Bilan Cert-IST 2016 des failles et attaques

1. Introduction

Comme chaque année, le Cert-IST propose un bilan de l'année écoulée afin de mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Nous présentons dans un premier temps une rétrospective des événements les plus marquants de l'année 2016 (cf. chapitre 2). Ces évènements sont pour nous les menaces les plus importantes pour les entreprises.

Nous fournissons ensuite un récapitulatif des différentes productions du Cert-IST au cours de cette année (cf. chapitre 3).

La conclusion (cf. chapitre 4) donne une synthèse du paysage actuel de la cyber-menace et des challenges auxquels les entreprises doivent faire face.

➢ A propos du Cert-IST

Le Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam - **I**ndustrie, **S**ervices et **T**ertiaire) est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises. Créé en 1999, il aide ses adhérents à identifier les menaces en analysant quotidiennement les nouvelles vulnérabilités, leurs criticités et les moyens de protection pour y répondre. En cas d'incident de sécurité touchant l'un de ses adhérents, le Cert-IST peut apporter son aide dans l'investigation de cet incident et permettre une remise en service opérationnelle et sécurisée.

Nota : Les encadrés bleus insérés tout au long du bilan sont extraits de publications rédigées par le Cert-IST au cours de l'année.

2. Les événements les plus marquants de 2016

2015 fut l'année de l'émergence et de la médiatisation des rançongiciels. 2016 a confirmé la tendance grandissante de cette menace, les rançongiciels étant devenus peu à peu le principal type de malware utilisé pour les attaques de masse. Malgré l'insolent succès de ces attaques à destination de l'utilisateur final et du poste de travail, les attaques visant les infrastructures (serveurs et réseaux) ne diminuent pas pour autant. 2016 est même l'année de tous les records, que ce soit en termes d'attaques par déni de service ou de vol de données personnelles.

En parallèle, les attaques ciblées (type APT) visant les entreprises et l'espionnage d'état semblent se porter toujours aussi bien. Dans ce cadre que beaucoup qualifient depuis quelques années de cyberguerre, l'attribution des attaques à tel ou tel pays va bon train, alors que l'obtention de preuves formelles en la matière est très difficile. Pourtant, gouvernements, lanceurs d'alertes, chercheurs et journalistes, se livrent souvent à ce jeu périlleux, offrant un terrain d'expression idéal pour les gouvernements et partis politiques du monde entier.

2.1. Le vol de données encore en constante évolution

L'actualité 2016 a été marquée par un nombre sans précédent d'annonces de vol massif de données personnelles. Le constat est simple aujourd'hui : tous les sites peuvent être victimes d'attaques et même les plus sérieux d'entre eux sont vulnérables.

En tête du classement se trouve Yahoo. Mi-septembre 2016, le géant américain confirme avoir subi en 2014 un vol de plus de 500 millions de comptes utilisateurs. Ce n'est que mi-décembre que la société a annoncé la compromission d'un milliard de comptes supplémentaires suite à une attaque survenue en août 2013.

Au mois d'octobre 2016, ce sont plusieurs sites de rencontres pour adultes appartenant au réseau FriendFinder Networks qui sont victimes de vol de données, avec près de 412 millions de comptes compromis.

Au mois de mai 2016, le réseau MySpace confirme le vol de 360 millions de comptes, mots de passe et adresses mail. Ce piratage concernerait les comptes créés avant le 11 juin 2013 d'après le communiqué MySpace. Le même mois, le site MotherBoard révèle le piratage de 117 millions de comptes Linkedin, revendus sur le dark web pour 5 bitcoins (environ 2 200 $).

Hormis ces vols massifs et particulièrement médiatisés, de nombreux autres sites ont vu leurs données dérobées tout au long de l'année 2016 : VK (100 millions) en juin, Dailymotion (85 millions) en octobre, Twitter (71 millions) en juin, Dropbox (68 millions) en aout, Tumblr (65 millions) en mai…

On imagine assez aisément l'intérêt de ce type de données pour les hackers. En les revendant sur le dark web sur des sites tels que TheRealDeal, à des prix relativement faibles (par exemple le hacker « Peace_of_Mind » revend 1 600 €, 200 millions de comptes Yahoo!, environ 2200$ pour 117 millions de comptes Linkedin ou encore 150$ pour 68 millions de comptes Tumblr), il devient facile pour les hackers d'engranger des bénéfices. On se rend bien compte de l'intérêt de nos données personnelles pour ces acteurs malveillants, même si leur prix à l'unité est dérisoire. C'est en fait le piratage massif de ces données qui est véritablement lucratif, les réseaux sociaux et autres acteurs du Big Data constituant des cibles idéales.

2.2. Attaques bancaires, le réseau SWIFT en ligne de mire

C'est au mois de février que le réseau bancaire SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) a été attaqué, et c'est la banque centrale du Bangladesh qui a été la première victime connue de ce cyber-casse.

Pour comprendre comment les hackers ont procédé, il faut remonter à mai 2015, lorsque 4 comptes bancaires ont été ouverts sous de de fausses identités auprès de la RCBC (Rizal Commercial Banking Corporation) aux Philippines. Ces comptes serviront aux hackers de destination finale pour l'argent dérobé.

Le 4 et 5 février 2016, 35 transferts SWIFT, représentant près de 950 millions de dollars, sont réalisés à la demande de la banque du Bangladesh. La FED refuse 30 de ces demandes car le formatage du message pour le système SWIFT n'est pas correct. C'est au final un ordre de virement de 20 millions de dollars donné vers la Shalika Foundation et transitant par la Deutsche Bank qui attire l'attention d'un employé et qui permettra certainement de découvrir le pot aux roses. D'après Reuters, une faute d'orthographe s'est glissée dans le nom du destinataire (« Shalika fandation » au lieu de « Shalika foundation »), qui est d'ailleurs une organisation inexistante.

Malheureusement, en faisant les comptes, ce sont quand même 4 transferts, représentant près de 80 millions de dollars qui ont été autorisés vers des comptes de casinos philippins avant de disparaitre.

En mai 2016, c'est la banque TPBank située à Hanoi qui est victime d'une tentative de vol similaire d'environ 1 million de dollars. Toutefois, la tentative de détournement de fonds est détectée à temps. Toujours en mai, on découvre qu'en 2015, la banque équatorienne BDA (Banco Del Austro of Cuenca) a été victime de 12 transferts frauduleux représentant environ 12 millions de dollars. Selon Bloomberg, au moins 7 autres institutions financières situées notamment au Japon, en Italie, en Chine et en Australie, auraient été victimes de transactions suspicieuses. En Juin, selon KyivPost, près de 10 millions de dollars sont dérobés à une banque ukrainienne via le système SWIFT.

