Eugène Kaspersky : « nous allons nous focaliser sur la sécurité industrielle »

Présent à l'occasion d'un sommet des analystes de sécurité à Cancun, notre confrère Susan Marvao de Bit magazine (une publication en ligne brésilienne du groupe Netmediaeurope) a rencontré Eugène Kaspersky, fondateur du groupe éponyme. Il est revenu sur différents sujets d'actualité et sur ses prévisions concernant les prochaines menaces.

BiT Magazine : Est-ce que 2014 a été une bonne année pour Kaspersky ?

Eugène Kaspersky : Oui, la société est en croissance. Elle se développe plus rapidement que le marché de la sécurité. Mais comme vous le savez, notre marché est majoritairement européen et nous publions nos résultats en dollars. Aussi, les variations des taux de change ont impacté plus fortement les résultats que prévu. Cela n'empêche pas l'entreprise de progresser, de proposer des nouveaux services et produits. Nous avons par exemple lancé un outil d'investigation et nous travaillons étroitement avec les autorités nationales de sécurité. En complément de nos clients traditionnels, nous allons nous focaliser sur la sécurité du secteur industriel.

Avez-vous déjà des clients sur ce secteur ?

Pas encore, mais il y en aura. Il est vrai que ce marché n'existe pas encore, mais il va arriver. Nous disposons de la technologie et de notre vision stratégique sur la cyber résilience des infrastructures critiques. Nous sommes en position d'attente.

Vous évoquez ces problèmes depuis des années, mais vous expliquiez que personne ne vous croyait à l'époque et maintenant ?

Aujourd'hui, cela devient réel et les cas vont augmenter. Nous commençons à parler de cyberterrorisme. Sur la partie cyber-sabotage, nous avons eu une attaque sur une infrastructure critique avec Stuxnet. En décembre dernier, un rapport allemand a mentionné une attaque similaire dans une industrie sidérurgique avec de vrais dommages physiques.

Sur Stuxnet, considérez-vous qu'il s'agisse de la première cyber-arme ?

La première à être connue, oui. Probablement, il y a eu d'autres attaques, mais nous ne les connaissons pas.

Est-il possible de protéger les infrastructures critiques ?

Oui c'est possible. Mais laissez-moi définir la protection. Elle doit être considérée comme bonne si une attaque coûte plus cher à mener que les dommages occasionnés. C'est le même principe pour le chiffrement, les algorithmes de cryptages sont intéressants si le coût pour craquer un code est plus onéreux que la valeur de la donnée.

A Cancun, plusieurs annonces ont été faites sur des attaques très sophistiquées comme Carbanak ou celles perpétrées par le groupe Equation. Quel impact peut avoir ces découvertes ?

Ces attaques que nous avons annoncées montrent un niveau de sophistication très importante. Dans le cas du groupe Equation, le message est clair pour les constructeurs de disques durs : tous les produits sont affectés. Il n'est pas possible de les nettoyer, car il n'y a pas d'outils pour le faire.

Est-ce que l'affaire Snowden a changé le monde ?

Pas vraiment. On peut distinguer deux secteurs. Le grand public et les entreprises ou les Etats. Pour les premiers, les consommateurs ne s'en soucient pas. Par exemple, combien de personnes ont cessé d'utiliser les services de Google depuis l'affaire Snowden ? Pour les entreprises, certaines commencent à travailler sur des services spécifiques pour garantir la vie privée.

Mais je suis sûr qu'une chose a changé c'est que les criminels et les terroristes ont appris. Par ailleurs, les États sont maintenant plus conscients de ces problématiques.

Kaspersky travaille étroitement avec les agences nationales de sécurité et les gouvernements partout dans le monde. Quel genre d'informations partager vous avec eux ?

Nous partageons toutes les données techniques que nous avons sur les attaques, les algorithmes, les victimes potentielles, les adresses IP, email, etc. Mais nous ne partageons pas les données d'autres pays. En d'autres termes, si je parle à la police portugaise, je donnerais seulement les données relatives à ce pays. En étant une structure globale, nous avons un vue mondiale des incidents de sécurité. Nous savons que le Portugal peut-être victime d'attaques de l'extérieur. Dans ce cas, nous partagerons avec les autorités portugaises des détails sur l'attaque mais sans mentionner les victimes portugaises. Dans le cas d'Interpol, c'est différent il s'agit d'une entité œuvrant sur plusieurs pays.

Dans le domaine de la cybercriminalité, est-ce que la criminalité traditionnelle s'empare de l'espace virtuel ?

Oui sans conteste. Malheureusement depuis ces dernières années, nous assistons à une augmentation des affaires où la criminalité traditionnelle s'appuie sur outils de social ingénierie ou trouve des informateurs pour attaquer les systèmes d'information. Nous ne sommes plus dans la cybercriminalité qui reste orientée vers la donnée.

Permettez-moi de vous donner un exemple pour mieux comprendre. Un cartel d'Amérique Latine utilisait des conteneurs pour transporter de la cocaïne via le port d'Antwerp. Il avait réussi à pirater le système d'information du port pour décharger les conteneurs dans une zone sécurisée sans passer le contrôle des douanes. Dans ce cas, il ne s'agit pas d'un cas de cybercriminalité habituelle. Les outils informatiques viennent en soutien à la criminalité classique. C'est effrayant car les criminels ont conscience de l'importance du cyberespace. Les prochains à comprendre ce pouvoir sont les terroristes.

Vous avez accès à des informations sensibles comme les données personnelles, vous surveillez mais qui contrôle vos activités ?

Qui nous contrôle ?… Notre karma. Nous équipons des milliers d'ordinateurs, mais nous faisons de notre mieux pour ne pas collecter des données personnelles, y compris les adresses IP. Si la police nous demande ces données, nous leur fournissons, mais nous ne les recueillons pas Nous

respectons la réglementation des pays dans lesquels nous sommes présents. Par contre, si une attaque est repérée et que nous découvrons un malware alors nous avertissons les victimes ou la police.

Quelle est votre opinion sur l'Internet des objets ?

Cela représente surtout l'Internet des menaces. Je vois l'Internet des objets comme une évolution de l'innovation. C'est un cycle avec en premier lieu l'innovation, puis ensuite les produits et les services, enfin les questions de sécurité qui seront résolues. Et le cycle recommence.

Comment voyez-vous l'avenir de votre société dans 5 ans ?

Très certainement dans la sécurité des systèmes industriels. Et dans la sécurité de ce que l'on nomme l'Internet des objets. Je ne sais pas quand, mais nous estimons que la prochaine attaque sera sur les Smart TV puis sur les systèmes connectés des habitations. Mais cela débutera sur les smart TV. Mais je rêve de la sécurité des systèmes industriels.

A lire aussi :

Desert Falcons : Kaspersky identifie un groupe de cybermercenaires arabes

Un malware résistant à un formatage de disque dur : l'œuvre de la NSA ?