1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée. L'objectif est de retracer les événements marquants de 2012 de façon à mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Nous présentons tout d'abord une synthèse de l'actualité de 2012 (cf. chapitre 2) en passant en revue les principales menaces identifiées par le Cert-IST, ainsi que les sujets qui ont été le plus discutés dans la communauté.

Nous identifions ensuite les évolutions les plus marquantes pour les entreprises, et analysons comment les prendre en compte (cf. chapitre 3).

Enfin, nous faisons une rapide synthèse sur la production du Cert-IST en 2012, en donnant par exemple le nombre d'avis et d'alertes publiés au cours de l'année (cf. chapitre 4).

➢ 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.

2) Synthèse de l'actualité de 2012

2.1 Les menaces identifiées par le Cert-IST

Ce chapitre présente les technologies à propos desquelles le Cert-IST a émis en 2012 des messages d'avertissement (sous forme d'Alerte, de Danger Potentiel1, ou via le bulletin mensuel) parce qu'il y avait un risque fort d'attaques les visant. La taille de chaque mot dans le graphique ci-dessous est proportionnelle au niveau de risque.

Nous commentons ci-après les principales tendances mises en évidence par ce graphique, par ordre d'importance.

[1] : Les différents types de publications du Cert-IST, tels que les Alertes ou les Dangers Potentiels sont présentés au § 4.1

- **Oracle-Java**

Les attaques visant le client Java installé sur les postes de travail (composant JRE) se sont multipliées en 2012. Ces attaques se produisent de façon silencieuse lors de la navigation Internet (pas d'alerte antivirus, pas de crash du navigateur web), au moment où la victime visite des sites anodins (probablement infectés à leur insu). Il ne s'agit pas d'un phénomène nouveau et nous avons déjà émis une mise en garde sur ce sujet en août 2010. Mais ce phénomène prend de l'ampleur et s'accélère, et les nouvelles vulnérabilités découvertes dans Java sont de plus en plus rapidement intégrées dans les outils d'attaques. En 2012 nous avons émis 1 Alerte et 3 Dangers Potentiels sur ce sujet.

- **Internet Explorer**

En 2012, Internet Explorer a été visé par deux séries d'attaques :

- **En juin,** nous avons émis le Danger Potentiel CERT-IST/DG-2012.008 à propos de la vulnérabilité **CVE-2012-1875**. Découverte le 1er juin par McAfee (mais probablement utilisée auparavant de façon ciblée), et maintenue secrète jusqu'à la publication du correctif par Microsoft (le 12 juin, via son bulletin MS12-037), cette vulnérabilité permet d'infecter le poste d'un internaute lors de sa navigation sur Internet. Suite à la publication des correctifs Microsoft, plusieurs programmes d'exploitation de la vulnérabilité ont été publiés sur Internet (et en particulier sur le framework Metasploit). Nous avons donc émis le 15 juin le Danger Potentiel CERT-IST/DG-2012.008 pour avertir notre communauté du risque croissant d'attaque et de l'urgence de déployer les correctifs Microsoft.
- **En septembre,** nous avons émis le Danger Potentiel CERT-IST/DG-2012.014 pour la vulnérabilité **CVE-2012-4969**. Cette fois, la vulnérabilité a été révélée (le 16 septembre) avant qu'un correctif Microsoft ne soit disponible (Microsoft a émis le bulletin MS12-063 le 21 septembre). Plusieurs programmes d'exploitation ont rapidement été publiés, ce qui nous a amené à émettre le Danger Potentiel CERT-IST/DG-2012.014 le 18 septembre.

On nous demande fréquemment quel est le navigateur le plus sûr.

Aucun navigateur n'est à l'abri de vulnérabilités, mais l'expérience montre que le plus souvent, c'est Internet Explorer qui est attaqué.

Cela est probablement dû au fait qu'Internet Explorer est le navigateur le plus utilisé, au moins dans les entreprises, et c'est donc contre ce type de navigateur que se concentrent les attaques. Qu'il s'agisse d'attaques en 0-days ou des vagues d'attaques opportunistes qui exploitent les vulnérabilités récemment corrigées, Internet Explorer se trouve donc particulièrement exposé.

Il s'agit dans les deux cas de vulnérabilités de type 0-day, c'est-à-dire que ces vulnérabilités ont été gardées secrètes jusqu'au jour où elles ont été utilisées dans des attaques.

- **Windows**

Windows reste une cible de choix pour les attaquants et nous avons émis cette année 4 Dangers Potentiels pour des composants de Windows :

- **Windows Media** (janvier 2012) pour une vulnérabilité dans les fichiers musicaux MIDI (CVE-2012-0003) qui permettait d'exécuter du code sur le poste d'un internaute visitant un site web hébergeant un fichier MIDI malveillant. Cette vulnérabilité a été corrigée le 10 janvier par Microsoft par le bulletin MS12-004. Elle a donné lieu ensuite, à plusieurs vagues d'infection, ce qui nous a amené à émettre le 30 janvier le Danger Potentiel CERT-IST/DG-2012.001.
- **Windows RDP** (mars 2012). Il s'agit ici d'une vulnérabilité (CVE-2012-002) qui peut permettre de prendre le contrôle à distance d'une machine Windows ayant activée le service RDP (Remote Desktop Protocol). Etant donnée la dangerosité de la vulnérabilité, nous avons émis le Danger Potentiel CERT-IST/DG-2012.003 dès l'apparition des premiers programmes d'exploitation, 3 jours après la sortie des correctifs Microsoft (bulletin MS12-020 du 13 mars 2012).

