L'actualité de la Menace et de la Protection des Entreprises et des Etats

SECURITY DEFENSE
Business review

L'actu de la Menace

N° 50 • 08 Novembre 2011

➔ L'Iran de plus en plus menaçante!

Suite à la révélation d'une tentative d'assassinat contre l'ambassadeur d'Arabie Saoudite aux Etats-Unis, par 2 iraniens manipulés par les Pasdaran et leur branche opérationnelle à l'étranger "la force Al-Qods", le guide suprême de la révolution islamique, l'ayatollah Ali Khamenei, s'en est pris directement au gouvernement saoudien et à la famille royale saoudienne les menaçant des pires représailles. Cet "incident" démontre que l'Iran n'a pas abandonné son désir d'expansionnisme dans la région.

➔ Le Kenya face aux islamistes

L'Union africaine soutient l'opération militaire kényane contre le groupe somalien Shebab en Somalie qu'elle considère comme une menace pour le Kenya et la paix dans la région. L'Ethiopie, que le Kenya considère comme un allié crucial dans la guerre contre les militants islamistes Shebab dans la région, lui a également exprimé son soutien. Face aux provocations des milices islamistes d'Al-Chebaab, le Kenya a fermé ses frontières avec la Somalie. *Xinhua*

➔ Narcotrafic sans foi ni loi...

La police du Texas a lancé une alerte face à la multiplication des cas de mineurs impliqués dans le trafic de drogue du fait des cartels de drogue mexicains qui étendent leur influence du côté nord de la frontière. Au début du mois d'octobre, un jeune de 12 ans a été arrêté au volant d'un camion qui contenait 300 kilos de marijuana. En 2011, plus de 25 adolescents ont été arrêtés pour trafic de drogue dans la région du Texas qui borde la frontière mexicaine. *L'atlantico*

➔ Londres 2012: menaces terroristes

Les services de sécurité britanniques travaillent à détecter les menaces d'attaques terroristes qui planent sur les JO de Londres de 2012. C'est la première fois que les Jeux olympiques se dérouleront dans un pays sous une forte menace d'attaque terroriste. Le 18 septembre, 7 personnes ont été arrêtées à Birmingham, accusées de préparer un attentat. Le MI5 est vigilant face aux habituelles attaques terroristes: complots organisés par Al-Qaeda ou djihadistes affiliés, attaques individuelles de personnes ayant un background islamiste, ou attaques de groupes d'Irlandais républicains rebelles voulant attirer l'attention. *The Economist*

➔ Cyber menace

Un des plus gros sous-traitants du ministère de la Défense japonais, Mitsubishi Heavy Industries (MHI), a subi une attaque informatique courant août. L'enquête interne confirmerait le vol de données sensibles: plans d'avions de chasse, d'hélicoptères et d'une centrale nucléaire. Il y a quelques mois, plusieurs sous-traitants de l'armée américaine ont eux aussi été victimes de cyber attaques (Lockheed Martin, L-3 Communications, Northrop Grumman) sans identification officielle des auteurs...*Reuters*

SOMMAIRE

AGENDA

➢**07 - 13 Novembre 2011 - Israël**
9th Israeli Transportation Security Solutions
➢**13 - 17 Novembre 2011 - Dubaï, EAU**
Dubaï Air Show
➢**17 - 18 Novembre 2011 - Genève, Suisse**
Homeland & Global Security Forum
➢**1er Décembre 2011 - Paris, France**
GRC Interchange
➢**12 - 14 Décembre 2011 - Sharjah, EAU**
Gulf Maritime

Plus d'infos

➔ Athènes

Le limogeage brutal, le 01/11 par le gouvernement socialiste grec, des chefs de l'armée de terre, de la marine, de l'armée de l'air et du chef d'état-major des armées, laisse planer un doute sur ses raisons profondes. Bruit de bottes de militaires mécontents de la diminution de leur solde ou malaise profond?

Interview du Gal Pierre-Jacques Costedoat

PDG de SSF*

♦ SDBR: Général, depuis combien de temps êtes-vous chez SSF ?

P-J C: J'ai commencé chez SSF en 2003, après une carrière militaire d'une quarantaine d'années. J'ai commencé comme conseiller, avant d'en devenir le Président Directeur Général il y a 3 ans.

