# Gérôme Billois, Solucom : « La NSA a une des meilleures DSI au monde »

Un milliard de dollars. C'est la somme considérable qu'a déboursée l'éditeur FireEye pour mettre la main sur Mandiant (Lire *FireEye absorbe Mandiant pour mieux lutter contre les APT*), un spécialiste de la réponse aux incidents ayant réalisé environ 100 millions de dollars de chiffre d'affaires en 2012. Un facteur multiplicateur qui montre bien l'effervescence que connaît en ce moment le secteur de la sécurité, secoué par les multiples révélations d'Edward Snowden sur les capacités d'écoute de la NSA et marqué par la recrudescence des attaques contre les entreprises. Gérôme Billois, **senior manager en gestion des risques et sécurité chez Solucom**, un cabinet de conseil intervenant surtout auprès des grandes entreprises, analyse les grandes manœuvres en cours.

***Silicon.fr* – Comment interprétez-vous rachat de Mandiant par FireEye, au prix fort (1 milliard de dollars) ?**

**Gérôme Billois –** Ce rachat répond à une logique de plus en plus prégnante dans la sécurité : la « threat intelligence ». Il s'agit des informations portant sur les attaques elles-mêmes mais aussi sur les groupes qui mènent ces attaques. Car si les premières sont très nombreuses, les secondes le sont beaucoup moins : disposer d'informations précises sur ces groupes s'avère donc très précieux. Cette « threat intelligence » est devenu l'or noir des cyberdéfenseurs. Pour la réunir, vous avez besoin d'outils de gestion des incidents et d'outils de surveillance réseau. Mais aussi de l'expérience d'équipes spécialisées dans la réponse aux incidents.

Pour Mandiant, avant tout une société de services, s'accoler à un vendeur de produits risque par contre d'être un frein sur des contrats d'assistance sur incident. En Europe au moins, les RSSI ont tendance à privilégier des équipes indépendantes des fournisseurs de solutions. Les entreprises achètent différemment des prestations de services et des produits.

**Pourquoi FireEye a-t-il décidé de se renforcer ?**

FireEye est arrivé sur le marché avec une innovation technologique réelle. Mais cette innovation a depuis été dupliquée par des acteurs traditionnels comme Trend Micro, Palo Alto ou CheckPoint. Naturellement, le marché de FireEye se contracte, les entreprises privilégiant la mise à jour de solutions déjà existantes et maitrisées par les équipes. En mettant la main sur Mandiant, la société peut construire une offre tout en un, allant de la détection d'attaques, aux contre-mesures, voire à la contre-attaque. Si le marché n'est pas prêt en France pour ce type d'offres – les achats combinés de produits et de services y demeurent assez rares -, peut-être que ce rachat va faire bouger les lignes aux Etats-Unis, en forçant des acteurs comme RSA ou Symantec à réagir et à mettre plus en avant leurs services de surveillance sécurité et d'intervention sur incident.

**Du fait du contexte de suspicion créé par les révélations d'Edward Snowden, peut-on imaginer voir un grand groupe hexagonal se tourner vers le duo FireEye-Mandiant ?**

Depuis le rapport APT-1 (rapport diffusé début 2013 et pointant la responsabilité d'une unité spéciale de hackers associée à l'armée chinoise dans des attaques contre des entreprises et

administrations américaines, NDLR), le nom de Mandiant est connu y compris dans l'Hexagone, où des sociétés envisageaient d'avoir recours à ses services. Ceci dit, je vois mal un grand groupe hexagonal à capital majoritairement français se tourner vers FireEye-Mandiant, du fait de la proximité de ces sociétés avec les services de renseignement américains. Et ce, même si aucune société française ne dispose aujourd'hui d'une offre ayant une portée et un degré d'industrialisation comparables.

**FireEye et Mandiant ont chacun de leur côté pointé le péril constitué par les assaillants originaires de Chine…**

Oui, et c'est assez logique. Car les hackers « de l'Est » emploient souvent une approche qui consiste à « ratisser large » en volant de nombreux documents et en touchant beaucoup de systèmes dans le SI. Une approche très peu discrète, et donc bien détecté par FireEye et facile à analyser par Mandiant. A la différence de méthodes plus fines, comme celles de la NSA ou d'autres services de renseignement, qui ne laissent aucune trace ou très peu et qui sont très difficiles à identifier.

**Justement, la fin d'année dernière a été marquée par les révélations de *Der Spiegel* sur une division de la NSA baptisée ANT qui fournit des services d'attaques « ciblées » sur étagère en interne. Quelle a été votre réaction à la lecture de ces documents transmis par Edward Snowden à nos confrères ?**

Je n'ai pas été surpris que ces moyens existent. Par contre, ce qui est incroyable, c'est le degré de professionnalisation et d'industrialisation de ces services. Sur un plan organisationnel, c'est très propre ! Si tout cela est vrai et fonctionne comme c'est indiqué sur papier, la NSA est une des meilleures DSI au monde, une DSI maîtrisant le Big Data et capable de mettre sur pied un catalogue de services très précis. Au-delà de ces aspects organisationnels, il faut aussi noter la compromission de très nombreux firewalls. Avec le chiffrement – que la NSA a largement attaqué -, c'est l'autre moyen le plus couramment utilisé pour protéger les données. Bref, quand on additionne toutes les informations qui ont fuité grâce à Edward Snowden, on se rend compte qu'il est vraiment très difficile de se protéger des écoutes de la NSA. On peut cependant remarquer que les produits français de Arkoon, Alcatel-Lucent ou Netasq ne sont pas cités dans le catalogue de services d'attaques de la NSA de 2007. Cela ne veut pas dire qu'ils sont invulnérables, loin de là, mais cela montre qu'en construisant des architectures mixant différents fournisseurs et catégories de produits, on augmente la résistance aux attaques. Il faut donc, pour les périmètres les plus sensibles, se mettre dans une logique de sanctuarisation des informations et de diversification des solutions de sécurité afin de rendre les attaques longues et coûteuses, tout en sachant qu'on ne pourra pas les empêcher complètement.

**En complément :**

– Sécurité : FireEye absorbe Mandiant pour mieux lutter contre les APT
– La NSA, éditeur de spywares pour téléphones mobiles
– NSA : les matériels Cisco, Juniper et Huawei transformés en passoire
– NSA : backdoors à gogo pour affaiblir les disques durs et les serveurs
– Piratage du câble sous-marin : le pétard mouillé qui met le feu à la presse française