- **Windows ActiveX** (avril 2012). Il s'agit d'une vulnérabilité (CVE-2012-0158) qui affecte 4 contrôles ActiveX inclus dans le composant « Contrôle Commun » (MSCOMCTL.OCX) de Windows. Elle permet d'exécuter du code sur l'ordinateur d'une victime visitant un site web ou ouvrant un document Office piégé. Corrigée le 10 avril par Microsoft (MS12-027), cette vulnérabilité a donné lieu à plusieurs campagnes d'infections qui nous ont amené à émettre, le 27 avril, le Danger Potentiel **CERT-IST/DG-2012.005**
- **Windows XML CoreServices** (juin 2012). Cette vulnérabilité (CVE-2012-1889) permet à une page web malveillante d'exécuter du code sur le poste de la victime visitant cette page. Elle a donné lieu à des attaques 0-days signalées le 12 juin par Microsoft, puis rapidement suivies par la publication de plusieurs programmes d'exploitation. Cela nous a amené à émettre le Danger Potentiel **CERT-IST/DG-2012.008** le 18 juin. Microsoft a finalement publié les correctifs pour cette vulnérabilité le 10 juillet dans son bulletin MS12-043.

Même si ces dernières années (cf. nos bilans 2010 et 2011), les attaques se sont plutôt détournées de Windows pour se concentrer sur des applicatifs moins protégés comme Adobe Reader, Flash ou Java, **Windows reste une cible très prisée des pirates** qui sont parfaitement rodés aux différentes techniques d'attaques dans cet environnement. Et les vulnérabilités découvertes dans cet environnement sont très rapidement intégrées dans les outils d'attaques.

Les autres OS ne sont pas pour autant à l'abri. Apple en a fait la triste expérience en 2012, avec le virus **Flashback** qui a infecté en avril plus de 600 000 ordinateurs Mac OS-X au moyen d'une vulnérabilité dans le client Java. En juin 2012, Apple a d'ailleurs changé son discours marketing en remplaçant, dans l'argumentaire de vente du Mac, la mention "Il est immunisé contre les virus PC" par "Il est conçu pour être sûr" (voir par exemple cet article de L'Expansion de juin 2012). En termes de gestion des vulnérabilités, Apple cherche à améliorer ses processus de façon à être plus réactif : Kaspersky a annoncé de façon provocatrice à ce sujet qu'Apple avait 10 ans de retard sur Microsoft et il est clair qu'effectivement Apple doit sans doute s'inspirer des efforts fait par Microsoft dans ce domaine.

- **Oracle-Database**

Nous avons émis en avril le Danger Potentiel **CERT-IST/DG-2012.006** pour une vulnérabilité **0-day dans le composant TNS-Listener d'Oracle** (pour les versions Oracle Database 8i à 11g) qui permet à un attaquant distant, d'espionner des communications (connection sniffing) ou d'injecter des commandes arbitraires dans ces communications (session hijack). La diffusion des outils d'attaque (le 18 avril) résulte d'un quiproquo entre le découvreur (qui pensait que cette vulnérabilité découverte en 2008 avait été corrigée début avril par Oracle) et Oracle (qui souhaitait corriger la vulnérabilité uniquement dans les futures versions du produit). Cette diffusion accidentelle a rendu publique cette faille. Du fait du risque induit, nous avons diffusé le 27 avril notre Danger Potentiel. Les correctifs Oracle ont finalement été disponibles quelques jours plus tard (le 30 avril).

- **PCAnywhere**

Nous avons émis le 28 juin le danger Potentiel **CERT-IST/DG-2012.009** suite à la publication sur Internet d'un programme d'exploitation pour une vulnérabilité (CVE-2011-3478) dans le produit PCAnywhere 12 de Symantec. Cette vulnérabilité était connue depuis janvier 2012 et semble liée au vol des codes sources de plusieurs produits Symantec (voir notre encart). En effet, Symantec a annoncé cette vulnérabilité (et publié les correctifs pour les versions les plus récentes de PCAnywhere) immédiatement après avoir confirmé ce vol.

- **Schneider-Electric**

Pour la première fois depuis que le Cert-IST suit les menaces SCADA, nous avons émis en 2012 un Danger Potentiel (**CERT-IST/DG-2012.004**) sur ce type d'équipements. Il s'agit du PLC **Modicon Quantum** de Schneider Electric pour lequel des programmes d'exploitation permettant à un attaquant de prendre le contrôle du PLC vulnérable ont été publiés.

En 2012, plusieurs cas de **vol de code sources** ont été révélés :

- **Symantec** en janvier 2012 confirme le vol du code source de certains de ses produits (Norton Antivirus Corporate Edition, Norton Internet Security, Norton Utilities, Norton GoBack et PCAnywhere). Ce vol a été revendiqué par un groupe de hackers se déclarant comme membres des Anonymous. Une demande de rançon sera faite par le voleur qui publiera finalement des extraits du code de Norton Utilities, PCAnywhere, et Norton Antivirus (voir cet article qui synthétise cette actualité).
- **VMware** en avril 2012 confirme qu'une partie du code source de VMware ESX a été volée (probablement chez un partenaire avec lequel certains codes sources sont partagés) et publiée sur Internet. Le voleur a lui indiqué avoir dérobé ces données chez un industriel chinois (voir cet article). Deux semaines plus tard, VMware publiera, par mesure de précaution, des correctifs de sécurité (voir cette annonce). En novembre l'éditeur réitérera ses recommandations et encouragera ses clients à appliquer scrupuleusement les mises à jour de sécurité.

