KASPERSKY lab

Kaspersky Security Bulletin 2015

# PRINCIPAUX ÉVÉNEMENTS EN MATIÈRE DE SÉCURITÉ

GREAT

#KLReport

# SOMMAIRE

ATTAQUES CIBLÉES ET CAMPAGNES DE MALWARES ..... 3
FUITES DE DONNÉES ..... 11
APPAREILS INTELLIGENTS (MAIS PAS FORCÉMENT SÛRS) ... 13
COOPÉRATION INTERNATIONALE DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ ..... 15
ATTAQUES CONTRE DES INFRASTRUCTURES INDUSTRIELLES ..... 17
CONCLUSION ..... 20

La fin de l'année est traditionnellement un temps de réflexion - pour faire le bilan de nos vies avant d'envisager ce qui nous attend. Nous aimerions offrir notre rétrospective traditionnelle des principaux événements qui ont façonné le paysage des menaces en 2015..

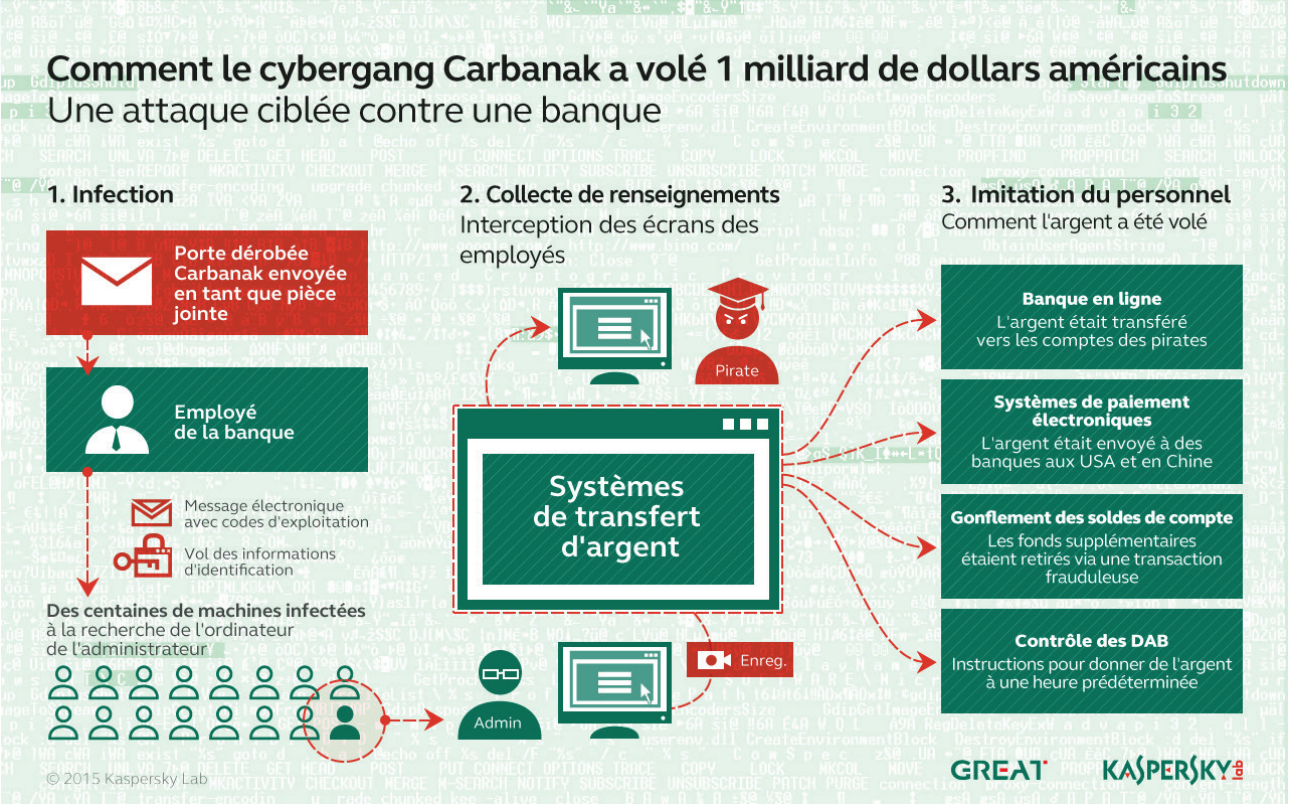
# ATTAQUES CIBLÉES ET CAMPAGNES DE MALWARES

Les attaques ciblées sont bien implantées parmi les menaces et il n'est dès lors pas étonnant de les retrouver dans notre rétrospective annuelle. Dans nos prévisions sur la sécurité de l'année dernière, nous avions souligné les développements que les menaces APT allaient suivre d'après nous.

- Convergence de la cybercriminalité et des menaces avancées persistantes
- Fragmentation des plus grands groupes APT
- Evolution des techniques de malwares
- Nouvelles méthodes d'extraction des données
- APT : course à l'armement

Voici les principales campagnes APT que nous avons évoquées cette année.

Carbanak a associé le cybercrime, dans ce cas le vol d'argent auprès d'institutions financières, aux techniques d'infiltration typiques d'une attaque ciblée. La campagne a été découverte au printemps 2015 : Kaspersky avait été invité à réaliser une enquête sur les systèmes d'une banque après que celle-ci s'était rendu compte que certains de ses DAB donnaient de l'argent de manière "aléatoire". La banque avait été infectée. Carbanak est une porte dérobée conçue pour réaliser des tâches d'espionnage, extraire des données et contrôler à distance les ordinateurs infectés. Les attaquants avaient compromis les victimes à l'aide de méthodes caractéristiques des menaces avancées persistantes, à savoir l'envoi de messages de harponnage aux employés de la banque. Une fois qu'ils avaient pu accéder à un ordinateur de la banque, les attaquants se livraient à des tâches de reconnaissance afin d'identifier les systèmes impliqués dans les opérations, la comptabilité et les DAB et ils se contentaient de reproduire les activités d'employés légitimes. Carbanak utilisait trois méthodes pour voler l'argent : (1) retrait d'argent liquide dans les DAB, (2) transfert d'argent aux cybercriminels via le réseau SWIFT et (3) création de faux comptes et recours aux mules pour récupérer l'argent. Les attaquants s'en sont pris à une centaine d'institutions financières et les pertes cumulées ont atteint près d'un milliard de dollars américains.