♦ Aujourd'hui SSF a changé d'actionnariat. Pouvez-vous nous parler de cette évolution ?

SSF est devenue le 01/02/2010 une filiale du groupe Scutum, groupe familial français centré sur la sécurité électronique: contrôle d'accès, vidéosurveillance, téléassistance, etc. Dans le cadre d'une politique de croissance externe, les dirigeants de Scutum ont entendu parler de SSF et ont considéré qu'il pouvait y avoir une complémentarité entre nos activités respectives, en termes de produits, de clients et de savoir-faire. Notre cœur de métier est le conseil et l'assistance, en matière de sûreté et de sécurité, et l'accompagnement de sociétés à l'Etranger pour sécuriser leurs collaborateurs. Donc, avec Scutum, nous avons vraiment une complémentarité en sûreté et à l'international. Scutum réalise environ 85 millions d'euros de chiffre d'affaires avec 700 personnes et commence à se porter sur l'international, avec SSF et grâce à l'acquisition de la société Inform Solutions GmbH (société allemande spécialisée dans la mise en sûreté des agences bancaires).

♦ Qu'est ce qui résulte de l'acquisition, il y a un an et demi, de SSF par Scutum ?

Nous avons appris à nous connaitre et Scutum a mis à notre disposition son savoir-faire technique, notamment dans le domaine de l'hébergement sécurisé de données, ce qui nous a aidé dans la mise au point du "Locator", l'outil de sécurisation de la mobilité des collaborateurs d'entreprise que nous venons de lancer. Nous connaissions bien les attentes des entreprises qui ont des collaborateurs voyageant dans le monde entier: elles ont besoin de préparer leur départ et de collecter de l'information, de savoir de façon permanente où sont localisés les collaborateurs et de pouvoir, instantanément en cas de crise, identifier qui est où et pouvoir communiquer avec eux. Depuis un an et demi, nous nous sommes aussi rapprochés géographiquement de nos clients, avec notre nouveau siège rue de Magellan à Paris, nous avons lancé un département Asie en 2010 et nous avons intégré plusieurs jeunes collaborateurs.

♦ Pouvez-vous nous parler de l'organisation de SSF ?

Au delà de notre équipe permanente nous fonctionnons avec des partenaires, dont certains nous assistent depuis plus de 10 ans: je pense à notre plateau d'appels en H24 et 7j/7j, je pense à notre partenaire logistique et opérationnel qui nous aide à accompagner des personnes dans certains pays du globe, etc. Chaque client et chaque déplacement étant particulier, nous construisons à chaque fois une prestation sur mesure en fonction du contexte local, du domaine d'activités de l'entreprise ou de sa visibilité dans le pays.

♦ Ces partenaires sont-ils donc des locaux ?

Cela dépend, ils sont français ou étrangers. En Afrique nous avons beaucoup de partenaires français, mais ailleurs cela peut-être différent.

♦ Pourquoi une entreprise choisira t'elle SSF pour son accompagnement à l'international ?

Dans ce domaine, la réputation et ce qu'on appelle "le bouche à oreille" sont notre meilleure publicité. Ce sont nos clients historiques qui parlent le mieux de SSF mais je ne peux pas vous les citer, vous comprenez bien pourquoi...

♦ Pouvez-vous nous détailler vos domaines d'intervention ?

Historiquement nous avons commencé par la création d'une base d'information, avec 2 produits d'information. Le premier est un site abonné où nous suivons 192 pays en français et en anglais. Pour chacun de ces pays, le client trouve des données (géographiques, économiques, etc.) mais aussi une analyse de sécurité "risque pays". Le deuxième produit est l'alerte quotidienne (20 à 30 alertes par jour selon l'actualité) que SSF adresse à ses abonnés pour les 192 pays couverts. Nous essayons d'aller au-delà de l'information brute, en commentant ce qui peut désorganiser l'activité de nos clients dans un pays sous alerte. En tant que de besoin et grâce à notre hotline, nos clients peuvent nous demander une analyse plus approfondie de la situation d'alerte dans un pays particulier. Notre activité d'information a été initiée pour répondre à l'obligation légale du chef d'entreprise d'informer ses salariés des risques encourus par un déplacement à l'étranger (jurisprudence Karachi).