Côté investigation, et selon BAE System, c'est un malware spécifique qui aurait permis le cyber-braquage de la banque du Bangladesh. Dans un second rapport, BAE System montre que le malware en question partage du code avec des malwares utilisés par le groupe Lazarus (cf. section 2.5 ci-dessous). Un rapport de Symantec tend à confirmer cette thèse, en mettant en évidence des lignes de code communes entre la backdoor Contopee (attribuée à Lazarus) et le cheval de Troie Banswift.

En Octobre, Symantec alerte sur le fait qu'une campagne d'attaques baptisée Odinaf, utilise des outils permettant de manipuler les journaux de transferts des clients SWIFT et d'effacer leurs traces d'activité. L'éditeur ne fait pas de lien direct avec les autres attaques concernant les banques du réseau SWIFT. Pour Symantec, Odinaf cible principalement des institutions financières aux États-Unis, à Hong Kong, en Australie, au Royaume-Uni et en Ukraine et aurait plutôt des liens avec le célèbre groupe Carbanak.

Extrait du bulletin de mai 2016 :

La banque centrale du Bangladesh s'est fait dérober 81 millions de dollars dans une cyberattaque en février dernier, et l'enquête a pointé, début mai, la responsabilité du réseau SWIFT. Puis une seconde attaque détectée contre une autre banque a également mis en cause la sécurité de ce réseau.

L'analyse technique de ces attaques, menée par des chercheurs en sécurité de BAE Systems, a trouvé des similitudes avec une autre attaque, celle contre Sony Pictures.

Extrait du bulletin du mois d'août 2016 :

Rapporté par l'agence Reuters, le réseau interbancaire Swift fait encore parler de lui par de nouvelles attaques qui ont permis à des pirates de faire des virements frauduleux. L'analyse semble montrer que ce n'est pas le réseau lui-même qui pose problème, mais plutôt les banques qui maintiennent difficilement leur infrastructure et leurs accès au réseau de manière sécurisée et à jour. Le réseau Swift fait pression sur les banques pour les inciter à augmenter leur niveau de sécurité, notamment en menaçant de divulguer des informations sur les piratages subis.

2.3. Les rançongiciels de plus en plus à la mode

Le nombre d'attaques par rançongiciels est également en pleine explosion en 2016. En effet, peu de jours ne passent sans qu'un nouveau rançongiciel ne soit découvert ou ne fasse de nouvelles victimes. Il s'agit certainement pour le moment du meilleur moyen pour les cybercriminels de réaliser de gros profits à moindre coûts.

Souvent diffusés à travers des pièces jointes vérolées, ces malwares prennent la plupart du temps en « otage » les données des utilisateurs en les chiffrant. Un message apparaissant à l'écran prévient alors l'utilisateur que ses données ont été chiffrées et que le seul moyen de les récupérer, est de payer une rançon souvent en bitcoins. La victime qui n'a pas fait de sauvegarde régulière de ses données considère à ce moment-là, n'avoir d'autre choix que de payer et d'espérer que le hacker transmettra la clé de déchiffrement.

En 2016, on note que pour maximiser leurs profits, les hackers ne se contentent plus de cibler des utilisateurs lambda, mais s'attaquent de plus en plus à des entreprises, des établissements de santé, des universités, etc. Par exemple, en février 2016, le Hollywood Presbyterian Medical Center, un établissement de santé américain a été victime d'un rançongiciel, bloquant une partie de son système d'information. Afin de reprendre le contrôle des PC infectés, le dirigeant a versé la somme de 40 bitcoins (soit environ 17 000$). En France aussi le milieu hospitalier a été touché, les centres hospitaliers d'Epinal ou Duchenne à Boulogne-Sur-Mer ont également été victimes d'un rançongiciel.

La multiplication rapide du nombre de rançongiciels démontre que l'imagination des cyber-escrocs est sans limite, certains rançongiciels intègrent des outils anti-détection, ou se spécialisent :

- Locky est certainement en 2016 le rançongiciel le plus célèbre ; il embarque des fonctionnalités d'anti-analyse et est capable de faire des demandes de rançons dans plus de 30 langues différentes.
- Petya chiffre non seulement les données, mais il altère aussi le secteur d'amorçage du disque dur (Master Boot Record ou MBR), de manière à rendre la totalité du système inutilisable.
- Ransoc ne chiffre pas les données. En revanche, il récolte des informations personnelles et sensibles concernant la victime sur les réseaux sociaux et les services de partage de fichiers. Lorsqu'il affiche la demande de rançon, il menace la victime de procédures judiciaires, en utilisant les informations récoltées pour rendre le message le plus réaliste possible.
- Stampado est distribué sur un modèle de RaaS (Ransomware-as-a-Service).
- Aucun système n'est oublié, FaireWare et Linux Encoder ciblent le monde Linux.
- Des bases de données ont été visées avec Cerber.
- Popcorn Time demande à la victime d'envoyer un lien malveillant à des amis et si au moins deux d'entre eux se retrouvent infectés, la victime initiale pourra récupérer ses fichiers gratuitement.

Même si des réponses techniques (par exemple la sauvegarde régulière des données) et organisationnelles (notamment la sensibilisation) existent, la lutte contre les rançongiciels reste difficile. Pourtant, la plupart des éditeurs de sécurité tels qu'Emsisoft, Trend Micro ou Kaspersky ont développé des outils de déchiffrement pour les rançongiciels les plus répandus. Des initiatives ont également vu le jour, citons notamment les projets « Ransomware Tracker », « ID Ransomware » ou encore « No More Ransom ». Ce dernier regroupe la police nationale néerlandaise, Europol, Intel Security, Kaspersky Lab, Bitdefender, Check Point et Trend Micro. Le projet a pour but d'aider les victimes en les informant et en leur proposant des outils pour déchiffrer leurs fichiers.

Malgré toutes ces bonnes volontés, on constate aujourd'hui que les personnes ou plus encore les entreprises sont souvent prêtes à payer pour récupérer leurs données. Une majorité des entreprises préfère en effet payer plutôt que de voir leur production s'arrêter, ou de perdre du temps à remettre en route leur système d'information à l'aide de sauvegardes saines.