Un des sujets les plus marquants dans l'actualité du premier trimestre 2015 a concerné le groupe de cyber-espionnage Equation. Les attaquants à l'origine d'Equation avaient réussi à infecter les ordinateurs de milliers de victimes en Iran, en Russie, en Syrie, en Afghanistan, aux Etats-Unis et ailleurs dans le monde. Il y avait parmi elles des institutions gouvernementales et diplomatiques, des sociétés de télécommunication et des sociétés du secteur de l'énergie. Il s'agit d'une des campagnes APT les plus sophistiquées que nous avons jamais vue : un des nombreux modules développés par le groupe modifie le micrologiciel des disques dur, ce qui confère à cette attaque un niveau de furtivité et de persistance jamais atteint par les autres attaques. Les débuts du développement de ce code remontent à 2001, voire plus tôt. Celui-ci est lié à d'autres attaques qui ont fait parler d'elles comme Stuxnet et Flame : ainsi, son arsenal contenait des vulnérabilités de type 0jour qui ont été utilisées par la suite dans Stuxnet.

Au cours d'une enquête que nous réalisions sur un événement survenu au Moyen-Orient, nous avons mis à jour l'activité d'un groupe inconnu jusque là qui réalisait des attaques ciblées. Desert Falcons est le premier groupe arabophone à organiser des opérations de cyberespionnage complètes, visiblement liées à la situation politique de la région. Les premiers signes de cette campagne sont apparus en 2011. Les premières infections ont été enregistrées en 2013 et le pic de l'activité s'est produit à la fin de l'année 2014 et au début de l'année 2015. Le groupe a volé plus d'un million de fichiers auprès de plus de 3 000 victimes. Parmi ces victimes, nous retrouvons des activistes et des leaders politiques, des organisations gouvernementales et

militaires, des médias et des institutions financières établies principalement en Palestine, en Egypte, en Israël et en Jordanie. Il ne fait aucun doute que les membres du groupe Desert Falcon ne sont pas des débutants : ils ont développé des malwares pour Windows et Android à partir de zéro et ils ont organisé de mains de maître des attaques qui reposaient sur des messages de phishing, de faux sites Internet et de faux comptes de réseaux sociaux.

En mars 2015, nous avions publié un rapport sur la campagne APT Animal Farm alors que des informations relatives aux outils utilisés par cette campagne avaient commencé à filtrer l'année antérieure. En mars 2014, le journal français, Le Monde, publiait un article au sujet d'un kit d'outils de cyber-espionnage qui avait été identifié par le Centre de la sécurité des télécommunications (CST) du Canada : ce kit avait été utilisé dans le cadre de l'opération 'Snowglobe' menée contre les médias francophones au Canada, mais également en Grèce, en France, en Norvège et dans certains pays d'Afrique. Le CST estimait que l'opération avait été lancée par les services de renseignement français. Un an plus tard, des chercheurs sur les questions de sécurité ont publié des analyses (ici, ici et ici) de malwares qui partageaient beaucoup de points communs avec 'Snowglobe'. Ces recherches contenaient notamment des échantillons de code avec le nom interne 'Babar', le nom du programme mentionné par le CTS. Après l'analyse des malwares et des liens qui les unissaient, Kaspersky Lab a désigné groupe à l'origine de ces attaques sous le nom d'Animal Farm. Le groupe comptait dans son arsenal deux des trois vulnérabilités 0jours que nous avions trouvées en 2014 et qui avaient été exploitées par des cybercriminels. Par exemple, une attaque depuis le site Internet du ministère syrien de la Justice, compromis à l'aide de codes d'exploitation CVE-2014-0515 entraînait le téléchargement d'un outil d'Animal Farm appelé 'Casper'. Cette campagne se distingue par un élément curieux : NBOT, un de ces programmes, est conçu pour organiser des attaques DDoS (déni de service distribué). Ce n'est pas fréquent parmi les groupes APT. Un des membres de cette ménagerie malveillante porte l'étrange nom de 'Tafacalou', peut-être un mot occitan (un dialecte de la France et d'autres régions).

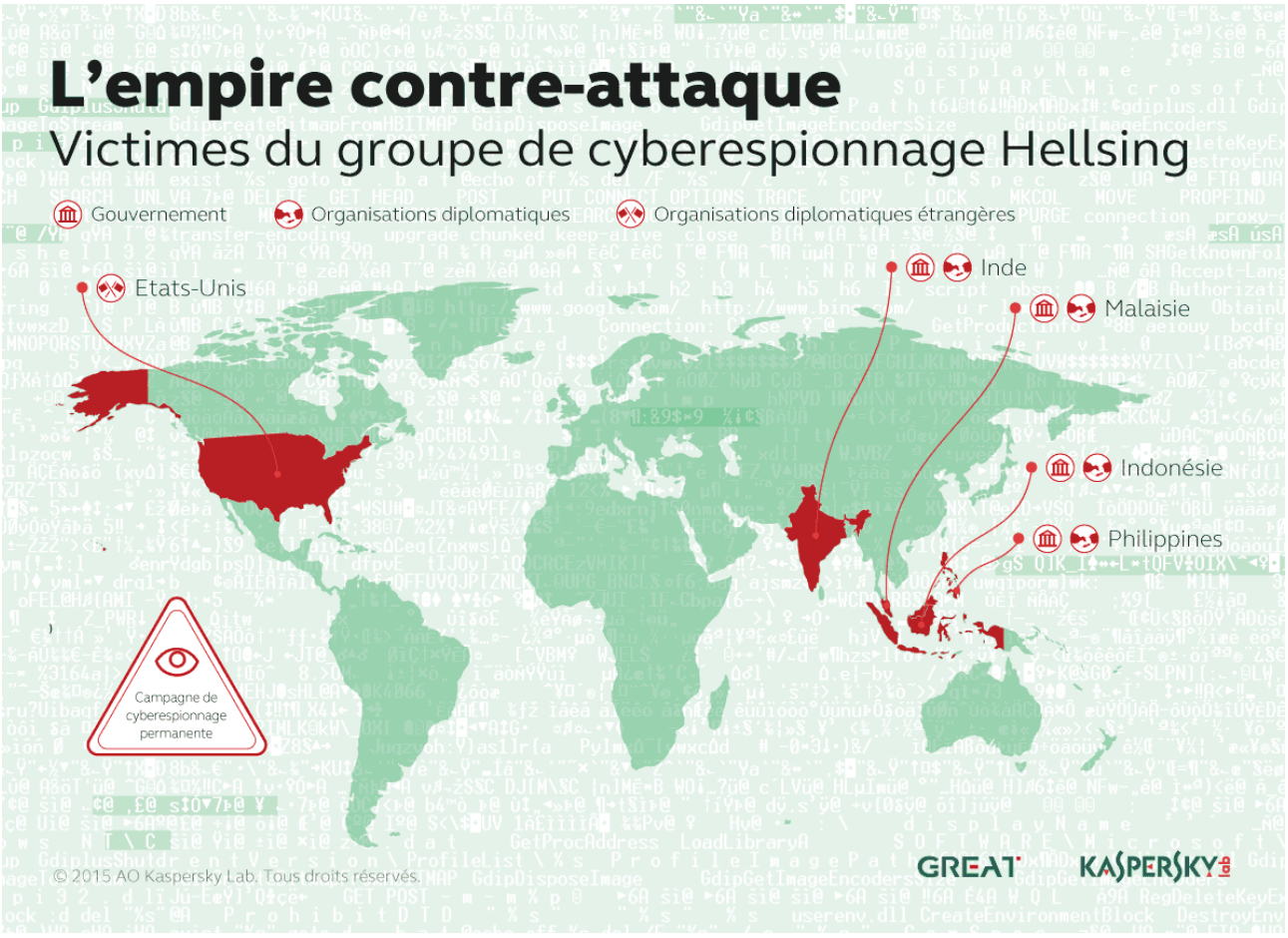
En avril 2015, nous avons publié un rapport sur un nouveau membre de la grande famille 'Duke' déjà composée de MiniDuke, CosmicDuke et OnionDuke. CozyDuke APT (connu également sous le nom 'CozyBear', 'CozyCat' et and 'Office Monkeys') cible des organisations gouvernementales et des entreprises aux Etats-Unis, en Allemagne, en Corée du Sud et en Ouzbékistan. L'attaque exploite une série de techniques de pointe, dont le chiffrement, des méthodes de lutte contre la détection et un ensemble bien développé de composants dont la structure évoque celle de menaces antérieures au sein de la famille 'Duke'. Ceci étant dit, ce groupe se distingue par son utilisation de l'ingénierie sociale. Certains des messages de harponnage envoyés par les attaquants contiennent un lien vers des sites piratés qui hébergent une archive ZIP. Certains de