Suite de l'interview page 3...

SSF: "Scutum Security First" anciennement "Sécurité Sans Frontières"

Interview du Gal Pierre-Jacques Costedoat
PDG de SSF*

♦ **Au delà de ce cœur de métier "information" vous offrez d'autres prestations, n'est-ce pas ?**

Oui bien sûr, le deuxième volet sécuritaire c'est la prévention, donc nous parlons d'audit. Nous avons une capacité à auditer des dispositifs, en France ou à l'Etranger, dans différents domaines: prise en compte de l'existant, règles et consignes de sécurité, plan d'évacuation, évaluation des risques, sécurité physique, sécurité électronique et informatique, etc. Nos recommandations peuvent s'accompagner de la mise à disposition d'un expert apte à mettre en place les bonnes pratiques sur le terrain, à recruter du personnel local, à assurer des formations, etc. Lorsque nous détachons un "Security manager" pour une période longue, nous le recrutons spécialement sous la forme d'un contrat de mission.

♦ **Faites-vous de l'assistance à la gestion de crise ?**

Oui, nous offrons le panel classique des prestations liées à la gestion de crise, y compris la protection rapprochée, que ce soit en France ou à l'Etranger. Nous avons aussi une activité d'intelligence économique qui permet d'accompagner certains clients sur des problématiques parfois complexes et leur éviter de tomber dans des pièges. Nous croyons beaucoup à l'humain dans l'analyse de l'information car, même si les moteurs de data mining sont bons, on peut passer parfois à coté de renseignements essentiels. Nos réponses à leurs problématiques sont de nature à permettre à nos clients de réduire l'incertitude au quotidien et à les accompagner au plus près dans leurs choix opérationnels et leur connaissance des circuits de décision. En fait, c'est très complémentaire de ce que nous faisons dans notre cœur de métier informationnel.

♦ **Revenons à Locator. Pourquoi avez-vous conçu ce produit ?**

Le Locator est un outil de sécurisation de la mobilité des collaborateurs. C'est historique. Depuis 2001, grâce à notre site dédié, les collaborateurs de nos abonnés pouvaient auto-déclarer leurs déplacements. Lorsqu'un incident survenait, avec notre base de données auto-déclarées, nous étions en mesure de dire à notre client combien de personnes étaient censées se trouver à tel ou tel endroit. Dans une phase ultérieure, nous avons récupéré auprès des agences de voyage les données de nos clients. En 2009, nous avons signé avec Selectour et Amadeus un contrat de partenariat pour rendre compatible les données de ces opérateurs avec Locator. En 2010, nous avons fait les premiers tests avec les données de voyage et en 2011 nous nous sommes mis d'accord avec les GDS** pour extraire les données dans leurs réservations. Nous opérons en liaison protégée (https) et nous hébergeons ces données-clients chez Scutum, dans un site sécurisé en France géré par du personnel habilité "confidentiel-défense". Au préalable, notre client a donné une consigne d'identification des réservations à son agence de voyage.

♦ **Et que faites vous avec ces données ?**

Nous restituons ces données sous la forme d'un tableau de bord et d'une cartographie, accessibles par internet avec un identifiant et un mot de passe. Le responsable désigné par notre client (risk manager, Security manager, etc.) peut alors localiser les collaborateurs itinérants et expatriés en temps réel: combien, dans quel pays, sur quel avion ? Il peut aussi les identifier et leur communiquer des informations ou consignes, par sms et email, toujours via le site internet Locator. C'est facile à utiliser et le Locator permet un gain de temps précieux en cas de crise. En option, le collaborateur de notre client peut accéder aux informations « sécurité » et « santé » sur notre site. Pendant son séjour, il a aussi la possibilité de recevoir sur son Smartphone les alertes quotidiennes que nous fournissons sur les conditions sécuritaires et sanitaires dans le pays où il se trouve. Avec le Locator nos clients sont sûrs que la mobilité de leurs collaborateurs est sécurisée. L'autre avantage du Locator est de pouvoir préparer un déplacement avec des outils d'informations détaillées en matière de sécurité et de santé.

