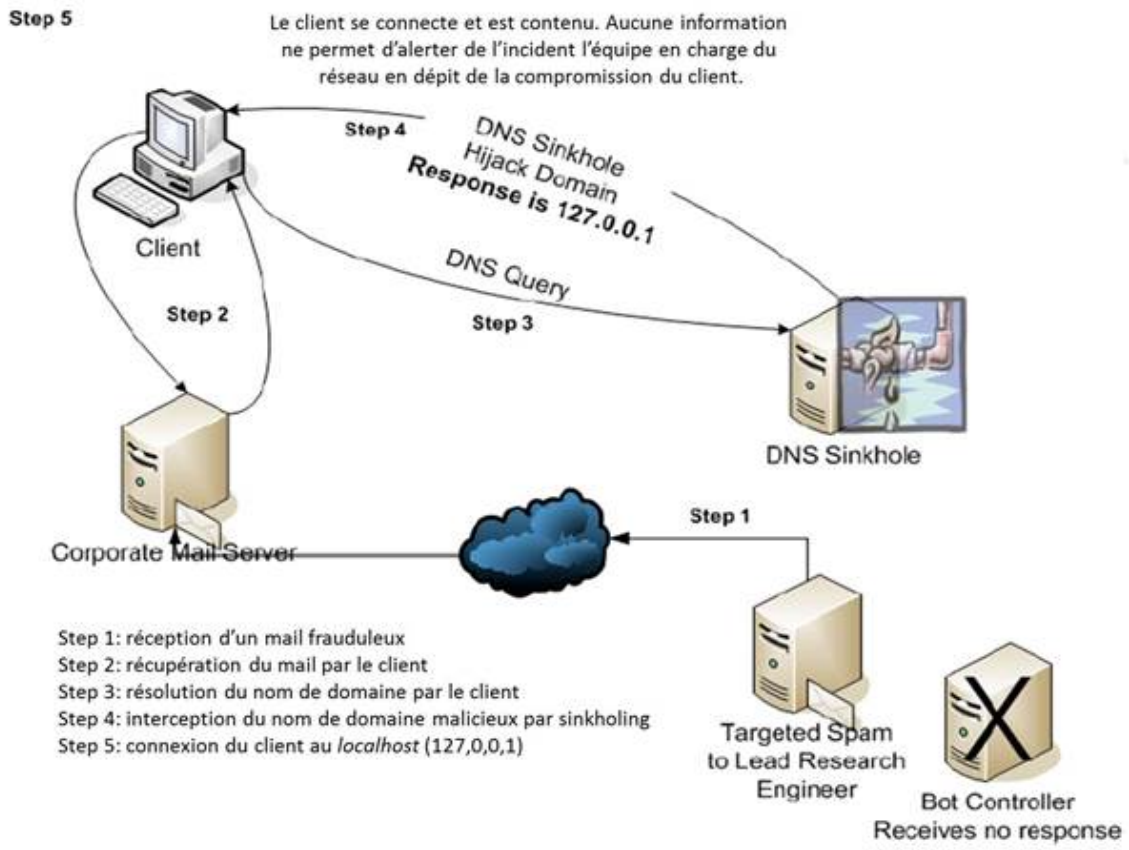

Figure 5 : schéma simplifié du principe du *DNS Sinkholing* aboutissant à un effet *blackhole* (destruction du flux sortant par modification locale du DNS du domaine malicieux (Source : SANS Institute)

Certaines entreprises (notamment les FAI et surtout celles œuvrant dans le domaine de la lutte contre la cybercriminalité) utilisent le principe du *DNS sinkholing* pour réaliser des statistiques, mais également pour démanteler des *botnets* en substituant leur propre serveur de *Command & Control* à celui des cybercriminels.

Même si l'on observe dans la pratique une certaine tolérance vis-à-vis de cette pratique[30], ce détournement de domaines compromis sur Internet peut cependant soulever des difficultés juridiques dans certaines juridictions. En raison de leurs conséquences directes, *honeypot* et *sinkholes* sont donc généralement mis en œuvre dans des conditions spécifiques par des tiers de confiance.

