Prism : le révélateur du lucratif (et très discret) business de la vente de failles

La série d'articles parus la semaine dernière dans le *Washington Post*, affirmant que la NSA avait mené 231 opérations offensives dans le cyber-espace en 2011 et détaillant les pratiques de l'agence pour se fournir en « cyber-armes » lui permettant de mener ces actions, ont placé sous les projecteurs un des marchés les plus opaques de la cybersécurité : la commercialisation de vulnérabilités logicielles mais aussi d'exploits, des codes informatiques permettant d'utiliser ces failles pour soutirer des données aux personnes ou organisations ciblées. Toujours selon le Washington Post, la NSA aurait dépensé 25 millions de dollars en achats de vulnérabilités rien que cette année.

Une des stars de ce marché des plus opaques n'est autre que la société française, **Vpen Security**, basée à Montpellier et dirigée par **Chaouki Bekrar**. Wikileaks publie une brochure de la société expliquant que celle-ci propose une sorte d'abonnement aux services de renseignement de certains Etats, un abonnement qui leur ouvre un accès aux recherches de Vupen (vulnérabilités et exploits zero day, autrement dit des attaques reposant sur des failles non patchées par les éditeurs) via un portail. Le *Washington Post* s'amuse enfin de voir la société montpelliéraine ouvrir des bureaux dans le Maryland, non loin du siège de la NSA.

Contacté par la rédaction, Chaouki Bekrar s'est refusé à commenter les rapprochements établis par le quotidien américain. Toutefois dans un très intéressant podcast diffusé par *SecurityWeek* en mars dernier, le même Chaouki Bekrar détaille sans fard le « business model » de sa société. Décrivant cette dernière comme un acteur « du business des exploits fonctionnels », le Pdg explique que Vupen a d'abord contribué à la communauté de la sécurité (en publiant le résultat de ses recherches), mais que, du fait du refus des éditeurs comme Microsoft de mettre en place un système de récompense couvrant les coûts de sa société, Vupen a changé son fusil d'épaule en 2010. Et a développé son propre modèle économique en vendant le fruit de ses recherches à des clients, en l'occurrence des Etats. Un virage fructueux : si le chiffre d'affaires de la société reste inférieur au million d'euros (924 000, en croissance de 55 % en un an), sa rentabilité est au beau fixe (résultat net de 415 000 euros).

Une distinction légale entre vulnérabilités et exploits

Chaouki Bekrar explique avoir mis en place des critères de sélection de ses clients, *« même si la régulation internationale ne s'applique pas aux exploits »*, en se limitant aux pays membres de l'OTAN ou non frappés de restriction par la communauté internationale. Toujours dans cet entretien, Chaouki Bekrar affirme encore se conformer à la loi française sur les exploits et réclame d'ailleurs un encadrement similaire aux Etats-Unis, *« car je travaille déjà avec un cadre réglementaire en Europe »*, note-t-il. Contrairement à ses concurrents américains qui, eux, ont les mains totalement libres.

Un cadre réglementaire en France, oui mais lequel ? Dans un e-mail à la rédaction, le Pdg cite l'article R226-3 du Code pénal, qui prévoit une autorisation du Premier ministre pour *« la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente »* de certains appareils ou dispositifs techniques dont la liste est précisée dans un arrêté du 4 juillet 2012.

Pourtant, pour **François Coupez**, avocat associé au sein du cabinet Caprioli & Associés, ce texte inséré dans la LOPSSI s'applique plutôt aux *malwares* permettant la captation de données informatiques. *« En ce qui concerne la découverte de vulnérabilités, aucun texte ne vient a priori réguler leur éventuelle commercialisation, même s'il s'agit de la diffusion de failles qui peuvent être potentiellement exploitées dans un cadre de cyberguerre. Par contre, un article du code pénal, ayant donné lieu à un arrêt de la Cour d'Appel de Montpellier, confirmé en Cassation, interdit clairement la commercialisation et la diffusion d'exploits »*, explique-t-il.

L'Europe veut pénaliser la diffusion d'exploits

Cet article du Code pénal (le 323-3-1 inclus via la loi n°2004-575 du 21 juin 2004) statue que *« le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée »*. Un texte qui a valu une condamnation de 1 000 euros à un gérant de SARL spécialisée dans la sécurité, qui avait mis à disposition sur son site *« des scripts permettant d'exploiter des failles de sécurité informatique »*. On retrouve ce même principe dans la toute récente **directive européenne 2013/40** (12 août 2013), où l'Europe presse, dans son article 7, les états membres de prendre les *« mesures nécessaires pour ériger en infraction pénale »* la diffusion d'exploits.

« Il existe une réflexion sur l'encadrement de la vente de produits de DPI (Deep Packet Inspection), explique François Coupez. *Dans un genre similaire, une extension de cette réflexion aux vulnérabilités pourrait être envisagée, même si interdire leur vente purement et simplement est illusoire et dangereux. Il ne faudrait pas que cela handicape la recherche en sécurité des systèmes d'information, voire nos propres services de renseignement. »*

La France va légaliser la contre-attaque

Ni que d'éventuelles dénonciations de pratiques attribuées à des services étrangers ne jettent une lumière trop crue sur les agissements de nos propres cyber-soldats. De facto, en l'absence d'accord international en matière de cyber-armes, une législation nationale a peu de chance de s'appliquer. Pour qu'un article du Code pénal s'exerce, encore faut-il qu'il y ait plainte, ce qui relève de l'aberration dans le secteur du renseignement.

« La commercialisation des failles zero-day se situe dans une zone grise », résume **Gérôme Billois**, senior manager en gestion des risques et sécurité chez Solucom, un cabinet de conseil intervenant surtout auprès des grandes entreprises. Et le problème ne devrait aller qu'en s'accentuant, à mesure que les Etats musclent leurs capacités offensives dans le cyber-espace. *« La loi de programmation militaire française, qui couvrira la période 2014-2019, prévoit de légaliser la neutralisation des serveurs à l'origine*

d'une attaque. Un exemple qui montre bien que la sécurité offensive, consistant à utiliser l'outil informatique pour attaquer un adversaire ou à minima contre-attaquer, est en passe de se légaliser », observe Gérôme Billois.

Cette reconnaissance officielle des cyber-attaques devrait encore renforcer les problématiques autour de la vente de ces armes du XXIe siècle que sont les vulnérabilités logicielles et les codes permettant d'en tirer parti. Interrogés sur ces questions, ni l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ni le ministère de l'Economie numérique n'ont répondu aux questions de la rédaction.

Voir aussi

Rétrospective : la saga PRISM