♦ **Le Locator est-il adapté à toutes les tailles d'entreprises ?**

Oui. C'est le nombre de déplacements de collaborateurs qui compte, que ce soit un grand groupe avec 200.000 déplacements annuels ou une PME avec 1500.

♦ **Quel regard portez-vous sur le marché français de l'accompagnement des entreprises aujourd'hui?**

Il y aura forcément un jour une concentration de ce marché. Des sociétés comme SSF doivent prendre un peu plus d'ampleur, car nous couvrons un spectre important de services à nos clients et nous devons peser plus en termes d'emplois. Nous avons un fort taux de développement interne, grâce notamment à l'ouverture de notre département Asie qui nous permet d'accompagner des entreprises en Chine et dans la région. Dans la compétition internationale, nous apportons notre professionnalisme et la culture de la prévention des risques et de l'anticipation qui nous rendent représentatifs de la "sécurité à la française". Mais pour enrichir nos savoir-faire, il faut probablement que nous étudions aussi des possibilités de croissance externe...

Interview réalisée par Alain Establier

***GDS: "global distribution systems" ou systèmes de réservation informatique. Dans les transports/hôtellerie les 4 plus gros sont: Sabre, Galileo, WorldSpan et Amadeus.*

Dans les secteurs

➔ Les exportations françaises d'armement en net reflux en 2010 !

Avec 5,12 milliards d'euros de prises de commandes en 2010, les industriels français du secteur Défense (330.000 emplois directs et indirects) réalisent leur plus mauvaise année depuis 2005! Alors que le plan de relance de 2007 devait doper durablement les exportations pour maintenir la France au 4ème rang mondial, est-ce qu'on assiste à un tassement du à la crise débutée en 2009 ou bien à une tendance lourde due à la surévaluation de l'euro? Il faudra attendre les chiffres de 2011 et de 2012 pour le savoir. Cinq pays se partagent près de 86% du marché mondial de l'armement: USA (53,7%), GB (12,5%), Russie (8,2%), France (6%) et Israël (5,3%).

➔ GRC Interchange: pour faire le point sur l'approche risque et conformité de vos SI

Organisé par SecurityVibes sur une journée, le 1er décembre à Paris "Fondation Dosne-Thiers", GRC Interchange sera un temps d'échange privilégié bâti autour de tables rondes thématiques, entre les praticiens de la sécurité (RSSI, Risk Managers…) et les spécialistes de ce marché. Parmi les thèmes abordés: la gestion du risque en environnement extrême, faciliter le passage des directives SSI à l'opérationnel, construire un véritable pilotage de la conformité, etc. www.securityvibes.com

➔ Cassidian se renforce dans le domaine des drones légers

Cassidian a racheté la société SurveyCopter dans le but d'accroître la synergie de son offre sur le segment des drones légers. Fondée en 1996, SurveyCopter est une société française, active dans le secteur de la défense, qui travaille avec Cassidian depuis 2003. Cassidian envisage de lancer un nouveau pôle industriel consacré aux drones tactiques et aux drones légers, incluant les programmes VTOL (Vertical Take Off and Landing - aéronef à décollage et atterrissage verticaux), afin de mieux répondre à la demande croissante du secteur pour les environnements de mission militaires ou privés.

➔ Scutum continue sa croissance externe

Acteur français de la protection des biens et de la sécurité des personnes, Scutum prend le contrôle de la société France Incendie, constructeur d'extincteurs et spécialiste certifié de la sécurité incendie pour les entreprises et les collectivités locales. Avec l'acquisition de la société France Incendie, Scutum intègre la sécurité incendie dans son offre globale de solutions de sécurité et de protection des personnes, destinée aux entreprises et établissements publics.