ces sites sont des sites légitimes et de renom. Cette archive contient un fichier RAR SFX qui installe le malware tout en affichant un PDF vide en guise de leurre. Une autre technique employée consiste à envoyer de fausses vidéos Flash en tant que pièces jointes de message. Parmi un des exemples les plus frappants (auquel le malware doit un de ses noms), citons 'OfficeMonkeys LOL Video.zip'. Quand ce fichier est exécuté, il installe un exécutable CozyDuke sur l'ordinateur tandis qu'une vidéo "comique" de singes travaillant dans un bureau est présentée. Ce contenu encourage les victimes à faire circuler la vidéo auprès de leurs collègues, ce qui augmente le nombre d'ordinateurs infectés. Le recours à l'ingénierie sociale pour amener les membres du personnel à réaliser une action qui met en danger la sécurité de l'entreprise, que ce soit dans le cas de CozyDuke ou de nombreuses autres attaques ciblées, souligne l'importance que doit avoir la formation du personnel dans toute stratégie de sécurité d'une entreprise.

L'APT Naikon est exploité dans des campagnes menées contre des cibles sensibles en Asie du Sud-Est et autour de la mer de Chine. Il semblerait que les attaquants parlent chinois et qu'ils sont actifs depuis au moins cinq ans. Ils ciblent des organisations gouvernementales de haut niveau, ainsi que des organisations civiles et militaires aux Philippines, en Malaisie, au Cambodge, en Indonésie, au Vietnam, au Myanmar, à Singapour, au Népal, en Thaïlande, au Laos et en Chine. A l'instar de nombreuses autres attaques ciblées, Naikon exploite abondamment l'ingénierie sociale afin d'amener des employés des organisations ciblées à installer le malware. Le module principal est un outil d'administration à distance qui prend en charge 48 commandes conçues pour contrôler les ordinateurs infectés : il s'agit de commandes pour réaliser un inventaire complet, télécharger et charger des données, ajouter des modules complémentaires et utiliser des enregistreurs de frappes afin d'obtenir les informations d'identification des employés. Les attaquants affectaient à chaque pays ciblé un opérateur capable d'exploiter les particularités culturelles locales, par exemple la coutume d'utiliser des comptes de messagerie personnels pour le travail. Les opérateurs utilisaient également un serveur proxy spécifique au sein des frontières du pays afin de gérer les connections avec les ordinateurs infectés et de transmettre les données aux serveurs de commande des attaquants. Notre rapport principal et notre rapport de suivi sont disponibles sur notre site Internet.

Lors de nos travaux de recherche sur Naikon, nous avons détecté les activités du groupe APT Hellsing. Ce groupe visait principalement des organisations gouvernementales et diplomatiques établies en Asie. La majorité des victimes a été recensée en Malaisie et aux Philippines. Mais nous avons également observé des victimes en Inde, en Indonésie et aux Etats-Unis. Hellsing en lui-même n'est qu'un petit groupe de cyberespionnage qui n'affiche aucune prouesse technologique (une vingtaine d'organisations ont été ciblées par Hellsing). Ce qui le rend

intéressant, c'est sa décision de contre-attaquer après avoir été victime d'une attaque de harponnage orchestrée par le groupe APT Naikon. Le destinataire ciblé par le message avait contacté l'expéditeur pour mettre son authenticité en doute. Il avait alors reçu une réponse de l'attaquant, mais n'avait pas ouvert la pièce jointe. Par contre, il avait renvoyé un message aux attaquants avec son propre malware. Il ne fait aucun doute que le groupe Hellsing, après s'être rendu compte qu'il était ciblé, a voulu identifier les attaquants et récolter des renseignements à leur sujet. Ce n'est pas la première fois que nous voyons un groupe APT empiéter sur un autre, par exemple en volant le carnet d'adresses des victimes afin d'envoyer des messages à tous les membres de ces listes. Ceci étant dit, les attaques entre groupes ATP demeurent inhabituelles.




Nombreuses sont les campagnes ciblées qui visent de grandes entreprises, des agences gouvernementales ou d'autres organisations de haut niveau. Il est dès lors facile de croire, en lisant les journaux, que ces organisations sont les seules qui intéressent les auteurs d'attaques ciblées. Toutefois, une des campagnes que nous avions signalée au trimestre dernier montre clairement que les attaquants ne s'intéressent pas uniquement aux gros poissons. La campagne de cyber-espionnage Grabit vise à voler les données de petites et moyennes entreprises principalement en Thaïlande, au Vietnam et en Inde. Mais nous avons

également recensé des victimes aux Etats-Unis, aux Emirats arabes unis, en Turquie, en Russie, en Chine, en Allemagne et dans d'autres pays. La chimie, les nanotechnologies, l'éducation, l'agriculture, les médias et la construction figurent parmi les domaines d'activité ciblés. Selon nos estimations, le groupe à l'origine de ces attaques aurait voler près de 10 000 fichiers. Il ne fait aucun doute que toute entreprise est une cible potentielle, soit pour ses propres actifs, soit en tant que point d'accès vers une autre organisation.