- **Autres vulnérabilités**

Nous résumons ci-dessous les autres menaces mentionnées dans le nuage de mots. Dans la plupart des cas il s'agit de risques d'attaques pour des vulnérabilités critiques qui viennent juste d'être corrigées sur des produits très répandus. Ces événements 2012 n'ont pas forcement été très médiatisés (en particulier lorsqu'il ne s'agit pas de technologies de premier plan), mais la menace est réelle pour les installations concernées. Les messages spécifiques envoyés par le Cert-IST tout au loin de l'année permettent à nos adhérents d'être tenu informés de ces menaces.

- **Cisco Iron Port** : En janvier, nous avons attiré l'attention de notre communauté sur une vulnérabilité très critique concernant les démons « telnetd » sur Linux car cette vulnérabilité affectait aussi les équipements Cisco Iron Port.
- **WordPress** En mars puis en octobre, deux vagues de compromissions de sites WordPress ont été observées.
- **Adobe Flash :** En mai puis en août, des codes d'exploitation ont été publiés pour des vulnérabilités Flash (CVE-2012-0779 et CVE-2012-1535) récemment corrigées par Adobe.
- **PHP** : En mai, de nombreuses tentatives d'attaques ont été observées pour une vulnérabilité (CVE-2012-1823) affectant les serveurs web qui utilisent des scripts CGI en PHP. Ces attaques permettaient de compromettre les serveurs web qui n'avaient pas été mis à jour (un correctif ayant été diffusé en début de mois par PHP).
- **IBM ClearQuest :** En juillet, un code d'exploitation a été publié pour une vulnérabilité (CVE-2012-0708) corrigée en avril dans le contrôle ActiveX CQOle d'IBM Rational ClearQuest.
- **Samba** : En septembre, un code d'exploitation a été publié pour une vulnérabilité (CVE-2012-1182) corrigée en avril qui permettait de prendre le contrôle à distance des serveurs Samba qui n'avaient pas été mis à jour.
- **Sophos** : En novembre, le chercheur en sécurité Tavis Ormandy a publié une étude identifiant une série de vulnérabilités dans les produits antivirus de Sophos. Certaines pouvaient permettre de prendre le contrôle des machines utilisant un antivirus Sophos. Les failles les plus graves ont été immédiatement corrigées par Sophos.

- **EMC NetWorker** : En novembre, un code d'exploitation a été publié pour une vulnérabilité (CVE-2012-2288) corrigée en août qui permettait de prendre le contrôle à distance des machines utilisant une solution de sauvegarde EMC-Networker.

2.2 Ce dont la presse a parlé en 2012

En complément de sa veille technique sur les vulnérabilités, le Cert-IST suit également plus largement l'évolution des technologies et l'actualité en sécurité informatique. Nous publions ainsi chaque jour, dans notre bulletin de Veille Média, la liste des articles les plus intéressants que nous avons vus dans la presse francophone et anglophone. Le nuage de mots ci-dessous présente les mots qui ont le plus souvent été cités dans la veille media Cert-IST de 2012.

Nous passons en revue dans la suite de ce chapitre, les principales thématiques mises en évidence par ce nuage : ce sont les sujets d'actualité de 2012.

- **Cloud et BIG-Data**

Cette année encore, il y a eu beaucoup de discussions autour du « Cloud ». Les aspects sécurité à prendre en compte avaient déjà été largement discutés en 2010 et 2011, et le discours 2012 a, cette fois, plutôt insisté sur la réticence des RSSI à la mise en œuvre de solutions Cloud du fait des problèmes de sécurité induits. On pourrait donc résumer l'actualité du Cloud de ces dernières années de la façon suivante :

- **2010 : Attention danger ! :** les experts avertissent que l'engouement qui s'annonce pour la technologie Cloud posera des problèmes de sécurité importants.

- **2011 : Le détail des difficultés.** Le discours se développe et s'argumente. Les experts détaillent les différentes difficultés à prendre en compte, sur les volets contractuels, juridiques et techniques.
- **2012 : Prêts pour la mise en pratique.** Les RSSI connaissent désormais bien les difficultés et les chantiers à couvrir dans un projet Cloud. L'effort à déployer est bien sûr proportionnel au niveau de sécurité à assurer.

Parallèlement au Cloud, la presse a commencé à parler en 2012 de la sécurité du « **Big data** ». Le « Big data » désigne en tout premier lieu, l'explosion du volume de données traitées, et le fait que ces données proviennent maintenant de sources multiples et hétérogènes. On parle alors ici de technologies comme NoSQL ou Hadoop. En termes de sécurité les discussions sur le Big-data sont actuellement de deux types :

- « **Big data = small security ?** ». Les contraintes du « Big data » (le volume et le fait que ces données proviennent de multiples sources) pourraient faire que la sécurité n'est pas correctement prise en compte.
- « **Big data = Big Brother ?** ». La possibilité d'accumuler et de traiter de grands volumes de données rend tentante l'idée de collecter des données anodines sur les personnes et leurs habitudes. Cela pose clairement des problèmes de respect de la vie privée. On peut être inquiet par exemple à propos de toutes les données dont disposent de grandes compagnies comme Google ou Amazon sur nos habitudes de vie et nos activités quotidiennes.

Si l'explosion du volume des données traitées est un fait certain, **le « Big data » reste pour le moment un marché de niche** (peu de sociétés ont besoin de mettre en place un « big data »), comme le sont depuis de nombreuses années les « grilles de calcul ». **L'explosion du volume des données pointe aussi à plus long terme des problèmes de société** (avec par exemple l'internet des objets ou le « profilage » des consommateurs) du fait des atteintes possibles à la vie privée.