[29] https://en.wikipedia.org/wiki/Denial-of-service_attack#Blackholing_and_sinkholing

[30] Par exemple, lorsque ces technologies sont considérées comme une détection d'intrusion avancée (détection de comportement anormal).

Les problématiques juridiques

La protection des données à caractère personnel

Le recueil de données par déploiement de *honeypot* et de *sinkhole* peut être sanctionné en cas de non-respect des formalités préalables (article 226-16 du code pénal) : information, demande d'autorisation, mais également mise en œuvre de mesures de sécurité afin de protéger les informations collectées et analysées. En effet, les données recueillies peuvent comprendre des données à caractère personnel qui doivent être protégées, y compris celles appartenant à l'attaquant.

L'infraction à un système automatisé de données

Il peut être tentant d'adjoindre aux capacités de cyberdéfense offertes par le *honeypot* ou le *sinkhole* des mesures pouvant être qualifiées de délit d'introduction frauduleuse dans un système automatisé de données. En effet, l'infraction pourra être caractérisée si l'utilisation d'un *sinkhole* visant à prendre le contrôle du réseau de machines infectées ou à détruire du trafic a un impact sur des tiers (impact souvent involontaire). Il en va de même lorsqu'un *honeypot* dispose de la capacité d'analyse de port permettant un accès à distance à une machine. En ce sens, le *honeypot* et le *sinkhole* peuvent constituer des outils de « *hack back* ». Or, cette pratique est aujourd'hui illégale.

Responsabilité civile en cas de victime de dommage collatéral

Une mauvaise utilisation du *honeypot* ou du *sinkhole* peut avoir des conséquences dommageables pouvant engager la responsabilité du responsable de l'outil selon les règles de droit commun de la responsabilité civile (article 1382 du code civil). Ainsi, une responsabilité juridique pourrait être engagée du fait d'une attaque par rebond dans le cas d'une négligence dans l'utilisation d'un *honeypot*. Ce dernier pourrait, en effet, servir à lancer une attaque contre des tiers. S'agissant du *sinkhole*, un paramétrage insuffisamment précis de la redirection du trafic pourrait également avoir un impact sur des tiers et entrainer des dommages collatéraux.

La provocation à la commission d'une infraction : le cas du *Honeypot*

Le *honeypot* fait l'objet d'une problématique juridique particulière relative à l'admissibilité des preuves recueillies par l'outil. La question s'est posée de savoir si un tel outil ne constituait pas une provocation à la commission d'une infraction. Il semble cependant que le *honeypot* ne constitue pas une telle provocation lorsqu'il a pour objet uniquement de rassembler des preuves de la commission d'une infraction et d'en identifier les auteurs (Cass crim, 30 avril 2014, n° 13-88162). En revanche, lorsqu'il met à disposition des cybercriminels des moyens de commettre une infraction en vue de les arrêter, le dispositif pourrait être qualifié de provocation à la commission d'une infraction (Cass crim 4 juin 2008, n° 08-81045).

Les responsables de *honeypots* ou *sinkholes* s'exposent enfin à un risque assurantiel. Une utilisation illégale de ces outils (formalités non respectées ou capacité d'atteinte à un système de traitement automatisé de données) ou une négligence entrainant des dommages (mauvais paramétrage d'un *sinkhole* ou défaut de surveillance d'un *honeypot*) pourraient en effet avoir pour conséquence une exclusion de garantie au profit de l'assureur.

L'exemple de la Pologne

En 2012, une attaque de *Dorkbot* a ciblé les internautes polonais[31], une grande partie du million d'ordinateurs formant le *botnet* y étant installés. Son principal objectif visait le vol de données bancaires, le malware comprenant notamment une fonction de désactivation des applications de sécurité hébergées sur les ordinateurs infectés. Le CERT Pologne était devenu l'une des cibles du *malware* qui fut finalement éradiqué en 2015, en partenariat avec Microsoft, le FBI et Europol. Cette opération a été rendue possible grâce à la mise en place d'un *DNS sinkhole* ciblant certains domaines « .pl » utilisés pour sa propagation et l'analyse très fine de la menace.

Plus de deux années auront été nécessaires pour neutraliser le *malware*. Le niveau de sophistication de *Dorkbot* a contraint le CERT et ses partenaires à une phase d'observation pour suivre les tendances du *malware* avant de pouvoir déployer une parade.