➔ Actualités du groupe Thales

- Le Comité Militaire de l'Atlantique Nord a accordé l'agrément Secret OTAN à ECHINOPS, la solution de chiffrement pour la sécurité des réseaux IP haut débit de Thales, développée conjointement avec la DGA et l'ANSSI. L'obtention de cet agrément permet aux forces armées françaises de répondre à leurs engagements vis à vis de leurs alliés tout en garantissant un haut niveau de maîtrise des systèmes et des informations sensibles échangées.
- Thales a déployé la Base de Données de Sécurité Publique (BDSP), le système de commandement et d'information de la Gendarmerie Nationale pour la conduite des opérations et le traitement du renseignement opérationnel. BDSP permet aux gendarmes, depuis les centres de commandement jusqu'aux patrouilles, d'accéder à la synthèse de toutes les informations disponibles en lien avec une mission ou une intervention. A terme, ce sont 60 000 gendarmes répartis sur 4300 sites qui utiliseront et alimenteront en permanence une base de données centrale du renseignement opérationnel.

➔ Morpho (groupe Safran) en position de leader sur son marché

Morpho, acteur mondial de la technologie de reconnaissance biométrique, vient de livrer son millionième dispositif biométrique à la société indienne STJ Electronics Pvt, spécialisée dans les solutions de gestion de présence et de contrôle d'accès. Morpho est un pionnier des terminaux biométriques multimodaux qui associent la reconnaissance des empreintes digitales et du réseau veineux.

➔ HID Global: une nouvelle génération de lecteurs et de cartes sans contact

HID Global a annoncé la disponibilité de iCLASS SE, un nouvel environnement et un écosystème basé sur l'architecture «Trusted Identity Platform» (TIP) qui permet des applications de pointe, la mobilité et un renforcement de la protection contre les menaces de sécurité en matière de contrôle d'accès. Une nouvelle méthodologie d'identifiants numériques portables, appelée SIO (Secure Identity Object), pourra être déployée tant sur des systèmes fixes que sur des Smartphones, cartes à micro-processeur, cartes à puce sans contact, jetons USB et terminaux connexes.

Les marchés financiers

➔ Tendance générale des marchés

Alors que les premières réactions des marchés aux décisions européennes du 26 octobre s'avéraient positives, malgré bien des incertitudes (notamment sur les modalités de l'augmentation de capacité du Fonds Européen de Stabilité Financière), le psychodrame du référendum en Grèce a entraîné une violente réaction négative des marchés qui craignent que la Grèce s'engage sur une voie hasardeuse et constatent que la crise grecque est loin d'être réglée. Il est possible que George Papandreou n'ait fait qu'avancer le calendrier des prochains soubresauts (on aurait cependant pu espérer un retour au calme jusqu'à début 2012) et que les faiblesses des décisions du 26 octobre, comme celles du 21 juillet, se seraient tôt ou tard imposées : il manque à ces accords le ciment politique, en clair au moins la réponse à ces deux questions : quelle vision pour l'Europe et la Zone Euro à horizon 10 ou 20 ans ? Comment la Grèce (ou un autre pays en difficulté) peut-elle se redresser à terme ? Les dirigeants européens avancent dans leur décision, mais d'autres Sommets seront encore nécessaires pour désamorcer les inquiétudes exprimées par les marchés.

Les Leaders du secteur Security & Defense

Nom	Pays	Cours au 31/12/10	Cours au 21/10/11	Cours au 04/11/11	▲ / ▼	Depuis le 01/01/11
Rheinmetall	DE	60,17	38,34	38,96	▲	-35%
ThyssenKrupp	DE	30,99	19,45	20,81	▲	-33%
Siemens	DE	92,70	72,55	73,94	▲	-20%
Alcatel-Lucent	FR	2,18	1,97	1,68	▼	-23%
Bull	FR	3,41	3,59	3,32	▼	-3%
Dassault Aviation	FR	601	662,65	694,99	▲	16%
EADS	FR	17,32	20,09	21,63	▲	**25%**
Gemalto	FR	31,84	32,23	32,97	▲	4%
Safran	FR	26,5	22,27	24,29	▲	-8%
Thales	FR	26,18	24,99	25,22	▲	-4%
Finmeccanica	IT	8,51	4,93	4,6	▼	-46%
Hitachi Ltd	JP	433	402	431	▲	0%
Mitsubishi Electric	JP	852	712	730	▲	-14%
Panasonic	JP	1153	776	733	▼	-36%
Sony	JP	2927	1556	1400	▼	**-52%**
Assa Abloy	SW	189,5	150	162,1	▲	-14%
Axis AB	SW	122,5	145,75	143	▼	17%
Saab Group	SW	123	125	121,8	▼	-1%