- **Smartphones**

Il n'y a pas eu en 2012 d'évolution significative de la menace visant les smartphones. Si l'on exclut l'aspect BYOD (que nous abordons ci-après dans un autre paragraphe), ce que nous disions dans notre Bilan 2011 reste vrai :

- Android est la plate-forme préférée des malwares mobiles.
- Il y a une montée en flèche du nombre de malwares identifiés par les éditeurs antivirus (mais comme le mentionne cet article cela pourrait être dû au fait que certains éditeurs comptent les variantes plutôt que les souches).
- La majorité des attaques consistent à cloner des applications à succès et à leurs ajouter une fonction cachée qui génère automatiquement des appels vers des numéros surtaxés.
- Ces applications malveillantes sont le plus souvent diffusées sur des marchés non officiels et visent des systèmes « rootés ».

On peut noter que :

- Les techniques intégrées en 2012 dans les malwares Android progressent en reproduisant celles que l'on connait déjà dans l'informatique traditionnelle (drive-by download, botnet, Ransomware).
- Le vol de données sur le smartphone (au travers d'applications malveillantes ou simplement peu scrupuleuses) est un risque réel, qui est encore mal maitrisé. Dans le cas d'attaques ciblées sur des personnes, le piégeage des téléphones mobiles est sans doute déjà une technique communément utilisée dans certains milieux (technique d'espionnage). Mais ces techniques vont se démocratiser avec la montée en force de plates-formes comme Android. La collecte déloyale de données est une illustration plus banale de la même catégorie de risque.
- En contre-point, et même si cela peut paraitre paradoxal, plusieurs organismes ont annoncé en 2012 avoir choisi Android comme base pour construire des solutions de téléphonie mobile sécurisée (par exemple, la NSA, Boeing, le gouvernement allemand). Android est choisi ici, non pas pour sa sécurité intrinsèque, mais parce qu'il s'agit d'une plate-forme ouverte.

Le smartphone est une plate-forme technologique qui ouvre des possibilités étonnantes pour le cyber-espionnage, et cela a été par exemple montré en 2012 par la publication du démonstrateur « PlaceRaider » : il s'agit d'un programme qui reconstitue une scène à partir des photos prises aléatoirement par un smartphone infecté. Par contre, il n'a pas encore été rendu public de cas d'incident où des smartphones avaient été vraiment utilisés dans des attaques réelles.

- **Réseaux sociaux**

Nous n'avons pas noté de réelle nouveauté sécurité en 2012 sur le sujet des réseaux sociaux, mais ces outils restent, bien sur, très présents dans l'actualité.

- **Hacktivisme**

En 2012, les mouvements hacktivistes ont continué à mener toute une série d'actions contre des sociétés et des états. Plusieurs épisodes Anonymous ont aussi montré certaines des limites de ce type de groupes, en particulier du fait de revendications parfois fantaisistes comme :

- Des annonces fracassantes d'attaques futures non réalistes (comme l'annonce d'une attaque le 31 mars 2012 des DNS racines - Opération « Blackout »),
- Etre à l'origine d'incidents qui se révèlent ne pas avoir été causés par ce groupe (par exemple, l'attaque en déni de service de GoDaddy ou l'annonce du vol de 1 million d'identifiants Apple sur un poste du FBI).

Bien sûr, dans le cas d'un mouvement comme les Anonymous (ou chacun peut se revendiquer comme Anonymous), ce genre de débordement n'est pas contrôlable par le groupe. Et cela ne remet pas en cause le fait que l'hacktivisme est une menace à prendre en compte par les entreprises.

- **BYOD**

Dans le nuage de mots, BYOD (Bring Your Own Device) est d'une taille bien modeste par rapport à l'impression que nous avons eu lors de notre Veille Media quotidienne : **Le BYOD est pour nous le sujet qui a été le plus commenté par la presse en 2012**.

Aujourd'hui, le phénomène du BYOD est essentiellement constitué par les smartphones et les tablettes personnelles que certains employés utilisent aussi pour leurs activités professionnelles. Il s'agit d'un phénomène émergeant, mais qui a de fortes chances de s'amplifier. A long terme, on peut même considérer le BYOD comme un phénomène d'externalisation complémentaire au Cloud : avec le Cloud, les serveurs quittent l'entreprise, et avec le BYOD c'est le terminal utilisateur qui disparait du parc. Les risques induits sont multiples (fuite de données vers Internet, intrusion dans l'entreprise via le terminal BYOD, etc.) et les solutions sont encore à chercher (sécuriser le terminal ou ne rien stocker dessus et le considérer comme un simple écran ?). Et le problème n'est pas uniquement technique : l'impact sur l'organisation du travail et la responsabilité juridique de l'entreprise sont des aspects tout aussi difficiles à résoudre.

Le BYOD est une menace latente, mais il n'existe pas encore, à notre connaissance, d'incident dans lequel des terminaux BYOD auraient été utilisés comme vecteur d'attaque. Compromettre le terminal BYOD d'un particulier et l'utiliser comme moyen d'entrer dans l'entreprise est sans aucun doute un scénario d'attaque réalisable dès aujourd'hui, mais on ne le verra probablement que dans le cas de cibles de grandes valeurs, pour lesquelles les autres scénarios d'attaques n'ont pas été possibles, ou se sont révélés plus complexes.