Enfin, si 2016 a certainement été l'année des rançongiciels, certains éditeurs pensent que 2017 risque de voir se développer :

- Les ransomworm (aka cryptoworm), des rançongiciels capables de s'auto-propager comme ZCryptor.
- Les jackware, aussi appelé RoT (Ransomware of Things), des rançongiciels qui s'attaquent aux objets connectés.

Extrait du blog sur les rançongiciels de Mars 2016

Découvert la semaine dernière par G-Data et baptisé Petya, ce nouveau ransomware, à la différence de Locky, CryptoWall ou encore TeslaCrypt, ne se contente pas de chiffrer quelques fichiers sur l'ordinateur des victimes, il chiffre l'intégralité du disque dur.

Ce malware vise essentiellement des entreprises. Il se propage via un email adressé aux ressources humaines et pointe vers un soit disant CV, hébergé sur Dropbox.
Ce fichier contient en réalité un exécutable qui, lorsque le fichier est ouvert par l'utilisateur, va charger le malware. Ce dernier va dans un premier temps manipuler le MBR (Master Boot Record) afin de prendre le contrôle du processus d'amorçage du système, puis dans un second temps, faire « planter » et redémarrer le système. Lors du redémarrage du système, un message MS-DOS apparait laissant croire à une vérification des disques (CheckDisk). C'est à ce moment que le ransomware commence à chiffrer les données stockées sur le disque, y compris les fichiers systèmes.

Extrait de la Brève du bulletin Cert-IST d'Avril 2016.

Cet article a pour objectif d'attirer votre attention sur 2 phénomènes relativement nouveaux qui visent les entreprises :

- les attaques par ransomware se tournent vers les entreprises,
- la destruction du SI par des malwares "wipers" devient plus fréquent.

2.4. Cyber-espionnage d'état

L'année 2016 confirme que les Etats sont de plus en plus impliqués dans la sécurité offensive. Ceux-ci ne font plus mystère du développement de centres de cyberdéfense offensive comme la Russie, l'Allemagne, les Etats-Unis avec leur USCYBERCOM créé en 2010, et même la France avec le Comcyber. En décembre 2016, le ministre de la défense, Jean-Luc Le Drian, inaugurait le pôle Cyberdéfense situé en Bretagne. Ce dernier sera en charge de la défense, du renseignement, mais aussi de la riposte. A cette occasion, Jean-Luc Le Drian a affirmé : « *Nos capacités cyber-offensives doivent donc nous permettre de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives, justifiées par l'ouverture d'hostilité à notre encontre. En utilisant pour cela des moyens sophistiqués, dont nous sommes parfois les concepteurs, et qui doivent résister à tout risque de détournement.* »

Malheureusement, la course aux cyber-armes, entre pays, entre experts sécurité et hackers est donc bien lancée. Elle s'accompagne de la création toujours plus pléthorique et imaginative d'outils de hacking, d'exploits 0-days ou encore de malwares permettant de mener des opérations de cyber-espionnage. D'ailleurs, pour de plus en plus d'éditeurs, le niveau de complexité de certaines de ces cyber-armes ne laisse que très peu de doutes sur le fait que des Etats sont derrière celles-ci.

Ainsi, plusieurs attaques probablement sponsorisées par des gouvernements ont été médiatisées en 2016 :

- ProjectSauron, ciblant des gouvernements, des infrastructures militaires, des centres de recherche scientifique, des opérateurs de télécommunication et des institutions financières.
- Sandworm Team, ciblant les télécoms, le secteur énergétique, des institutions gouvernementales et militaires.
- Sofacy (ou APT28), ciblant des médias, des organismes gouvernementaux, militaires, et des entreprises du domaine de la sécurité.
- Grizzly Steppe, visant des organisations gouvernementales via des campagnes d'e-mails ciblées (spear-phishing), des infrastructures critiques, des universités, des organisations politiques ou encore des entreprises du secteur privé. D'après le rapport du DHS et du FBI, il s'agirait des groupes de cyber-espionnage appartenant aux services de renseignement russes également connus sous les noms d'APT28 (Fancy Bear, Pawn Storm, Sednnit, Strontium, Sofacy et Threat Group-4127) et APT29 (Cozy Bear, Dukes, CozyDuke, Office Monkeys, CozyCar). Ces groupes auraient notamment, d'après certains experts et gouvernements, compromis le Comité National Démocrate (DNC) aux Etats-Unis durant la campagne présidentielle.

Il reste qu'attribuer une attaque à un pays ou à un groupe de hackers est un exercice extrêmement délicat, malgré les indices obtenus par les experts en sécurité. Ainsi McAfee affirme « *les pirates peuvent fausser leur emplacement, leur langue et tous les marqueurs qui pourraient les ramener à eux. Tout pirate qui avait les compétences nécessaires pour pénétrer le DNC serait également en mesure de cacher ses traces* ». Le débat relatif à l'attribution des attaques est de ce fait plus que jamais ouvert dans la communauté des CERTs et autres experts en sécurité. De plus en plus d'acteurs du renseignement cyber appellent à une approche raisonnée : par exemple, Microsoft a demandé en juin, à ce qu'un organisme indépendant impliquant des experts techniques des secteurs publics et privés soit créé afin d'attribuer les attaques à des Etats selon des standards communs.

Enfin, une autre question se pose : il arrive que des cyber-armes d'Etats soient divulguées sur Internet comme lorsque les Shadow Brokers ont mis à disposition en 2016 des outils piratés à la NSA. Dans le même genre en 2015, c'est l'entreprise italienne de sécurité offensive Hacking-Team qui a été attaquée, 400 Go de données furent alors divulgués sur Internet dont le code source de ses outils de « surveillance ».

Une chose est sûre, 2017 verra certainement de nouvelles attaques dans le but de mener des opérations d'influences publiques mais aussi politiques comme le suggère déjà le piratage du parti démocrate aux Etats-Unis en fin d'année 2016.

Extrait de la fiche attaque CERT-IST/ATK-2016-011 d'août 2016 :

Strider (aussi connue sous le nom ProjectSauron) est une plate-forme de cyber-espionnage modulaire et extrêmement sophistiquée, qui a été conçue dans l'idée de pouvoir lancer, puis de gérer des attaques sur du long terme. […] D'après Kaspersky, ProjectSauron atteint un tel niveau de complexité qu'il ne peut qu'avoir été sponsorisé par un gouvernement (l'évaluation du coût de développement est de l'ordre de plusieurs millions de dollars).