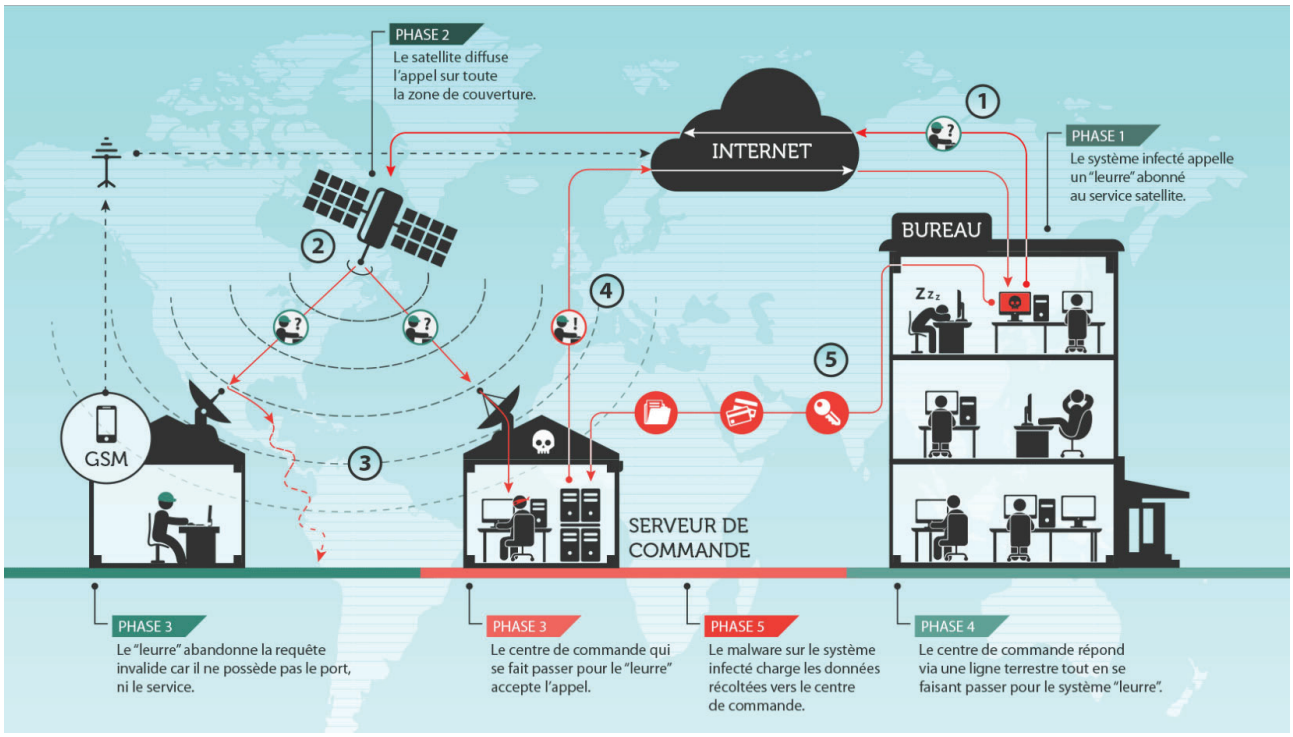
Au printemps 2015, lors d'une opération de nettoyage organisée dans ses installations, Kaspersky Lab a identifié une cyberintrusion qui touchait plusieurs de ses systèmes internes. L'enquête menée par la suite a permis de mettre à jour le développement d'une nouvelle plateforme malveillante par l'un des groupes APT les plus doués, les plus mystérieux et les plus puissants au monde : Duqu, parfois présenté comme le demi-frère de Stuxnet. Nous avons baptisé cette plateforme 'Duqu 2.0'. Dans le cas de Kaspersky Lab, l'attaque exploitait une vulnérabilité 0jour dans le noyau Windows (éliminée par Microsoft le 9 juin 2015) et peut-être deux autres (éliminées depuis lors) de type 0jour également à l'époque. Les attaquants cherchaient avant tout à espionner sur les technologies de Kaspersky Lab, les recherches en cours et les processus internes. Mais Kaspersky Lab n'était pas la seule cible. Certaines infections de Duqu 2.0 étaient liées aux événements P5+1 en rapport avec les négociations sur le programme nucléaire iranien : les attaquants semblaient avoir lancé des opérations sur les lieux de certains de ces pourparlers de haut niveau. Le groupe avait également lancé une attaque similaire en rapport avec la commémoration du 70e anniversaire de la libération du camp d'Auschwitz-Birkenau. Une des principales caractéristiques de Duqu 2.0 était son manque de persistance : il ne laissait pratiquement aucune trace dans le système. Le malware n'introduisait aucune modification dans les paramètres du disque ou du système : la plateforme malveillante avait été conçue de telle sorte qu'elle survivait presqu'exclusivement dans la mémoire des systèmes infectés. Ceci laisse penser que les attaquants avaient confiance en leur capacité à maintenir leur présence dans le système, même si l'ordinateur d'une victime était redémarré et que le malware était effacé de la mémoire. Le dossier technique Duqu 2.0 et l'analyse du module de persistance sont disponibles sur notre site Internet.

Nous avons abordé l'attaque APT Blue Termite au mois d'août. Cette campagne ciblée a pour objectif le vol d'informations d'organisations au Japon. Il s'agit d'agences gouvernementales, d'organismes publics régionaux, de groupes d'intérêt public, d'universités, de banques, de services financiers, ainsi que d'entreprises actives dans les secteurs de l'énergie, des communications, de l'industrie lourde, de la chimie, de l'automobile, de l'électricité, des médias, des services d'information, de la santé, de l'immobilier, de l'alimentaire, des semi-conducteurs, de la robotique, de la construction, des assurances, du transport et autres. L'administration

des retraites du Japon figure parmi les victimes qui ont fait couler le plus d'encre. Le malware est adapté en fonction de chaque victime. La backdoor de Blue Termite stocke toutes les données qui la concernent, dont le centre de commande, le nom API, les chaînes contre l'analyse, les valeurs des exclusions mutuelles, ainsi que la somme de contrôle MD5 des commandes de la backdoor et les informations du proxy interne. Les données sont stockées sous forme chiffrée, ce qui complique l'analyse du malware. Chaque échantillon requiert une clé de déchiffrement unique. A l'instar de nombreuses autres attaques ciblées, les messages de harponnage constituent la principale méthode d'infection. Nous avons toutefois détecté d'autres méthodes. Il y a notamment des attaques par téléchargement de type drive-by à l'aide d'un code d'exploitation Flash (CVE-2015-5119), un des codes d'exploitation divulgués après l'incident de sécurité impliquant de Hacking Team – qui ont permis d'infecter plusieurs sites Internet Japonais. Nous avons également observé des attaques impliquant la technique du trou d'eau, dont un sur le site Internet d'un membre de haut niveau du gouvernement japonais.