- **Cyber-espionnage et APT**

Les attaques par infiltration (que l'on nomme communément APT – Advanced Persistent Threat) ont été l'événement majeur de notre Bilan 2011. Bien entendu ce phénomène perdure en 2012 et **il constitue de notre point de vue la menace immédiate la plus préoccupante pour les entreprises**. Nous analysons plus complètement ce phénomène majeur dans le paragraphe 3.2.

- **La montée des états**

Depuis plusieurs années, les états ont pris une importance grandissante dans le paysage cyber :

- Tout d'abord, du fait de la **mise en place ou le renforcement de structures dédiées à la cyber sécurité**. Il s'agit par exemple de la création d'organismes nationaux consacrés à la sécurité informatique (comme la création en France de l'ANSSI en 2009), mais aussi plus récemment de l'officialisation de la possibilité de cyber-guerres. Dans ce second domaine, on pourra noter au printemps 2011, la publication par les USA du plan « Cyber 3.0 », dans lequel le DOD (Department of Defense) annonce que l'espace numérique devient un domaine de guerre à part entière comme la terre, la mer, l'air ou l'espace. En 2012, l'OTAN a également publié le « Manuel de Tallinn » qui étudie le droit applicable à la cyberguerre.
- Et d'autre part, dans la **médiatisation d'incidents où l'on soupçonne que les attaques puissent être d'origines étatiques**. On cite ainsi depuis plusieurs années la Chine comme probablement impliquée dans des attaques de cyber-espionnage ou les Etats-Unis et Israël (soupçonnées de l'attaque Stuxnet contre le programme nucléaire Iranien). En 2012, l'Iran a pour sa part été soupçonné de l'attaque Shamoon contre le pétrolier Aramco (compagnie pétrolière nationale d'Arabie Saoudite).

- **Cybercrime**

Le terme « cybercrime » désigne ici la délinquance informatique, c'est-à-dire les escroqueries visant, par le moyen de l'informatique, à dérober de l'argent aux particuliers ou aux entreprises. Il s'agit d'un domaine qui est devenu majeur dans les années 2005, et qui inclut des phénomènes comme :

- Les botnets (infection massive de machines utilisées ensuite pour des actions malveillantes : DDOS, Spam, etc.),
- Le vol de données bancaires (phishing),
- Les faux antivirus,
- Etc.

En 2012, il a été observé une montée en flèche du phénomène des « **ransomwares** », avec en particulier le malware « Reveton » (aussi appelé « malware de la Police ») : ce malware affiche un message prétendant venir de la Police, indiquant que l'ordinateur a été identifié comme impliqué dans des activités illégales (par exemple des téléchargements illégaux) et réclame le paiement d'une amende en ligne. Il s'agit d'une opération d'envergure et particulièrement bien faite (le même message a été adapté pour au moins 25 pays).

- **Vol de données personnelles**

Il y a eu en 2012, un très grand nombre d'annonces concernant des vols de données personnelles (typiquement des vols de bases de données de comptes contenant des logins, mots de passe, numéros de cartes bleues, etc.). Il ne s'agit pas d'un phénomène nouveau, mais il continue à s'amplifier d'année en année. Dashlane.com a publié en septembre 2012 un poster qui illustre ces vols de données de 2012 :

- Zappos : 24 millions de coordonnées clients volées en janvier 2012
- LinkedIn : 6,5 millions de comptes volés en juin 2012
- Apple : 12 millions de données relatives à des terminaux iPad, iPod et Iphone volés en septembre 2012
- Etc.

3) Les faits majeurs de 2012

Nous décrivons dans ce paragraphe les éléments qui nous paraissent les plus importants du point de vue d'une entreprise :

- SCADA : la menace progresse,
- APT et cyber-espionnage : un risque à prendre en compte,
- Attaques 0-day : un risque plus grand qu'estimé.

3.1 SCADA : la menace progresse

Dans le domaine de la sécurité des systèmes industriels, plusieurs attaques ont été médiatisés en 2012 :

- En avril, l'ICS-CERT émet une alerte concernant des tentatives d'attaques visant les sociétés de transport gazier (l'attaque consiste en l'envoi de mails piégés vers des personnels de ces sociétés).
- Durant l'été 2012, le malware Shamoon a infecté les réseaux informatiques de la société pétrolière Aramco (en Arabie Saoudite). Ce même malware aurait aussi infecté à la même période le producteur de gaz RasGas (au Qatar). Certaines sources pensent que ce malware aurait été conçu en Iran.
- En septembre, la société Telvent (groupe Schneider) annonce qu'elle a subi une intrusion. La cible visée par les attaquants serait le produit OASyS, que Telvent commercialise, et les clients utilisant ce produit. Certaines sources pensent que ces attaques proviennent de Chine.

Les deux premiers cas ne visent pas à proprement parler des installations industrielles (comme l'avait fait Stuxnet en 2010). **Il s'agit plus d'attaques visant des sociétés du domaine de l'énergie que d'attaques visant des systèmes SCADA**. Le dernier cas est, par contre, plus préoccupant puisqu'il vise lui un système SCADA particulier (OASys).