Extrait de la fiche attaque CERT-IST/ATK-2016-070 de décembre 2016 :

Sandworm Team est un groupe de cyber-espionnage qui est probablement actif depuis 2009, et qui a été attribué à la Russie

Extrait de la fiche attaque CERT-IST/ATK-2016-013 d'août 2016 :

Sofacy (aussi connu sous les noms APT28, Pawn Storm, Fancy Bear et Sednit) est un groupe de cyber-espionnage supposé lié au gouvernement russe.

2.5. Le groupe Shadow Brokers

Piratage ou fuite de données liée à une personne interne à la NSA ? Difficile de le savoir. Pour rappel, c'est au milieu de l'été 2016 que le groupe Shadow Brokers fait parler de lui en publiant sur Pastebin et GitHub, 2 archives contenant des logiciels espions « piratés » au groupe Equation, ce dernier étant d'après certains spécialistes, l'unité en charge des cyber-opérations offensives de la NSA (Tailored Access Operations - TAO).

Une des archive contenait des programmes d'exploitation concernant les équipements réseau de plusieurs fabricants notamment Cisco, Fortinet, Juniper etc. Celle-ci a été rendue publique a priori dans le but de démontrer l'existence et l'efficacité des outils pour mieux revendre la seconde archive. The Intercept a confirmé que certains de ces outils figurent bien dans le catalogue ANT de la NSA dévoilé en 2013 par Edward Snowden.

Devant l'échec de la revente de ces premiers outils, le groupe a dévoilé à plusieurs reprises des codes offensifs supplémentaires sur un site nommé ZeroNet. Pour réaliser des profits sur la revente de ces cyber-armes, le groupe a, plus tard changé de stratégie et cible désormais des acheteurs individuels en proposant des outils à l'unité ou en package.

A l'heure actuelle, les vulnérabilités pouvant être exploitées par les programmes de Shadow Brokers en accès libre ont été corrigées, les programmes eux-mêmes étant détectés par la grande majorité des antivirus.

Extrait du Danger Potentiel CERT-IST/DG-2016.004 d'août 2016 :

Nous émettons ce Danger Potentiel pour attirer votre attention sur le fait que des programmes d'exploitation, affectant les systèmes Cisco ASA et le système d'exploitation FortiOS de Fortinet, ont été publiés sur Internet.

Ces programmes ont été révélés publiquement par le groupe "Shadow Brokers", et il est fort à parier que d'autres équipementiers seront impactés. Juniper enquêtes sur d'éventuel "0-day" sur ses produits.

Extrait du Hub de Crise « Shadow Brokers » d'août 2016 :

Nous ouvrons ce hub de crise pour suivre l'évolution des menaces liées aux codes d'exploitations et aux outils permettant de contourner la sécurité de pare-feu, publiés sur Internet par le groupe de hackers « Shadow Brokers ».

Ces programmes d'exploitation affectent plusieurs équipementiers. Cisco, Fortinet et Juniper investiguent sur les programmes touchant leurs équipements et exploitant des vulnérabilités « 0-day ».

2.6. Les APT : les menaces les plus dangereuses pour les entreprises ?

La plus grande menace pour les entreprises reste certainement les attaques sophistiquées et ciblées dites APT (Advanced Persistent Threat) dont le but est le cyber-espionnage ou le cyber-sabotage. Avec des infrastructures de plus en plus ouvertes vers l'extérieur (phénomènes Cloud, IoT, BYOD…), les données des entreprises sont plus que jamais exposées et ce, malgré les investissements et les efforts déployés pour augmenter le niveau de sécurité.

Ce qui caractérise ce type d'attaque est le mode opératoire utilisé par les groupes de hackers :

1. Reconnaissance de l'écosystème de l'entreprise à l'aide d'informations publiques,
2. Ciblage d'un point d'entrée (spear-phishing). Une fois la phase de reconnaissance réalisée, l'attaquant envoie un e-mail ciblé qu'il aura pris soin de mettre en forme de manière à ce qu'il paraisse légitime (par exemple en choisissant avec soin un sujet et un contenu adéquat, en utilisant un nom d'expéditeur connu, en s'adressant personnellement et nominativement au destinataire). Le mail est accompagné d'une pièce jointe piégée, ou contient un lien vers un site malveillant sur lequel un malware aura été préalablement déposé et qui sera téléchargé lorsque l'utilisateur naviguera sur le site (drive-by download). Le malware permet de compromettre la machine en y installant une porte dérobée donnant ainsi un accès au réseau.
3. Utilisation de serveurs de commandes et de contrôles permettant à l'attaquant d'envoyer, depuis Internet, des instructions aux machines compromises.
4. Mouvements latéraux pour compromettre d'autres machines du réseau, obtenir des informations d'identification, élever ses privilèges et ainsi maintenir un contrôle permanent sur le réseau.
5. Adaptation à l'évolution de l'écosystème pour rester sous les radars des outils de surveillance de l'entreprise.
6. Recherche des serveurs hébergeant les données sensibles et installation d'outils permettant l'exfiltration des données.
7. Transfert des données vers un serveur de stockage interne, puis fragmentation, compression et chiffrement des données avant transfert vers un serveur externe.

Nous listons ci-dessous les acteurs et attaques qui nous ont semblés les plus significatifs en 2016 :