Le groupe qui se cache derrière la campagne de cyber-espionnage Turla est actif depuis plus de huit ans (notre rapport initial, notre analyse de suivi et notre présentation de la campagne sont disponibles sur securelist.com), et il a infecté des centaines d'ordinateurs dans plus de 45 pays. Les attaquants identifient leurs victimes à l'aide d'attaques qui reposent sur la technique du trou d'eau au cours des premières étapes. Toutefois, comme nous l'avons indiqué dans notre rapport le plus récent, le groupe exploite les communications par satellite pour gérer le trafic de ses centres de commande. La méthode choisie par le groupe Turla pour détourner les connexions satellites descendantes ne requiert pas d'abonnement valide à un service d'accès à Internet par satellite. L'avantage principal est l'anonymat offert : il est très difficile d'identifier les attaquants. Les récepteurs du signal satellite peuvent se trouver n'importe où dans la zone de couverture, en général assez grande, et il est très difficile d'identifier l'emplacement exact du serveur de commande et de saisir le matériel. Cela revient également moins cher que d'acheter une liaison satellite et la démarche est plus simple que le détournement du trafic entre la victime et l'exploitant du satellite et l'injection de paquets en cours de route. Le groupe Turla semble se concentrer sur les fournisseurs d'accès Internet par satellite au Moyen-Orient et en Afrique, dont le Congo, le Liban, la Libye, le Niger, le Nigeria, la Somalie et les Emirats arabes unis. Les diffusions par satellite dans ces pays n'atteignent pas en général les pays d'Europe et d'Amérique du Nord, ce qui complique énormément la tâche des chercheurs en sécurité qui voudraient analyser ces attaques. Le recours à des liaisons Internet par satellite constitue un développement intéressant. Le détournement de la bande passante descendante ne coûte pas cher (environ 1 000 dollars d'investissement initial, puis près de 1 000 dollars pour l'entretien annuel), il est facile à mettre en œuvre et garantit un degré d'anonymat élevé. D'un autre côté, il n'est pas toujours

aussi fiable que les méthodes plus traditionnelles comme l'hébergement "bullet-proof", plusieurs niveaux de proxy ou les sites Internet piratés, qui sont d'autres techniques utilisées par Turla. Il est moins probable que cette méthode soit utilisée pour maintenir de grands réseaux de zombies. Toutefois, si cette méthode devait se propager parmi les groupes APT ou les cybercriminels, elle poserait un grave problème au secteur de la sécurité de l'information et aux autorités judiciaires et policières.




En août 2015, nous avons publié une mise à jour sur l'APT Darkhotel. Ces attaques se caractérisaient au départ par l'utilisation détournée de certificats volés, le déploiement de fichiers HTA à l'aide de diverses méthodes et l'infiltration des réseaux Wi-Fi des hôtels pour installer des backdoors sur les ordinateurs des victimes.

Alors que ces méthodes sont toujours adoptées par les attaquants, on notera des nouveautés dans l'arsenal, dont une plus grande attention portée au harponnage des victimes sélectionnées. En plus de l'utilisation de fichiers HTA, les attaquants déploient également des fichiers RAR et utilisent le mécanisme RTLO (forcer l'écriture de droite à gauche) pour masquer la véritable extension du fichier. Les attaquants utilisent aussi des codes d'exploitation Flash, y compris un code d'exploitation 0jour diffusé suite à l'atteinte à la sécurité qui a frappé Hacking Team. Le groupe a étendu sa présence et inclut désormais des victimes en Corée du Nord, en Russie, en Corée du Sud, au Japon, au Bangladesh, en Thaïlande, en Inde, au Mozambique et en Allemagne.

# FUITES DE DONNÉES

Les atteintes à la sécurité des données n'ont pas manqué au cours de cette année. Il n'y a malheureusement rien d'étonnant à ce que ces événements deviennent routiniers : les données personnelles sont un bien précieux, non seulement pour les sociétés sérieuses, mais également pour les cybercriminels. Parmi les événements les plus retentissants de cette année, il faudra retenir les attaques menées contre Anthem, LastPass, Hacking Team, l'Office of Personnel Management des Etats-Unis, Ashley Madison, Carphone Warehouse, Experian and TalkTalk. Certaines de ces attaques ont débouché sur le vol d'imposants volumes de données, ce qui a souligné les lacunes de nombreuses entreprises en matière de protection. La sécurité ne peut se limiter au seul périmètre de l'entreprise. La sécurité absolue est un leurre et il est impossible de garantir qu'un système ne sera pas piraté, surtout si une personne au sein de l'entreprise est amenée par une ruse à réaliser une action qui met en danger la sécurité de l'entreprise. Ceci étant dit, toute organisation qui détient des données personnelles se doit d'adopter des mesures de protection efficace. Celles-ci doivent prévoir notamment le hachage et le salage des mots de passe des clients et le chiffrement d'autres données sensibles.

De leur côté, les clients peuvent limiter les dégâts liés à une éventuelle atteinte à la sécurité chez un prestataire en ligne en veillant à toujours utiliser des mots de passe uniques et complexes : le mot de passe idéal compte au moins 15 caractères et doit être composé de lettres, de chiffres et de symbole de l'ensemble du clavier. Il est possible d'utiliser une application de gestion des mots de passe qui s'occupera automatiquement de l'ensemble de ces détails.

La problématique des mots de passe refait surface de manière cyclique. Si les mots de passe que nous choisissons sont trop faciles à deviner, nous nous exposons au vol d'identité. Le danger augmente si nous utilisons le même mot de passe pour plusieurs comptes. Dès qu'un compte est compromis, tous les autres sont en danger. C'est la raison pour laquelle de nombreux prestataires de service, dont Apple, Google et Microsoft, proposent désormais un système d'authentification à deux facteurs. Autrement dit, les clients doivent saisir un code généré par un token ou envoyé à un appareil mobile pour pouvoir accéder au site, ou du moins pour modifier les paramètres du compte. Certes, l'authentification à deux facteurs améliore la sécurité, mais uniquement si elle est obligatoire et non pas facultative.

Le vol de données personnelles peut avoir de graves conséquences pour les personnes touchées. Parfois, les répercussions sont plus graves : l'atteinte à la sécurité chez Hacking Team a par exemple entraîné la publication de 400 Go de données. Parmi celles-ci, des codes d'exploitation utilisés par la société italienne dans son logiciel de surveillance. Certains de ces codes d'exploitation ont été utilisés dans des attaques APT comme Darkhotel et Blue Termite. Bien entendu, cet incident a été suivi d'une course-panique pour éliminer les vulnérabilités exposées par les attaquants.