L'ensemble de l'opération a fait l'objet d'un rapport rédigé par le CERT Pologne et brossant le paysage de la sécurité informatique et les actions préconisées pour lutter contre ce type de *malware*[32].

L'exemple de la Corée du Sud

Le Centre coréen de coordination des interventions d'urgence informatique (KrCERT / CC) fait partie de l'agence gouvernementale KISA (*Korea Internet & Security Agency*). En 2005, il a lancé un partenariat public-privé avec les FAI coréens pour lutter contre les logiciels malveillants infectant les ordinateurs des utilisateurs coréens. Agissant comme acteur principal dans la lutte contre les logiciels malveillants, il recueille et vérifie l'information sur les vecteurs d'infection malveillante au profit de ses partenaires. A ce titre, il exploite un *sinkhole* DNS qui redirige le trafic de ces hôtes et domaines malveillants et indésirables. Presque tous les principaux FAI coréens répliquent volontairement les informations de routage issues du *sinkhole* de l'Agence dans leurs propres serveurs DNS.

Ce dispositif a permis de faire baisser le taux d'infection de *botnet* en Corée et a empêché leurs activités malveillantes telles que les attaques de déni de service (*DDoS*).

Le cas WannaCry

Du 12 au 15 mai 2017, le monde a été confronté à une attaque sans précédent de *ransomware* qui a touché des centaines de milliers d'individus et d'organisations dans plus de 150 pays. L'impact de cette cyber-attaque a eu plusieurs conséquences : plus de 40 hôpitaux infectés au Royaume-Uni, la fermeture des lignes de fabrication de certaines industries telle que Renault en France, etc. Par chance, quelques heures après la sortie initiale du *ransomware*, un chercheur de sécurité informatique qui analysait les logiciels malveillants a trouvé un domaine non enregistré dans le code du logiciel[33]. En enregistrant ce domaine en

[31] La majorité des PC infectés était basée en Pologne ; d'autres étaient situés en Allemagne, en France, aux Etats-Unis, en République Tchèque et au Royaume-Uni.

[32] https://www.cert.pl/wp.../RAPORT_Cert-NASK_ANG_www.pdf

[33] iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

vue de créer un *sinkhole* pour collecter des données sur le *malware*[34], il s'est rendu compte qu'il avait également activé un "*killswitch*"[35]. En effet, le malware, lorsqu'il infectait un ordinateur, vérifiait d'abord si le domaine en question était actif. Tant qu'il ne l'était pas, l'infection de l'hôte survenait, le chiffrement du disque dur se poursuivait et le verrouillage des fichiers devenait inéluctable.

Notons à ce sujet que des pirates ont tenté de neutraliser le *sinkhole* à l'aide de *botnets* d'objets connectés (de type Mirai), avec des résultats cependant mitigés : le *malware* étant programmé pour cesser son activité de recherche de cible au bout de 24h, son action était déjà largement endiguée lorsque le sinkhole a été attaqué.

Conclusion

Même s'ils sont complexes à mettre en œuvre, tant pour des raisons techniques que juridiques, ces systèmes de défense active se révèlent particulièrement efficaces pour faire face à certains types de menaces. Ils permettent en effet de comprendre le comportement des attaquants sans que ceux-ci ne puissent le soupçonner. Leur performance dépend cependant avant tout des capacités de détection employées, d'où l'importance stratégique des sondes de détection.

Après les *honeypots* et *sinkholes*, l'étape ultime pour leurrer les attaquants serait de parvenir à des systèmes auto-adaptatifs, c'est à dire susceptibles de reconfigurer automatiquement leur topologie réseau : saut d'adresse IP, numéros de ports aléatoires, etc. La DARPA a d'ailleurs inclus le *Moving Target Defense* comme une composante potentielle de son programme de Cloud résilient [36].

[34] En procédant à l'enregistrement de cette adresse, il créait un DNS Sinkhole visant à recueillir des informations sur le comportement de WannaCry

[35] Bouton d'arrêt d'urgence

[36] https://fcw.com/Articles/2012/04/15/FEAT-cybersecurity-moving-target-defense.aspx

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.eu