- BlackEnergy, (peut désigner à la fois le groupe cybercriminel et le malware qu'il utilise) a mené une cyberattaque contre le secteur énergétique ukrainien en début d'année 2016 ainsi que fin 2015. Cette attaque a mis hors service une partie du réseau de distribution d'électricité en Ukraine. De plus, le malware possède un module KillDisk qui permet d'effacer des données et le secteur de boot d'un disque dur pour empêcher le redémarrage du système. Pour FireEye, l'attaque aurait été menée par un groupe russe nommé Sandworm.
- Lazarus est un groupe de cybercriminels probablement originaire de Corée du Nord qui serait à l'origine de l'attaque contre Sony Pictures en 2014. Plusieurs compagnies de sécurité ont enquêté sur les activités du groupe lors de l'Opération Blockbuster, dont les résultats ont été publiés début 2016. D'après cette enquête, le groupe Lazarus ciblerait des institutions financières, des médias et des usines dans plus d'une dizaine de pays.
- Au cours du premier semestre 2016, les groupes Danti et SPIVY ont utilisé un exploit de la vulnérabilité CVE-2015-2545 pour mener des attaques contre des organisations gouvernementales en Inde, en Asie Centrale et en Asie du Sud-Est. Le premier groupe serait probablement lié à NetTraveller et DragonOK.
- ScarCruft est un groupe qui a utilisé des vulnérabilités alors non corrigées (0-day) de Flash Player (CVE-2016-1010, CVE-2016-4171) pour mener les campagnes de cyber-espionnage baptisées Operation Daybreak et Operation Erebus par Kaspersky. Le groupe a ciblé des autorités judiciaires asiatiques, des sociétés de trading en Asie et dans le monde, une société publicitaire et de monétisation d'applications mobiles aux Etats-Unis, ainsi que des particuliers en rapport avec l'Association Internationale des Fédérations d'Athlétisme.
- Dropping Elephant (connu aussi comme « Chinastrats » et « Patchwork ») est un groupe de cyber-espionnage qui a volé des documents et données sensibles à des organisations diplomatiques et économiques impliquées dans les relations étrangères chinoises.
- Le groupe Operation Ghoul a ciblé majoritairement des entreprises industrielles et d'ingénierie en Asie, au Moyen-Orient, en Europe et aux Etats-Unis. Le groupe a utilisé le malware HawkEye, fournissant de très nombreux outils permettant de récupérer des informations sur ses victimes.
- Le groupe Wekby connu aussi sous les noms de Dynamite Panda, TG-0416 et APT 18, a mené des attaques contre des entreprises américaines dans les secteurs de la santé, des télécoms, de l'aéronautique et du spatial, de la défense et des technologies.
- FruityArmor a ciblé des chercheurs, des militants et des individus liés à des organisations gouvernementales en utilisant une vulnérabilité 0-day Windows (CVE-2016-3393), permettant aux attaquants d'élever leurs privilèges une fois les systèmes infectés. Les victimes sont situées en Thaïlande, en Algérie, au Moyen-Orient et en Suède.

Il n'est pas toujours évident de s'y retrouver dans les noms donnés à ces différents groupes/malwares. C'est d'autant plus difficile que chaque acteur du renseignement cyber utilise sa propre nomenclature, sans forcément faire le lien avec celle utilisée par les autres.

Par exemple, APT1, APT2, APT3... sont des appellations souvent utilisés par FireEye. Microsoft, lui, utilise des noms d'éléments chimiques pour les différents groupes d'acteurs (PROMETHIUM, NEODYMIUM, PLATINUM, TERBIUM, STRONTIUM…), ce qui n'est pas franchement parlant.

A l'inverse, l'éditeur CrowStrike catégorise et nomme ces groupes de façon assez simple :

- Implication supposée des Etats : utilisation de noms d'animaux représentant le pays :
  - Panda = Chine
  - Bear = Russie
  - Kitten = Iran
  - Tiger = Inde
  - Chollima = Corée du Nord (cheval mythique)
- Pas d'implication étatique :
  - Jackal = Groupe d'activistes
  - Spider = Groupe criminels

Extrait de la fiche attaque CERT-IST/ATK-2016-009 d'août 2016 :

PatchWork (aussi connue sous les noms "Dropping Elephant", "Monsoon", ou "Chinastrats") est une APT qui a pris pour cible différents organismes publics diplomatiques ou économiques, en utilisant un ensemble d'outils d'attaques existants.

Extrait de la fiche attaque CERT-IST/ATK-2016-012 d'août 2016 :

Operation Ghoul désigne une campagne d'attaques ciblées à l'encontre de diverses entreprises du monde industriel, visant sans distinction l'ingénierie et la fabrication. Ces vagues d'attaques ont été révélées le 17 août par la société Kaspersky.

Extrait de la fiche attaque CERT-IST/ATK-2016-040 d'octobre 2016 :

FruityArmor est le nom donné par Kaspersky à un groupe d'attaquants qui a utilisé une vulnérabilité de Windows (CVE-2016-3393 décrite dans l'avis CERT-IST/AV-2016.0965) alors qu'elle n'était pas encore corrigée par Microsoft. Pour information, cette vulnérabilité a été corrigée via les mises à jour d'octobre 2016 (MS16-120).

2.7. L'Internet des objets à l'heure du DDoS

L'année 2016 restera également marquée par la multiplication des attaques en Déni de Service Distribué (DDoS), atteignant des puissances jusque-là jamais observées. D'une année à l'autre le constat est identique : ces attaques restent toujours aussi populaires, notamment en raison de la grande diversité d'outils gratuits et de services en ligne peu coûteux (DDoSaaS : DDoS as-a-service), permettant à n'importe qui ayant quelques connaissances et une connexion Internet de lancer une attaque.

En parallèle, de nouveaux vecteurs d'attaques DDoS font leur apparition avec l'émergence de l'Internet des objets (IoT). Le nombre d'objets connectés étant en pleine explosion et leur niveau de sécurité étant encore très faible, les hackers ont rapidement compris l'intérêt d'utiliser la bande passante cumulée de ces objets pour créer des botnets et lancer de puissantes attaques. Beaucoup de ces objets utilisent des mots de passe par défaut souvent partagés par des gammes entières de produits. En se connectant illégalement à ceux-ci et en y installant les bons outils, il devient possible de créer un très large réseau d'objets connectés zombies qui serviront à lancer des attaques.

Pour constituer ces différents botnets, les hackers peuvent utiliser des services en ligne comme Shodan. A l'image d'un moteur de recherche, Shodan référence et indexe entre autres, les appareils connectés à Internet qui sont mal sécurisés. Pour ce faire, Shodan envoie des requêtes aux équipements sur différents ports. Si certains sont ouverts et sans protection ou avec une faible protection, c'est-à-dire utilisant le mot de passe par défaut du constructeur, l'information est enregistrée par Shodan.

LizardStresser, est un malware créé par le groupe Lizard Squad, dont le code source a été publié en 2015 pour que des apprentis pirates puissent à leur tour, créer leurs propres réseaux de bots. Le groupe loue d'ailleurs leur « booter » pour que n'importe qui puisse lancer des attaques. En 2016, LizardStresser a commencé à cibler et à infecter des objets connectés. En juin dernier, des hackers ont lancé, à l'aide de ce nouveau botnet IoT, une attaque atteignant 400 Gbit/s contre des sites de jeux, des établissements bancaires, des opérateurs de télécommunications et des agences gouvernementales au Brésil.