Nom	Pays	Cours au 31/12/10	Cours au 21/10/11	Cours au 04/11/11	▲ / ▼	Depuis le 01/01/11
Volvo AB	SW	118,5	73,95	81,9	▲	-31%
Babcock Int Group	UK	571	676,5	704,5	▲	23%
Bae Systems	UK	330	274,5	273,3	▼	-17%
Qinetiq Group	UK	130	116,4	119,3	▲	-8%
Ultra Electronics	UK	1696	1595	1626	▲	-4%
Cisco Systems	US	20,23	17,19	17,9	▲	-12%
Elbit Systems	US	53,13	42,75	42,11	▼	-21%
General Dynamics	US	70,96	63,15	63,07	▼	-11%
Honeywell Int.	US	53,16	48,46	53,58	▲	1%
Ingersoll Rand	US	47,09	27,38	32,32	▲	-31%
L3 Communications	US	70,49	68,81	67,95	▼	-4%
Lockheed Martin	US	69,91	75,7	75,29	▼	8%
Northrop Grumman	US	57,9	54,11	56,96	▲	-2%
Raytheon	US	46,34	42,76	43,73	▲	-6%
SAIC Inc	US	15,86	12,54	12,59	▲	-21%
Texas Instruments	US	32,5	29,95	31,52	▲	-3%
Tyco International	US	41,44	43,78	44,93	▲	8%
United Technologies	US	78,72	74,25	76,99	▲	-2%

DE: Frankfurt, FR: Paris, IT: Milano, UK: London, SW: Stockholm, US: NYSE, JP: Tokyo

➔ Flash sur une valeur

SAAB Group

Flottant: 37 749 614 actions soit 35,2 % du total des actions
Cours au 31/12/2010 : 123 SEK
Cours au 21/10/2011 : 125 SEK
Cours au 04/11/2011 : 121,80 SEK
Variation par rapport au 31/12/2010 : - 1 %
Dividende 2010: 3,50 SEK soit un rendement de 2,84 %
Actualités: CA 2010: 24,4 milliards de couronnes suédoises dont 62% réalisés hors de Suède (12.536 employés). 5 Gripen sont intervenus avec l'OTAN pendant la campagne libyenne (650 missions de combat). Signature avec l'armée britannique d'une extension de contrat de maintenance et de formation (150MSEK) sur systèmes à code laser OSAG 2.0. Large compétence en systèmes de radars et C4i. Développement du drone Skeldar V200 maritime à voilure tournante.

Infos utiles

➔Une publication bimensuelle
➔Rédacteur en chef : Alain Establier
➔Société Editrice : SDBR Conseil, SAS domiciliée
26 rue de la République 92150 Suresnes, France
520 236 662 RCS Nanterre
E-mail : admin@securitydefensebusinessreview.com
Web: **www.securitydefensebusinessreview.com**

➔Abonnements: +33 (0) 9 77 19 76 40
Abonnement annuel : 900 € HT (TVA 5,5 % : 949,50 € TTC)
Abonnement semestriel : 550 € HT (TVA 5,5 % : 580,25 € TTC)
ISSN 2107-7312

Prochain Numéro: **Mardi 22 Novembre 2011**

Entretien avec Laurent Heslault* de Symantec

➔ SDBR: On entend souvent que les antivirus des grands éditeurs seraient désarmés face à la multiplication exponentielle des "malware". Que répondez-vous à cela?

LH: Moi aussi j'entends souvent que nos antivirus ne détecteraient que 50%, voire 25% des malware en circulation...Demandez donc à ceux qui disent cela de vous fournir les études qui le prouvent! D'où sortent-ils ces chiffres? Moi je n'en connais pas! Les seules études sérieuses faites sur le sujet le sont par l'AMTSO** et on sait qu'il est extrêmement difficile de tester objectivement un antivirus.

➔ Pour autant est-ce que vos clients sont bien protégés avec les solutions Symantec ?