# APPAREILS INTELLIGENTS (MAIS PAS FORCÉMENT SÛRS)

Internet est désormais incontournable dans notre vie quotidienne. Sa présence se manifeste dans un nombre croissant d'objets domestiques présents dans les foyers d'aujourd'hui. On ne compte plus les téléviseurs, les compteurs, les dispositifs de surveillance pour bébés, les bouloirs, etc dits "intelligents". Vous vous souviendrez peut-être de l'article publié l'année dernière par un de nos chercheurs en sécurité qui avait analysé sa propre demeure, afin de voir si elle était vraiment à l'abri des menaces cybernétiques. Nous vous proposons ici un suivi de cette recherche. Ceci étant dit, l'Internet des objets ne se limitent pas à l'électroménager.

Cela fait quelques années par exemple que les chercheurs se penchent sur les risques potentiels associés aux véhicules connectés. En juillet 2014 Kaspersky Lab et IAB ont publié une étude qui portait sur les problèmes potentiels que pouvaient présenter les véhicules connectés. Jusqu'à cette année, les chercheurs s'intéressaient plus particulièrement à la possibilité d'accéder aux systèmes du véhicule via une connexion physique. Ce point de vue a changé après que les chercheurs Charlie Miller et Chris Valasek ont trouvé un moyen d'accéder aux systèmes critiques d'une Jeep Cherokee via une connexion sans fil. Ils avaient réussi à prendre les commandes du véhicule et provoquer une sortie de route. (L'article est accessible ici).

Cet incident souligne quelques-uns des problèmes liés aux appareils connectés qui vont au-delà du secteur automobile et qui touchent n'importe quel appareil connecté. Malheureusement, les fonctions de sécurité sont difficiles à vendre ; sur un marché concurrentiel, tout ce qui simplifie la vie du client a priorité. De plus, la connectivité est souvent ajoutée à un réseau de communication préexistant qui avait été mis en place sans penser à la sécurité. Et l'Histoire nous montre que la sécurité est parfois introduite après qu'un événement sérieux a souligné l'impact de la faiblesse de la sécurité. Si vous souhaitez en savoir plus sur le sujet, nous vous invitons à lire un billet d'Eugène Kaspersky publié suite à la recherche décrite ci-dessus.

Ces problèmes concernent également les 'villes intelligentes'. Par exemple, au cours de ces dernières années, les gouvernements et les autorités judiciaires et policières ont favorisé le déploiement de systèmes de vidéosurveillance dans les lieux publics pour garantir notre sécurité. De nombreuses caméras de vidéosurveillance établissent une connexion sans fil à Internet, ce qui permet aux autorités de les surveiller à distance. Mais ces connexions ne sont pas forcément sécurisées : des cybercriminels pourraient observer passivement les images des caméras de sécurité,

injecter un code dans le système afin de remplacer les images d'une caméra par d'autres, voire mettre le système hors ligne. Vasilios Hioureas de chez Kaspersky Lab et Thomas Kinsey de chez Exigent Systems ont réalisé récemment un travail sur les faiblesses potentielles au niveau de la sécurité des systèmes de vidéosurveillance d'une ville. Le rapport de Vasilios Hioureas est disponible sur notre site Internet).

Malheureusement, aucun effort n'avait été réalisé pour masquer les caméras, si bien que les chercheurs ont pu définir la marque et le modèle, étudier leurs caractéristiques techniques et recréer leur propre réseau en laboratoire. Le matériel utilisé fournissait des contrôles de sécurité efficaces, mais encore aurait-il fallu qu'ils soient mis en œuvre. Les paquets de données envoyés via le réseau maillé n'étaient pas chiffrés. Cela signifie qu'un attaquant pouvait créer sa propre version du logiciel et manipuler les données en transit. Des attaquants pourraient exploiter cette faille en envoyant de fausses images aux opérateurs du centre de contrôle pour faire croire à un incident dans un lieu donné, ce qui créerait une diversion pendant que le véritable incident se déroule dans un autre quartier.

Les chercheurs ont signalé ces problèmes aux autorités responsables des systèmes de vidéosurveillance dans le monde réel et ces dernières sont occupées à éliminer les problèmes de sécurité. En règle générale, il est important de respecter les points suivants dans ce genre de réseau : il faut utiliser le chiffrement WPA, protégé par un mot de passe robuste ; les étiquettes doivent être retirées du matériel afin de priver les attaquants éventuels d'une source d'informations sur le fonctionnement du matériel ; les images transmises doivent être chiffrées quand elles transitent sur le réseau.

Ce qu'il faut retenir ici, c'est que le numérique intervient de plus en plus souvent dans notre vie de tous les jours : si la sécurité n'est pas mise en œuvre dès l'étape de la conception, les dangers potentiels peuvent avoir de sérieuses conséquences. Qui plus est, l'intégration a posteriori des mesures de sécurité n'est pas toujours évidente. L'initiative Securing Smart Cities qui bénéficie de l'appui de Kaspersky Lab vise à aider les développeurs de cités intelligentes à ne pas perdre de vue les questions de cybersécurité.

# COOPÉRATION INTERNATIONALE DANS LA LUTTE CONTRE LA CYBERCRIMINALITÉ

La cybercriminalité est bel et bien implantée. Elle se nourrit de nos activités en ligne de plus en plus nombreuses. Les statistiques officielles le confirment. Ainsi, l'Office for National Statistics du Royaume-Uni inclut désormais la cybercriminalité dans ses évaluations des taux de criminalité et tient compte ainsi des changements de la nature du crime dans nos sociétés. Il ne fait aucun doute que la cybercriminalité peut rapporter beaucoup d'argent, mais les cybercriminels n'échappent pas toujours à la justice. Les actions menées par les autorités judiciaires et policières à travers le monde peuvent avoir un impact significatif. La coopération internationale est particulièrement cruciale au vu du caractère transfrontalier de la cybercriminalité. Cette année aura été marquée par quelques opérations retentissantes sur ce terrain.

Au mois d'avril, Kaspersky Lab a participé à une opération visant à mettre le réseau de zombies Simda hors d'état de nuire. Cette opération était coordonnée par le Complexe mondial Interpol pour l'innovation. L'enquête avait été lancée par Microsoft, avant d'impliquer d'autres participants dont Trend Micro, le Cyber Defense Institute, des membres de la NHTCU des Pays-Bas (brigade nationale de lutte contre les délits technologiques), du FBI, de la police grand-ducale section Nouvelles technologies du Luxembourg et du bureau "K" de lutte contre la cybercriminalité du ministère russe de l'Intérieur, avec le bureau central national d'Interpol à Moscou. L'opération avait débouché sur la mise hors service de 14 serveurs aux Pays-Bas, aux Etats-Unis, au Luxembourg, en Pologne et en Russie. Les premières analyses des journaux des serveurs neutralisés via la méthode du sink-hole avaient indiqué que le réseau de zombies avait touché 190 pays.