En septembre, ce sont les malware Mirai et Bashlite qui ont infecté des objets connectés, essentiellement des caméras vidéo et des enregistreurs numériques (DVR). Le botnet ainsi créé a été utilisé pour mener des attaques à l'encontre de l'hébergeur OVH (1 Tbit/s) et du site du journaliste Brian Krebs (620 Gbit/s). En octobre 2016, les serveurs DNS de Dyn ont été attaqués par Mirai, rendant inaccessibles pendant plusieurs heures de grands sites tels que Airbnb, AWS, GitHub, le New York Times, Twitter, Spotify… Un peu plus tard, le code source de Mirai ayant été publié, des pirates ont développé leur propre botnet, baptisé botnet #14 ; des attaques ont été lancées en novembre 2016 avec des pics de trafic enregistrés à 500 Gbit/s, non plus contre des sites web, mais contre un pays, le Libéria.

Enfin, en décembre 2016, c'est le malware Rakos découvert par ESET, qui s'attaque à des serveurs et des objets connectés fonctionnant sous Linux pour constituer son botnet. Pour le moment aucune attaque de type DDoS ne lui a été attribuée. Cependant, il est fort à parier que des cas d'attaques provenant de Rakos verront le jour en 2017.

Extrait de l'article : Des objets connectés « zombies » du bulletin d'octobre 2016 :

Le mois de septembre a été marqué par des attaques par déni de service distribué (DDoS) d'une ampleur jusqu'alors inégalée. Un record a été atteint avec une attaque DDoS à 1 térabit par seconde le 20 septembre à l'encontre de l'hébergeur français OVH, suivi le 21 septembre d'une attaque de 620 Gb/s contre le site web du journaliste et expert en sécurité informatique Brian Krebs, krebsonsecurity.com.

Le point commun entre ces deux attaques, l'utilisation d'un réseau d'objets connectés à Internet (IoT: Internet of Things) tels que des caméras IP ou des enregistreurs vidéos (DVR). Même si les attaques DDoS sont fréquentes à l'encontre de la plupart des hébergeurs, l'utilisation d'objets connectés à Internet pour mener ce type d'attaques marque un tournant dans l'évolution des botnets.

Extrait de la Brève : Les algorithmes DGA du bulletin de décembre 2016 :

Des chercheurs en sécurité ont observé début décembre des variantes sophistiquées de Mirai ayant implémenté des algorithmes de type DGA (Domain Generation Algorithm).

2.8. La fraude au président, cette indémodable

Avec la médiatisation systématique des APT et du cyber-espionnage d'état, on oublierait presque d'évoquer les tentatives de fraudes basées sur l'ingénierie sociale et tout particulièrement la « fraude au président » (parfois appelée escroquerie aux Faux Ordres de Virement International – FOVI, « business e-mail compromise scam » ou « bogus boss » aux Etats Unis). En effet, en se fiant aux discussions que le Cert-IST entretient régulièrement avec ses adhérents et homologues notamment français, cette menace est toujours bien d'actualité.

Bien que peu médiatisée mais observée en France au moins depuis 2010, la « fraude au président » a d'abord visé les grands groupes cotés en bourse, pour désormais sévir sur toutes les entreprises du monde entier. L'arnaque consiste à obtenir un virement vers un compte à l'étranger, sur ordre supposé d'un dirigeant ou d'un fournisseur, derrière lequel se cache en réalité un internaute malveillant (usurpation d'identité). Les cibles font généralement partie du service comptable ou de la trésorerie de l'entreprise victime.

Si ces attaques sont peu mises en avant par rapport aux APT par exemple, c'est que les entreprises qui en sont victimes craignent une mauvaise publicité. En effet, on admet communément qu'une APT est difficile à parer, alors qu'une « fraude au président » peut être beaucoup plus facilement évitée via des précautions élémentaires.

D'après un bulletin d'actualité du CERT-FR de janvier 2016, les modes opératoires évoluent constamment, et on peut aujourd'hui observer des arnaques sous différentes formes :

- Un individu se fait passer pour le PDG et demande un virement financier vers un compte bancaire illégitime.
- les escrocs se font passer pour des informaticiens de la banque et, sous le prétexte de tester la comptabilité de l'entreprise avec le protocole SEPA, demande à effectuer un virement bancaire soi-disant de test.
- Les escrocs se font passer pour un fournisseur et demandent le paiement d'une facture sur un nouveau compte bancaire.
- Les escrocs peuvent aussi agir directement en passant un virement auprès de la banque détentrice des comptes.

Dans tous les cas, même si ces arnaques ne requièrent pas une expertise informatique forte de la part des escrocs (inutile de coder un malware par exemple), leur réussite dépend malgré tout d'un certain nombre de prérequis :

- Etre capable de créer de fausses adresses mail (prérequis le plus technique en réalité),
- Maitriser parfaitement la langue locale, et les procédures financières du pays concerné,
- Réaliser une démarche d'ingénierie sociale, parfois longue, pour collecter un maximum d'informations publiques sur l'environnement économique et humain de l'entreprise,

- Choisir minutieusement le moment de l'attaque : veille de long week-end, vacances, plan social, absence du patron, etc.
- Disposer de bases en psychologie pour acquérir rapidement la confiance des victimes.

Sur le plan international, le FBI a publié début janvier 2016 un rapport alarmant sur le sujet. D'après l'agence américaine, cette fraude aurait couté 2,3 milliards de dollars entre octobre 2013 et février 2016, pour un panel de 17000 entreprises présentes aux Etats Unis et dans 79 pays du monde entier.

Des géants, comme Michelin, Intermarché, Coca Cola, KPMG, etc., en ont fait les frais. Un montant record de 42 millions d'euros a même été détourné début 2016 chez FACC, un équipementier autrichien de l'aéronautique. La société en question a vu son cours de bourse chuter de 17% dans la foulée de cette révélation et a limogé sa directrice financière en février, puis, au mois de mai, son PDG à la tête de l'entreprise depuis 17 ans.

Rien qu'en France depuis 2010, et d'après le ministère de l'intérieur, environ 2300 plaintes ont été recensées pour un préjudice global de 485 millions d'euros.