Au-delà de ces incidents, la préoccupation majeure reste :

- **Le faible niveau de protection dont bénéficient certaines installations industrielles**. Dans une note émise en octobre 2012 l'ICS-CERT indique par exemple avoir connaissance d'une liste de 500 000 équipements industriels apparemment accessibles depuis Internet. De même, certains constructeurs informés de failles avérées dans leurs équipements déclarent ne pas pouvoir les corriger. Cette nouvelle classe de failles a été tout d'abord baptisée ironiquement les « Forever-days » (en référence aux failles « 0-days »), mais on parle maintenant plutôt de vulnérabilités de type « Insecure by design » (qui ne peuvent pas être corrigées parce qu'intrinsèques à la conception du produit).
- **L'activité de plus en plus poussée dans le domaine de la recherche de failles**. Alors qu'en 2011 les vulnérabilités ont été plutôt découvertes par des novices du monde SCADA (des spécialistes de la recherche de failles IT), en 2012 des spécialistes du monde SCADA se sont eux aussi mis à chercher activement des vulnérabilités (cf. le projet nommé « BaseCamp » conduit par DigitalBond). La dernière découverte de ce groupe est une vulnérabilité dans la runtime du produit CoDeSys. Ce runtime est intégré dans plusieurs centaines de produits SCADA tiers qui se trouvent donc aussi touchés par la vulnérabilité.

La sécurité industrielle est un domaine où la menace progresse et où le niveau de sécurité de certaines installations parait encore très insuffisant. Cette situation est préoccupante.

3.2 APT et Cyber-espionnage : un risque à prendre en compte

Depuis plusieurs années, de plus en plus de sociétés sont victimes d'intrusions dans leurs systèmes d'information (attaques souvent désignées sous le terme d'APT : Advanced Persistent Threat), qui sont menées contre elles, à des fins d'espionnage industriel ou même de sabotage. Le phénomène des attaques par infiltration avait été identifié comme la menace numéro 1 dans notre bilan 2011. Et en 2012, cette menace est toujours très présente. Le tableau ci-dessous liste les annonces les plus significatives faites en 2012 sur des attaques de ce type.

Février	Verisign annonce qu'il a subi en 2010 des attaques par infiltration.
Février	Le Wall Street Journal annonce que Nortel a été victime d'intrusions dans ses réseaux pendant près de 10 ans.
Mars	La NASA annonce avoir subi en 2011 13 intrusions majeures dans ses réseaux.
Avril	Nissan annonce avoir découvert une attaque par infiltration dans ses réseaux.
Juillet	AlienVault annonce que le malware Sykipot aurait été utilisé dans des attaques visant l'industrie aéronautique.
Juillet puis octobre	Le Télégramme, puis L'Express annoncent que L'Elysée a subi des attaques par infiltration en mai 2012.
Septembre	SecureWorks annonce que le malware Mirage aurait été utilisé dans des attaques de cyber espionnage visant entre autres des sociétés du domaine de l'énergie.
Septembre	La société Telvent annonce avoir subi une intrusion visant son produit SCADA OASyS.
Novembre	Coca-Cola annonce avoir subi en 2009 une attaque qui pourrait avoir causé l'échec d'une acquisition en Chine.
Décembre	L'agence spatiale japonaise annonce que des informations sur ses nouvelles fusées on été dérobées par un virus informatique.

Le risque d'attaques APT concerne en tout premier lieu les entreprises ou les organisations qui sont exposées à la concurrence internationale. En effet, le risque de poursuite d'un attaquant qui serait découvert est faible du fait de la difficulté de poursuites judiciaires transfrontalières. Dans ce contexte, le rapport « gain/prise de risque » est à son maximum pour l'attaquant et l'attaque informatique est probablement la « meilleure arme » pour lui.

Il n'existe pas de solution facile pour contrer la menace APT, en particulier parce que ces attaques sont conçues pour exploiter les vulnérabilités de l'entreprise. Le Cert-IST a communiqué plusieurs fois sur ce sujet en 2012 (en interne vers ses adhérents tout d'abord, mais aussi lors de sa journée « Forum » annuelle) et a recommandé les actions suivantes :

- Renforcer les fondamentaux : sensibiliser les utilisateurs, renforcer les mots de passe, limiter les comptes administrateurs, protéger les données sensibles sur des serveurs sécurisés, appliquer les correctifs de sécurité et mettre en place une collecte et une gestion des logs.
- Mettre en place une surveillance active au sein de l'entreprise, au travers d'une structure responsable de la supervision de la sécurité.
- Définir une procédure de réaction en cas d'incident définissant le comportement à adopter et les personnes à impliquer.

Les entreprises exposées à la concurrence internationale ne doivent plus se demander si un jour elles seront touchées ou non par une attaque par infiltration (APT), mais quand cela se produira. Elles doivent surtout se préparer à cet événement en limitant son impact potentiel et en développant leur capacité de détection et de réaction face à ce type d'incident.

3.3 Attaques 0-days : un risque plus grand qu'estimé

On appelle « 0-day » des attaques qui utilisent des vulnérabilités jusque-là inconnues, qui ont été gardées secrètes par leur découvreur jusqu'au jour où elles ont été utilisées dans une attaque. Puisque la vulnérabilité utilisée est inconnue, il est difficile de s'en protéger et l'on ne peut que chercher à limiter l'impact lorsqu'une attaque de ce type réussit.

Les attaques 0-day existent depuis longtemps. Autour des années 2005, l'arrivée des fuzzers et la recherche accrue sur les failles de sécurité, a transformé cette menace, qui était jusque-là plutôt théorique, en un phénomène réel. Et on sait depuis cette époque, qu'une attaque 0-day est un risque possible. Par contre, on se rend compte désormais que le nombre de failles 0-days dont disposent les attaquants est plus important que ce que l'on pensait. En 2010, il a été constaté par exemple que le malware Stuxnet utilisait pour une seule attaque quatre 0-days, et cela a été considéré comme un fait tout à fait exceptionnel. En 2012, l'étude « Elderwood » publiée par Symantec montre que certains groupes de pirates (il pourrait s'agir en l'occurrence d'un groupe soutenu par un état) semblent disposer d'un grand nombre de vulnérabilités 0-days. De même, une autre étude (baptisée « Before we knew it » montre qu'une vulnérabilité 0-day pourrait être utilisée pendant plus de 300 jours avant d'être finalement découverte.