En Septembre, la police des Pays-Bas a arrêté deux hommes soupçonnés de participer aux attaques du ransomware CoinVault. Cette arrestation était le fruit d'une coopération entre Kaspersky Lab, Panda Security et la brigade nationale de lutte contre les délits technologiques (NHCTU) des Pays-Bas. Cette campagne de malware a débuté en mai 2014 et s'est poursuivie cette année. Elle a ciblé des victimes dans plus de 20 pays, principalement aux Pays-Bas, en Allemagne, aux Etats-Unis, en France et en Grande-Bretagne. Les auteurs avaient réussi à chiffrer des fichiers sur plus de 1 500 ordinateurs Windows et ils exigeaient un paiement en bitcoins pour déchiffrer les données. Les cybercriminels à l'origine de cette campagne ont modifié le ransomware à plusieurs reprises pour s'en prendre sans cesse à de nouvelles victimes. En novembre 2014, Kaspersky Lab et la brigade nationale de lutte contre les délits

technologiques (NHCTU) des Pays-Bas ont lancé un site Internet pour l'hébergement des clés de déchiffrement ; nous avons également mis un outil de déchiffrement en ligne à la disposition des victimes pour les aider à récupérer leurs données sans devoir payer la rançon. Ne manquez pas de lire notre analyse des différentes astuces employées par les auteurs de CoinVault. Les ransomwares sont devenus des habitués de la scène des menaces. S'il est vrai que ce cas illustre les résultats positifs que peut donner la coopération entre les chercheurs et les autorités judiciaires et policières, il est essentiel que les consommateurs et les entreprises adoptent les mesures pour atténuer les risques que pose ce genre de malware. Les cybercriminels qui utilisent les ransomwares vivent des victimes qui paient. En septembre, un agent du FBI a créé la polémique en affirmant que les victimes devraient payer la rançon afin de récupérer leurs données. On peut reconnaître le pragmatisme de la solution, ne serait-ce que pour le simple fait qu'il n'existe parfois aucun autre moyen de récupérer les données, mais cette stratégie est dangereuse. Tout d'abord, rien ne garantit que les cybercriminels fourniront bel et bien les mécanismes de déchiffrement des données après avoir reçu la rançon. Ensuite, cela conforte leurs opérations et favorise la poursuite du développement des ransomwares. Nous préférons conseiller aux entreprises et aux particuliers de réaliser des copies de sauvegarde régulières de leurs données afin de ne pas avoir à décider de payer ou non la rançon.

# ATTAQUES CONTRE DES INFRASTRUCTURES INDUSTRIELLES

Les incidents touchent des infrastructures industrielles en raison de problème de cybersécurité sont assez fréquents. Par exemple, d'après les données de l'US ICS CERT, 245 incidents de ce genre ont été recensés au cours de l'année financière 2014. Pour la période allant de juillet à août 2015, ce chiffre s'élève à 22. Toutefois, nous estimons que ce chiffre ne reflète pas la réalité : le nombre de cyberincidents est beaucoup plus élevé. Et si les exploitants et les propriétaires d'entreprises préfèrent simplement passer sous silence une partie des incidents, il en existe une autre dont ils ne soupçonnent même pas l'existence.

Nous souhaiterions revenir sur deux incidents qui ont attiré notre attention en 2015.

Le premier s'est déroulé dans une usine sidérurgique en Allemagne. A la fin de l'année 2014, le Service fédéral allemand pour la sécurité de l'information (Bundesamt für Sicherheit in der Informations technik, BSI) a diffusé un communiqué de presse (le document est disponible en allemand, cf. l'annexe en anglais) qui décrivait un incident survenu dans une usine sidérurgique en Allemagne. Cet incident avait provoqué des dégâts au haut fourneau.

Il s'agit du deuxième cas de cyberattaque, après Stuxnet, ayant entraîné des dégâts matériels à l'équipement. D'après des représentants du BSI, l'attaque avait débuté par l'infection du réseau informatique des bureaux de l'entreprise via une campagne de phishing. Une fois à l'intérieur du réseau, les hackers avaient réussi à infecter un ordinateur SCADA et lancer l'attaque contre le matériel. Malheureusement, le BSI n'a offert aucun détail complémentaire et nous ne savons pas comment le malware a été utilisé, ni comment il fonctionne.

Cette volonté de maintenir le secret n'arrange pas tout le monde. Les exploitants d'usines similaires (et pas seulement en Allemagne) ne peuvent pas étudier l'attaque et adopter des contre-mesures, les experts en cybersécurité sont également maintenus à l'écart et ne peuvent pas développer de solutions pour leurs clients.

L'autre cas qui a attiré notre attention fut l'attaque menée contre l'aéroport Frédéric Chopin de Varsovie en juin 2015. Un week-end, le système électronique de préparation des plans de vol de la compagnie aérienne polonaise LOT a été mis hors service pendant 5 heures. D'après Reuters, cet incident avait provoqué le retard de dizaines de vols.

La direction de l'aéroport n'avait fourni aucune information et les experts se sont prononcés uniquement sur la base de leur expérience. Ruben Santamarta, conseiller principal de la société IOActive spécialisé en sécurité, s'était déjà intéressé à la problématique de la sécurité de l'information dans l'aviation. Sur la base de déclarations de représentants de LOT, il avait supposé que la compagnie avait été victime d'une attaque ciblée : le système n'avait pas été en mesure de créer les plans de vol, soit parce que des nœuds clés du back office avaient été compromis, soit parce que l'attaque avait visé les dispositifs de communication au sol et avait empêché le chargement et la validation des données dans les ordinateurs de bord (y compris les plans de vol).

Nos experts s'étaient également exprimé sur le sujet : d'après leurs hypothèses, il existait deux autres scénarios potentiels pour expliquer ces attaques. L'incident aurait pu être le résultat d'un facteur humain ou d'une panne d'équipement. Ou l'attaque contre l'aéroport relativement petit de Varsovie n'était qu'une répétition générale avant des actions plus ambitieuses d'individus malintentionnés contre d'autres aéroports importants à travers le monde.

Plus tard, une déclaration officielle allait annoncer que l'incident avait été provoqué par une attaque DDoS et qu'il n'y avait eu aucune intrusion dans le système. Ici aussi, aucun détail n'est communiqué et le seul choix qu'il nous reste est soit de croire la version officielle, soit d'élaborer des hypothèses sur les causes et les objectifs véridiques de l'attaque.