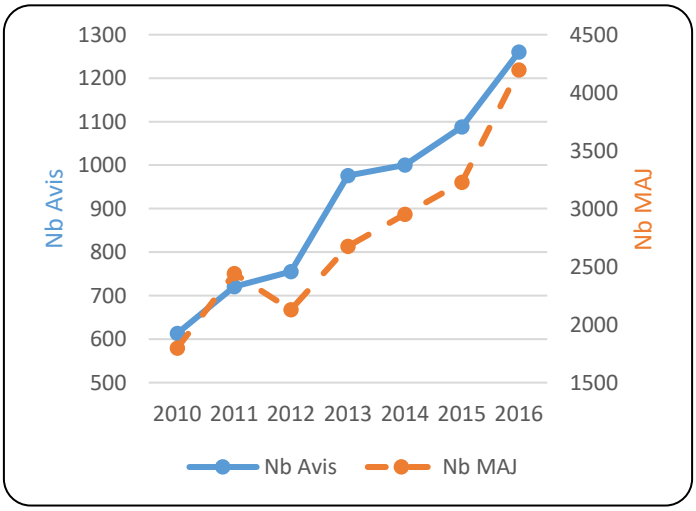
3. Production du Cert-IST en 2016

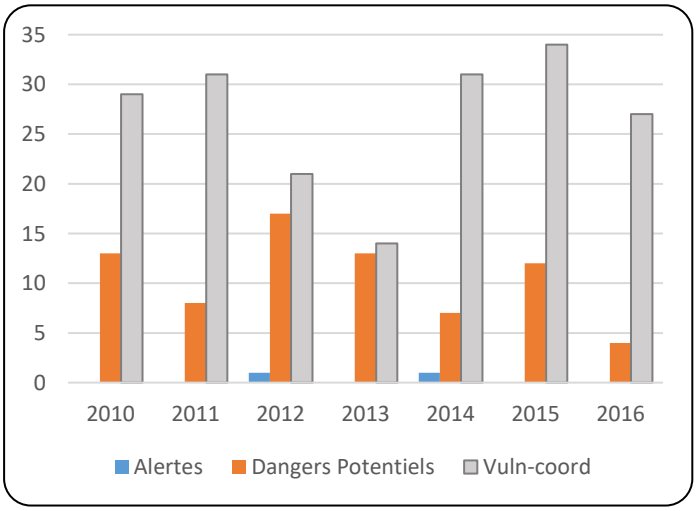
3.1. Veille sur les vulnérabilités et des menaces

Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST suit de façon continue, différentes sources d'informations (annonces constructeurs, blogs sécurité, mailing-lists, échanges s entre CERTs, etc.) afin d'être informé des nouvelles vulnérabilités. Ces informations sont analysées quotidiennement pour fournir à nos adhérents des informations triées, qualifiées et priorisées.
Le Cert-IST émet ainsi plusieurs types de publications :

- **Les Avis de sécurité** : ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis sont enrichis de façon continue avec des mises à jour mineures ou majeures. Ces dernières correspondent typiquement au cas où des programmes d'attaques – des "exploits" – sont publiés.
- Des **Alertes**, des **Dangers Potentiels** et des **messages "Vuln-coord"**. Les **Alertes** du Cert-IST sont utilisées pour les menaces majeures et exceptionnelles nécessitant un traitement spécifique et très prioritaire. L'émission d'une alerte est un événement rare. . Les **Dangers Potentiels** décrivent des menaces significatives mais non encore imminentes (ou d'une gravité modérée) pour lesquelles le Cert-IST recommande des mesures de protection spécifiques. Les **messages "Vuln-coord"** enfin, sont des informations de coordination qui attirent l'attention sur des vulnérabilités particulières mais d'une dangerosité immédiate plus faible. Ces 3 catégories complémentaires sont axées sur les risques d'attaques alors que les avis de sécurité répertorient eux de façon systématique toutes les vulnérabilités (quelle que soit leurs probabilités d'être utilisées dans des attaques).
- Des **Fiches Attaques** et des **indicateurs de compromission** (IOC) à travers une base de données MISP. Depuis le 1er juillet 2016, le Cert-IST a ouvert un nouveau service orienté sur la détection des attaques et basé sur la diffusion d'IOC qualifiés.

Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.

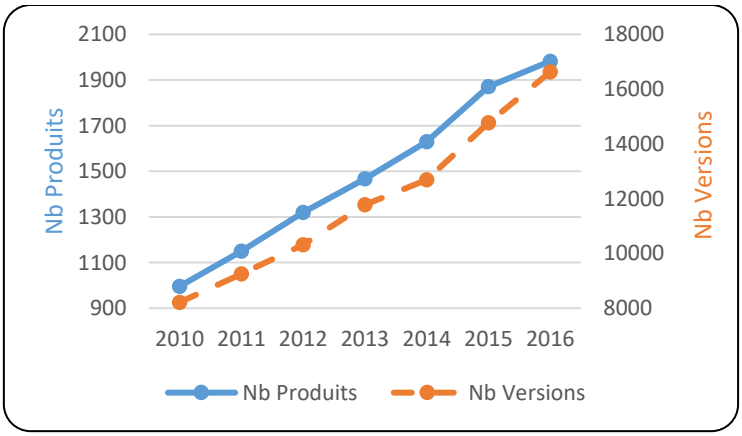




Ainsi, en 2016, le Cert-IST a publié :

- **1 260** avis de sécurité (dont 65 avis Scada), suivis de façon continue au cours de l'année avec **4 075** mises à jour mineures et **122** mises à jour majeures. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec une augmentation de **16%** par rapport à 2015. Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène en constante augmentation. Le maintien du niveau de sécurité passe donc encore et toujours par une application régulière des correctifs de sécurité sur les produits présents dans le système d'information.
- **4** Dangers Potentiels et **27** messages "Vuln-coord". En 2016 aucune alerte n'a été émise. Le nombre de dangers Potentiels a, quant à lui, diminué pour passer de 12 à 4, et le nombre de messages Vuln-coord est passé de 34 à 27.
- **71** fiches attaques ont été publiées sur le deuxième semestre 2016, avec dans la base de données MISP **790** évènements qui ont été enrichies, et **62 674 IOC** utilisables comme signature.

Concernant les produits et les versions suivis par le Cert-IST, fin 2016 le Cert-IST suivait **1 982** produits et **16 624** versions de produit. Le graphique suivant montre l'évolution de nombre des produits et des versions qui sont suivis par le Cert-IST.



3.2. Veille technologique

En plus de la veille sur les vulnérabilités, le Cert-IST publie également des bulletins de veille technologique :

- Un **bulletin quotidien de veille média** recensant les articles les plus intéressants parus sur Internet sur un ensemble de sites francophones et anglophones traitant de sécurité,
- Un **bulletin mensuel de veille SCADA** présentant une synthèse de l'actualité sur la sécurité des systèmes industriels,
- Un **bulletin mensuel** généraliste donnant une synthèse de l'actualité du mois (en termes d'avis et d'attaques) et traitant de sujets d'actualité au travers d'articles rédigés par le Cert-IST,
- Un **bulletin mensuel de veille sur les attaques et IOC** qui permet de synthétiser les événements les plus marquants dans le domaine des attaques.