La problématique est bien plus large. A partir du moment où nous parlons de sécurité informatique, nous devons intégrer l'analyse des risques dans ses 3 dimensions: humaine, procédurale et technologique. Reparlons de "Conficker" si vous permettez. Fin octobre 2008, Microsoft annonce une vulnérabilité critique, d'ailleurs corrigée le jour même. Quelques jours plus tard, Symantec observe une exploitation de cette vulnérabilité sur "Conficker A" (grâce aux signatures sur vulnérabilités que nous mettons systématiquement en place), puis nous observons dans les semaines qui suivent l'apparition de versions B, C, etc. Résultat: 12 millions de postes sont infectés parce que 12 millions de postes ne sont pas "patchés" (non mis à jour par le correctif Microsoft)! Pourquoi? Parce que nous avons affaire à des logiciels Microsoft piratés, ou non actifs, qui ne reçoivent pas les mises à jour automatiques envoyées par Microsoft.

➔ Est-ce que ce sont des particuliers ou des entreprises qui sont concernés ?

La plupart des particuliers qui achètent un ordinateur sous Windows reçoivent ensuite les mises à jour automatiques. Ce n'est pas le cas pour les entreprises pour différentes raisons: plate-forme complexe, autorisation des correctifs par l'intranet, vieille version de Windows plus fragile, copie craquée, etc. Résultat: ce sont souvent dans les entreprises que l'on observe les plus grands risques alors même qu'elles sont les plus menacées. C'est exactement ce qu'a dit monsieur Patrick Pailloux, DG de l'ANSSI, aux Assises de Monaco en octobre. Il y 3 ans, nous avons développé une nouvelle technologie pour répondre justement à la croissance exponentielle des maliciels (près d'un par machine en fait, avec l'apparition de singleton). En effet, un antivirus qui travaille uniquement en mode signature identifie aujourd'hui de moins en moins de maliciels. C'est pourquoi Symantec crée cette année 17 millions de signatures (en 2001, 5 signatures créées par jour et en 2011 30.000 par jour)!

➔ Donc la technologie de simple gestion des signatures est dépassée ?

Bien sûr. C'est pourquoi un certain nombre d'éditeurs d'antivirus sont passés au mode "heuristique" qui permet de lire les codes. Mais ce n'était pas encore suffisant, donc nous avons développé une couche comportementale qui observe le comportement d'un programme au démarrage. Par rapport à des profils d'action bienveillante, nous sommes maintenant capables de détecter la légitimité d'un programme donné (écoutes de clavier, envoi d'information dans des pays à risques, etc.). Pour arriver à ce niveau de performances, Symantec dépense plus de 800 millions de dollars par an en recherche et développement. C'est ce qui a permis à un de nos chercheurs d'imaginer il y a 3 ans de baser la sécurité sur l'analyse de la réputation des fichiers (pas simplement la réputation des sites web qui existe depuis longtemps). En gros nous avons décidé de collecter tous les exécutables de l'internet (+ de 3,5 milliards) et de rajouter des tests de profiling, la taille des codes, etc. pour sortir un score de réputation. Avec ce dispositif nos clients bénéficient d'un niveau de protection inégalée (également en mode portable).

➔ Est-ce grâce à ce dispositif que vous êtes tombés sur "Duqu" ?

Il s'agit d'autre chose car nous sommes là en présence d'une attaque très ciblée, qui a été remontée par la communauté informatique où il existe une grande solidarité lorsqu'il s'agit de sécurité fondamentale. "Duqu" ressemble un peu à "Stuxnet" qui est apparu l'année dernière. C'est un "Trojan" qui cherche des informations sur des personnes produisant des logiciels pour des environnements SCADA. Stuxnet ciblait Siemens, mais il y en a d'autres. Cela veut dire que certains cherchent des éléments qui permettraient de lancer des attaques de type Stuxnet. Stuxnet était un vrai cyber-sabotage alors que Duqu est un logiciel de repérage et de captation d'informations. Mais les éditeurs sont vite remplacés dans ces enquêtes par des services officiels...

Propos recueillis par Alain Establier

** Laurent Heslault est directeur des technologies de sécurité pour Symantec Europe de l'ouest*

*** AMTSO "Anti Malware Testing Standards Organization": association, regroupant plus de 40 éditeurs et organismes de tests, qui a pour ambition de répondre au besoin général d'amélioration de l'objectivité, de la qualité et de la pertinence des méthodologies d'évaluation.*