Quelle que soit l'identité des auteurs des attaques que nous venons d'évoquer et quel que soit leur objectif, ces deux exemples nous rappellent avec force à quel point l'informatique s'est intégrée à nos vies et à quel point les infrastructures sont devenues de plus en plus vulnérables au fil des années.

Malheureusement, de nombreux gouvernements et régulateurs préfèrent imposer le secret en la matière. Quant à nous, nous estimons que la transparence et l'échange d'informations relatives aux cyberattaques sont deux éléments essentiels à l'élaboration d'une protection adéquate des implantations industrielles car sans ses informations, il est difficile se de préparer aux menaces de demain.

En guise de conclusion, nous aimerions évoquer une autre tendance qui a déjà ou qui aura au cours des prochaines années un impact sur chacun d'entre nous : le matériel utilisé dans les usines est de plus en plus souvent connecté à Internet. L'Internet a été inventé il y a longtemps et voici qu'il fait son apparition dans les processus industriels. On peut parler sans exagération d'une nouvelle révolution industrielle : nous assistons à la naissance de l'Internet des objets industriel ou de l'Entreprise 4.0. Les entreprises peuvent en tirer de nombreux avantages et améliorer la productivité.

Pour ne pas rater le coche, les fabricants d'équipement se contentent d'ajouter des capteurs et des dispositifs de commande au matériel fiable qui a fait ses preuves, développé à une époque où Internet n'existait pas. Ils connectent ensuite l'appareil à Internet et obtiennent un "nouvel équipement". Mais ils oublient que l'ajout de fonctions qui permettent à un appareil quelconque de se connecter à Internet engendre de nouveaux risques et menaces liés à la cybercriminalité. Il ne s'agit plus d'un appareil "physique", mais bien "cyberphysique".

Dans le monde des appareils physiques, l'ensemble des appareils, des outils, des protocoles de communication, etc. a été mis au point en mettant l'accent sur la sécurité fonctionnelle. Ils sont à l'"épreuve des idiots". Cela signifie qu'un appareil développé selon cette logique ne doit connaître aucun dysfonctionnement, ni provoquer de dégâts matériels ou écologiques s'il est utilisé dans le respect des mesures de sécurité.

L'entreprise 4.0 hérite d'une nouvelle dimension dans la sécurité : la sécurité de l'information ou la sécurité contre une intervention extérieure non sollicitée. On ne peut pas se contenter de tout simplement connecter à Internet un objet ou un appareil "d'avant Internet" car les conséquences d'une telle connexion pourraient être malheureuses.

Les ingénieurs, nourris par les anciens principes "pré-révolutionnaires", oublient souvent que leur appareil pourrait être "utilisé" non seulement par un ingénieur qui connaît les limites de l'appareil en question, mais également par un hacker qui ne maîtrise pas du tout la notion "d'action non autorisée avec un objet distant". C'est une des principales raisons pour laquelle les sociétés riches d'une expérience et d'une tradition produisent du matériel de qualité et qui adhère au principe de sécurité fonctionnelle mais qui ne garantit pas un niveau suffisant de cybersécurité pour l'entreprise.

Dans le monde des appareils cyberphysiques, les composantes cybernétiques et physiques sont étroitement liées. Une cyberattaque peut mettre un processus technique hors service, endommager le matériel, voire provoquer une catastrophe technologique. Les hackers représentent une menace réelle et tout ce qui est connecté à Internet peut être attaqué. C'est la raison pour laquelle les fabricants doivent prévoir des mesures de protection contre les cybermenaces aussi soignées que les mesures qui garantissent la sécurité fonctionnelle lorsqu'ils développe un nouvel équipement industriel qui sera connecté.

# CONCLUSION

En 2015, la problématique de la protection des réseaux et de la sécurité sur Internet a été abordée dans tous les secteurs d'activité économique ainsi que dans la vie de tous les jours. C'est une première dans l'histoire d'Internet. Vous pouvez choisir n'importe quel secteur, qu'il s'agisse des finances, de l'industrie, de l'automobile, de l'aviation, des périphériques portables, de la santé et de bien d'autres encore, et vous trouverez sans aucune difficulté un article publié cette année au sujet d'incidents ou de problèmes liés à la cybercriminalité dans le secteur en question.

Malheureusement, la cybersécurité est désormais associée au terrorisme. Les méthodes d'attaque et de défense sur Internet intéressent énormément les groupuscules et structures illégales les plus diverses.

Les questions de cybersécurité sont désormais débattues aux échelons les plus hauts de la diplomatie et des gouvernements. Ainsi, des accords sur la cybersécurité ont été conclus cette année entre la Russie et la Chine, entre la Chine et les Etats-Unis ou entre la Chine et le Royaume-Uni. Dans le cadre de tels accords, les Etats s'engagent non seulement à coopérer, mais également à s'abstenir de s'attaquer entre eux. L'Arrangement de Wassenaar sur la limitation des exportations des logiciels espion a également fait l'objet de nombreux débats. L'un des sujets qui aura fait le plus parler de lui cette année aura été l'utilisation de services de messagerie non protégés par des hommes et des femmes politiques à travers le monde, dont Hillary Clinton, l'ex-Secrétaire d'Etat des Etats-Unis (toujours en fonction au moment des faits).

Cela a entraîné un regain d'intérêt pour la problématique de la cybersécurité non seulement dans les médias, mais également dans l'industrie du loisir : des films et des séries ont été tournés, certains experts dans le domaine de la cybersécurité ont été invité à jouer un rôle, parfois le leur.

Le fait que le mot "cybersécurité" soit devenu courant en 2015 ne signifie pas que les problèmes ont été résolus. Nous observons une croissance exponentielle de tout ce qui est lié à la cybersécurité : augmentation du nombre d'attaques, d'attaquants, de victimes, des budgets de protection, des lois et des accords qui régissent ou établissent de nouvelles normes. D'après nous, tout ceci s'explique par la complexité des attaques dévoilées. La résistance s'est activée, mais il lui faudra encore beaucoup de temps pour atteindre la maturité.

Nous avons dressé un panorama de l'avenir dans nos prévisions pour 2016.

Viruslist, la ressource pour la recherche technique, les analyses et réflexions des experts Kaspersky Lab.

Suivez-nous

Site Kaspersky Lab

Blog Eugène Kaspersky

Blog Kaspersky Lab B2C

Blog Kaspersky Lab B2B

Service info sécurité Kaspersky Lab

Académie Kaspersky Lab

Twitter.com/
kasperskyfrance

Facebook.com/
kasperskylabfrance

AO Kaspersky Lab, Rueil, France
www.kaspersky.fr

Informations sur la sécurilté online :
www.viruslist.com/fr
www.kaspersky.fr/entreprise-securite-it/

Informations sur les partenaires proches de chez vous :
http://www.kaspersky.fr/partners