4. Conclusion

A l'heure de la transformation numérique, les entreprises sont plus que jamais dépendantes de l'outil informatique, des applications, et des réseaux. De plus, la forte croissance des nouvelles technologies, qui sont toujours plus interconnectées :

- poussent les entreprises à s'ouvrir d'avantage, que cela soit via le cloud, le BYOD ou encore l'Internet des objets,
- tendent à dissiper l'information tout en y facilitant l'accès.

L'ouverture des infrastructures vers ces technologies rend plus complexe la gestion de la sécurité des biens matériels et des données. On constate qu'il n'est alors pas évident de choisir entre réduction des coûts et sécurité du point de vue des DSI et RSSI.

L'année 2016 démontre que le risque reste encore et toujours d'actualité :

- Des attaques, des vols de données, des rançongiciels sont découverts quotidiennement,
- Les systèmes industriels et critiques sont de plus en plus visés (cf. attaque BlackEnergy),
- Les systèmes bancaires sont toujours très appréciés par les attaquants,
- La sécurité offensive des états prend une place plus importante sur le plan géopolitique,
- L'Internet des objets est désormais une cible de choix pour les hackers,
- L'évolution des attaques se fait toujours sur fond de grands classiques nécessitant peu de compétences techniques. L'ingénierie sociale, caractérisée par l'arnaque dite de « fraude au président », en est le meilleur exemple.

La sécurité est plus que jamais un enjeu stratégique. Pour ce faire, les entreprises doivent s'adapter de plus en plus vite pour faire face à ces menaces croissantes en :

- Sécurisant les systèmes critiques tels que les infrastructures industrielles,
- Appliquant une politique de sécurité en profondeur :
    - Hardening,
    - Segmentation des réseaux,
    - Limitation des comptes à privilèges,
    - Utilisation de technologies d'authentification multi-facteurs,
    - Application des correctifs pour maintenir à jour le niveau de sécurité…
- Evaluant les informations sensibles en mettant en œuvre une classification des données,
- Réalisant des sauvegardes régulièrement,
- Développant sa capacité de détection et de réaction aux intrusions, via des systèmes de supervision tels que les SIEM, ainsi qu'à l'aide d'un service de Threat Intelligence pertinent et efficace fournissant et contextualisant l'information sur les menaces.
- Sensibilisant encore et toujours les utilisateurs sur les risques d'attaques, les problématiques de mots de passe trop faibles et leur réutilisation.

En dépit d'une année 2016 assez alarmante d'un point de vue médiatique, il convient de prendre du recul sur les nombreux incidents rapportés dans l'actualité. En effet, même si le nombre d'attaques détectées est toujours en augmentation, le vol de données toujours plus important, il est difficile de corréler directement ces faits à une prolifération des acteurs malveillants pendant. Certains événements découverts ou signalés en 2016 se sont en fait produits bien plus tôt : le vol massif de données chez Yahoo!, entre autres, s'est produit en 2013 et 2014.

D'autres indicateurs vont également dans le bon sens :

- En 2016, le nombre de vulnérabilités corrigées n'a jamais été aussi important (cf. les 1260 avis du Cert-IST).
- En proportion, le nombre de failles réellement exploitées ou pour lesquelles des codes d'exploitation ont été publiés a diminué.
- L'année 2017 s'amorce avec une baisse significative de la diffusion de rançongiciels, et notamment de Locky. Cette tendance pourrait se poursuivre grâce à la collaboration de plus en plus visible des éditeurs de sécurité (démantèlement de botnets, intégration de défenses spécifiques dans les solutions antivirus …).

2016 est apparue comme une année charnière pour ce qui est de la lutte cyber. En effet, elle a vu l'apparition de bon nombre d'initiatives et l'émergence de comportements encourageants parmi les acteurs de cette lutte. 2017 sera très certainement dans cette continuité positive :

- Les sociétés éditrices de logiciels se dotent davantage d'équipes dédiées à la sécurité de leurs produits (PSIRT), une tendance que nous observons clairement dans le cadre de notre veille quotidienne sur les vulnérabilités.
- Outre les classiques audits, de plus en plus d'entreprises n'hésitent pas à éprouver leur sécurité à travers des programmes ouverts de rémunération de type « Bug Bounty ».
- La coopération entre acteurs du renseignement cyber se met en place (cf. l'opération Blockbuster qui a permis de décrire le groupe Lazarus début 2016).
- Le partage d'informations (marqueurs/indicateurs) au sujet des groupes d'attaquants et des APT tend à améliorer les capacités de détection des entreprises. De fait, les standards concernant l'échange d'indicateurs sont désormais mûrs, et les solutions SIEM sont aujourd'hui de plus en plus capables d'utiliser ces informations en entrées.
- Les différentes législations, comme la future loi européenne sur la protection des données (entrée en application en mai 2018), tendent à soutenir ces efforts.

Malgré tout, 2017 s'annonce comme un véritable challenge, car la dispersion des informations via l'évolution des nouvelles technologies continue à augmenter. Côté nouvelles technologies et Internet des objets, on peut imaginer que les attaques visant les drones, les smartphones et les installations domotiques auront une place dans l'actualité. Les objets connectés ne serviront peut-être plus simplement de robot pour lancer des attaques en déni de service, mais seront de plus en plus utilisés comme point d'entrée pour infiltrer des réseaux.

Tandis que le cyber-espionnage d'Etat se maintiendra sans aucun doute, on peut imaginer que d'autres groupes cybercriminels vont peu à peu s'intéresser aux clouds privés des entreprises. En effet, les éditeurs de gros clouds publics type Amazon ou Microsoft sont aujourd'hui davantage protégés suite à d'importants investissements dans le domaine, ce qui n'est pas forcément le cas d'éditeurs plus modestes offrant des services de cloud privé.

Enfin, les responsables sécurité devront garder à l'esprit les problématiques d'ingénierie sociale et de Phishing personnalisé. Grâce à l'intelligence artificielle, au « Machine Learning », les cybercriminels n'auront de cesse d'améliorer ces techniques. En limitant les informations publiquement disponibles concernant l'entreprise, et en réalisant des sensibilisations régulières des utilisateurs, ce risque pourra être limité.