La prise en compte de ce risque nécessite de développer des capacités similaires à celles déjà évoquées pour les attaques APT :

- Etre capable de détecter au plus tôt que cet événement s'est produit,
- Limiter la conséquence pour le S.I. de la compromission d'un poste de travail ou d'un serveur,
- Définir une procédure d'isolation, d'analyse d'impacts et de remise en service des éléments compromis.

Ces différents éléments montrent que la possibilité d'une attaque 0-day doit être considérée comme un événement probable et doit donc être intégré au processus de gestion de la menace.
Cela implique en particulier de considérer comme un fait certain qu'un jour un poste de travail ou un serveur de l'entreprise sera victime d'une attaque réussie.

Nota : Il existe des produits qui se revendiquent comme conçus pour arrêter les attaques 0-day. Il s'agit par exemple d'outils capables de détecter des comportements anormaux (comme les débordements de pile) et de les stopper. Cependant, ces outils ne sont pas efficaces à 100% et ne permettent pas d'éliminer complètement le risque.

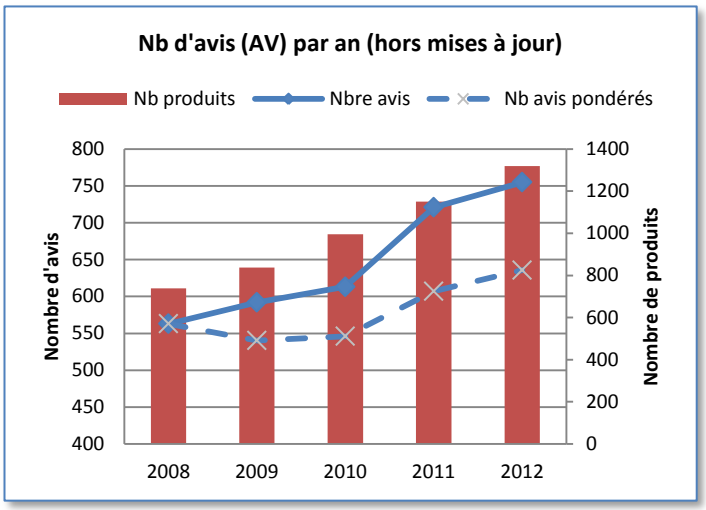
4) La production du Cert-IST en 2012

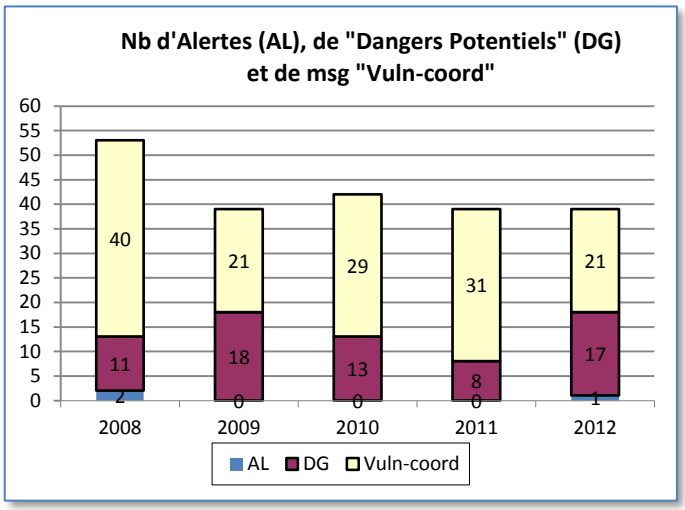
4.1 Veille sur les vulnérabilités et des menaces

Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST suit de façon continue les différentes sources d'informations (annonces constructeurs, blogs sécurité, mailing-lists, échanges privés entre CERT, etc.) de façon à être au courant des nouvelles vulnérabilités. Ces informations sont analysées quotidiennement afin de fournir à nos adhérents des informations triées, qualifiées et prioritisées. 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'attaque – des "exploits" – ont été publiés.
- Des **Alertes**, des **Dangers Potentiels** et des **messages "Vuln-coord"**. Les Alertes du Cert-IST sont utilisées pour les menaces majeures nécessitant un traitement prioritaire. L'émission d'une alerte est un événement rare : par exemple le Cert-IST a émis en 2008 une alerte pour le virus Conficker et une pour la vulnérabilité DNS (Kaminsky). 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 faiblesses (quelque soit leurs probabilités d'être utilisées dans des attaques)

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





Ainsi, en 2012, le Cert-IST a publié :

- **755 avis de sécurité**, suivis de façon continue au cours de l'année avec 2128 mises à jour mineures et 85 mises à jour majeures. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), et ce phénomène n'est pas dû à l'augmentation du nombre de produits suivis par le Cert-IST (cf. la courbe pondérée, qui prend en compte le nombre de produits ayant généré des avis au cours de l'année). Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène qui ne se tarie pas : invariablement, d'année en année, des vulnérabilités sont trouvées dans les produits qui constituent le S.I. de l'entreprise. Le maintien du niveau de sécurité passe donc forcement par une application régulière des correctifs de sécurité sur ces produits. Au

31/12/2012 le Cert-IST suivait les vulnérabilités concernant 1320 produits et 10 312 versions de produits.

- **1 Alerte, 17 Dangers Potentiels et 21 messages "Vuln-coord"**. L'alerte publiée cette année par le Cert-IST concerne le client **Java** installé sur les postes de travail (composant JRE) et fait suite à toute une série d'attaques Java vues au cours de l'année. Le chapitre 2.1 analyse plus en détail les Alertes et Dangers Potentiels émis en 2012 par le Cert-IST. On peut noter globalement que les chiffres 2012 pour les Alertes et Dangers sont en augmentation par rapport à 2011 et reviennent à des valeurs comparables à 2009.

4.2 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 recense les articles les plus intéressants parus sur Internet sur un échantillon de sites francophones et anglophones traitant de sécurité.
- Un bulletin mensuel de veille SCADA présente une synthèse de l'actualité sur la sécurité des systèmes de contrôle industriel.
- Un bulletin mensuel généraliste donne une synthèse de l'actualité du mois (en termes d'avis et d'attaques) et traite de sujets d'actualité au travers d'articles rédigés par le Cert-IST.

5) Conclusions

- **L'année 2012 montre à nouveau l'importance de la gestion des vulnérabilités pour l'entreprise**

Chaque année, plus de 4000 vulnérabilités sont publiées sur Internet. Le recueil de cette information, son analyse et son classement, sont une partie significative du travail quotidien du Cert-IST. Il donne lieu à l'émission d'environ 750 avis de sécurité qui alimentent les processus de gestion des correctifs chez nos adhérents. Ce travail de fond leur permet de maintenir leurs installations au meilleur niveau de sécurité.

- **La gestion des vulnérabilités ne se limite pas au déploiement de correctifs**

Lorsqu'une menace particulière apparait, le Cert-IST émet vers ses adhérents des messages spécifiques les informant de l'imminence de l'événement (Alerte ou Danger Potentiel) et des moyens disponibles pour s'en protéger. Cela permet à l'entreprise d'évaluer son exposition et de décider des mesures les plus adaptées et du timing de leur déploiement.

Enfin, l'entreprise doit considérer que la compromission d'un poste de travail ou d'un serveur est un événement possible (du fait d'une attaque 0-day ou d'une malveillance interne) et l'architecture du S.I. doit être conçue pour résister à cette éventualité. La détection rapide et le traitement des infections doivent permettre un retour rapide à une situation normale.

- **L'entreprise doit faire face à un risque accru d'attaques**

Depuis de nombreuses années, l'entreprise sait traiter de cette façon des infections virales ordinaires. Mais la menace a changé, et il faut désormais faire face à des attaques intelligentes pilotées directement par des personnes (ou des groupes) déterminés. Les attaques de cyber-espionnage (APT) ou la montée de la menace contre les systèmes SCADA montrent clairement ce changement.

- **Les attaques peuvent être très sophistiqués**

Les attaques 0-day, ou les techniques de contournement des moyens de protections classiques (antivirus, anti-débordement mémoire, protection par bacs à sable, etc.) montrent le niveau d'expertise technique atteint par les attaquants. De même, les schémas d'attaques sont aujourd'hui bien plus élaborés qu'auparavant. Par exemple, un attaquant pourra tout d'abord compromettre un site web qu'il sait fréquenté par sa victime, pour infecter celle-ci lors de sa visite sur le site, et ensuite se propager depuis son poste de travail vers les serveurs critiques au sein de l'entreprise.

Les attaquants sont aujourd'hui des professionnels disposant d'un panel étendu de compétences : acheter des 0-days, développer des exploits ou gérer des infrastructures d'attaques sont des outils qu'ils ont facilement à leur disposition. De même, pour les attaques les plus pointues, des développements spécifiques sont tout à fait possibles : piéger un smartphone ou une tablette, s'infiltrer dans une infrastructure Cloud sont, des éventualités parfaitement réalistes.

- **L'évolution des technologies demande une ouverture de plus en plus grande**

Les réseaux sociaux, le Cloud ou le BYOD sont des exemples de l'évolution rapide des technologies. Celles-ci deviennent de plus en plus présentes dans notre vie quotidienne, jusqu'à changer profondément nos modes de communication (Tweeter, Facebook) et nos usages (beaucoup d'utilisateurs réclament désormais un accès universel à leurs données : Anywhere, Anytime, Anyway). Cette évolution augmente fortement la surface d'attaque de l'entreprise.

- **Il faut composer avec une situation complexe**

Le RSSI se trouve en face d'une situation complexe, entre des attaques de plus en plus sophistiquées et des demandes utilisateurs pour toujours plus d'ouverture vers les nouvelles technologies. Le Cert-IST, au travers de son activité de veille technologique et ses bilans, lui donne une vision argumentée de la menace. Et pour nous, celle-ci est en augmentation. Les attaquants savent où se trouvent généralement les points faibles des entreprises (comme parfois le manque de cloisonnement des réseaux internes ou un niveau de surveillance interne trop faible) et exploitent ces faiblesses. De nombreux organismes nationaux appellent à un renforcement du niveau de sécurité. Par exemple, le guide « 20 Critical Security Controls For Effective Cyber-Defense » publié aux USA ou le « Guide de l'hygiène informatique » publié en France par l'ANSSI en octobre 2012, recommandent tous les deux une application stricte des principes traditionnels d'une sécurité en profondeur (sécurisation des plates-formes, application des correctifs de sécurité, segmentation des réseaux, limitation des privilèges, etc.). Ils mettent en avant des mesures strictes que certains jugeront comme contraignantes ou inadaptées à l'environnement informatique actuel. Mais ils présentent en fait, les principes de référence d'une architecture sécurisée et maitrisée.

Fin du document