1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée. L'objectif est de retracer les événements marquants de 2011 de façon à mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Dans un premier temps, nous faisons un bilan des principales attaques survenues au cours de l'année (cf. chapitre 2).

Ensuite, nous identifions les événements les plus marquants de l'année et analysons la façon dont ils pourraient influencer le domaine de la sécurité dans les années à venir (cf. chapitre 3).

➢ 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) Les vulnérabilités, virus et attaques en 2011

2.1 Une évolution de la nature des cibles

➢ La menace change de nature et se fait plus indirecte

En termes de menaces, l'année 2011 marque un changement par rapport aux années précédentes. Jusqu'en 2010, les menaces les plus courantes étaient liées à la découverte de nouvelles vulnérabilités impactant les équipements ou les logiciels (et en particulier à la découverte de vulnérabilités "0-day", c'est-à-dire de vulnérabilités inconnues jusqu'à ce qu'elles soient utilisées dans des attaques réelles), ou à la propagation massive d'une attaque (campagne de compromissions de sites web, ou même plus anciennement propagation d'un ver). En 2011 par contre, les menaces qui ont été traitées étaient d'une autre nature et plus indirectes. Il s'agit par exemple du vol de données SecurID chez RSA, ou des multiples incidents relatifs à TLS/SSL (attaques protocolaires "BEAST" ou compromission des autorités de certification Comodo et DigiNotar). En 2011 les équipes sécurité des entreprises ont ainsi dû répondre à des questions comme :

- Mes accès VPN sont-ils encore sûrs (suite à l'incident RSA SecurID) ?
- Puis-je encore faire confiance à HTTPS (suite aux incidents TLS/SSL) ?
- Faut-il se protéger plus activement contre les attaques DOS (suite à la publication d'outils d'attaque) ?
- Le groupe "Anonymous" est-il une menace à prendre en compte ?
- Etc…

On le voit sur ces exemple, les menaces en 2011 étaient plus indirectes que celles traitées les années précédentes (elles n'étaient que la conséquence indirecte d'une attaque subie par un tiers) et souvent complexes à évaluer (à quel point mon système d'information est-il affaibli par ces événements de sécurité ?).

En 2011, si le nombre de vulnérabilités n'a pas augmenté de façon très significative, et si le nombre d'alertes est resté faible (cf. chapitre 2.2 ci-dessous), la menace est pourtant restée importante du fait de ces événements d'une nouvelle nature. Le nombre et la gravité des incidents annoncés publiquement (probablement du fait de l'évolution législative dans ce domaine) ont en particulièrement largement augmenté.

➢ Des attaques qui utilisent l'informatique pour viser l'entreprise

L'actualité de 2011 confirme également que les attaques informatiques ont changé d'objectifs (ou plutôt qu'un nouveau type d'attaque s'est ajouté aux attaques déjà vues jusque là) :

- Dans les années 2000 les attaques saturaient les réseaux (du fait de propagations virales exponentielles).
- Depuis 2006 les attaques se sont tournées vers le poste de travail de l'utilisateur, dans le but d'escroquer cet utilisateur, ou d'inclure sa machine dans un botnet.
- En 2011 les attaques visent l'entreprise (espionnage industriel ou sabotage) et l'attaque informatique est simplement un outil pour arriver à la finalité visée. Pour l'attaquant, l'informatique est un vecteur pour entrer dans l'entreprise et aussi le conteneur qui renferme les données vitales de l'entreprise qu'il cherche à dérober.

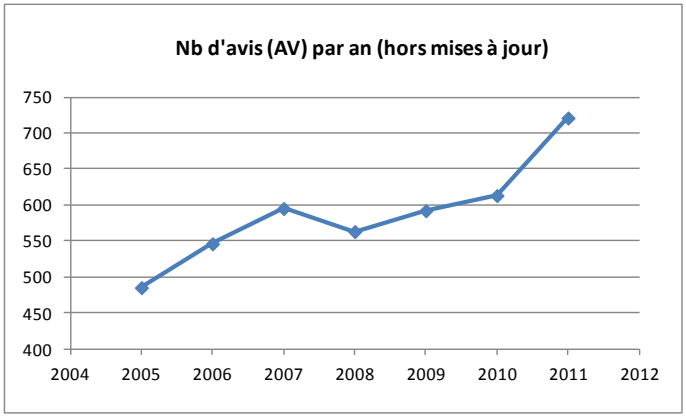
2.2 Les chiffres de 2011

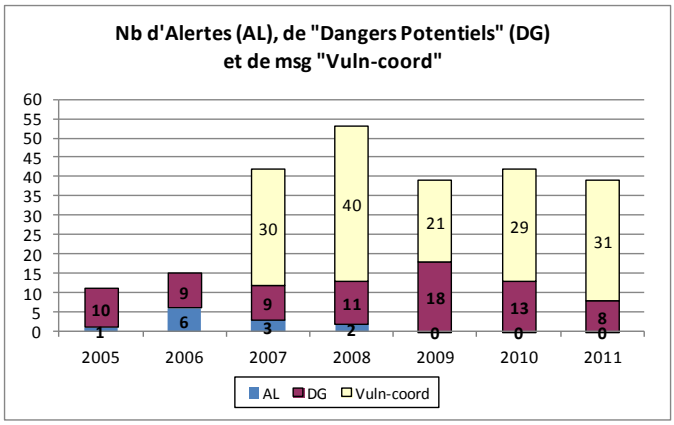
➢ Les avis et alertes de sécurité

Le Cert-IST a publié en 2011 :

- **721 avis de sécurité**. Ces avis décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis ont été suivis de façon continue et ont donné lieu au cours de l'année à 2427 mises à jour mineures et 84 mises à jour majeures (ces dernières correspondent typiquement au cas où des programmes d'attaque -des "exploits"- ont été publiés). Le nombre d'avis est en augmentation par rapport à 2010 (cf. la courbe à la page suivante), mais cette augmentation est avant tout due à l'augmentation du nombre de produits suivis par le Cert-IST. Au 31/12/2011 le Cert-IST suivait les vulnérabilités concernant 1150 produits et 9248 versions de produits.

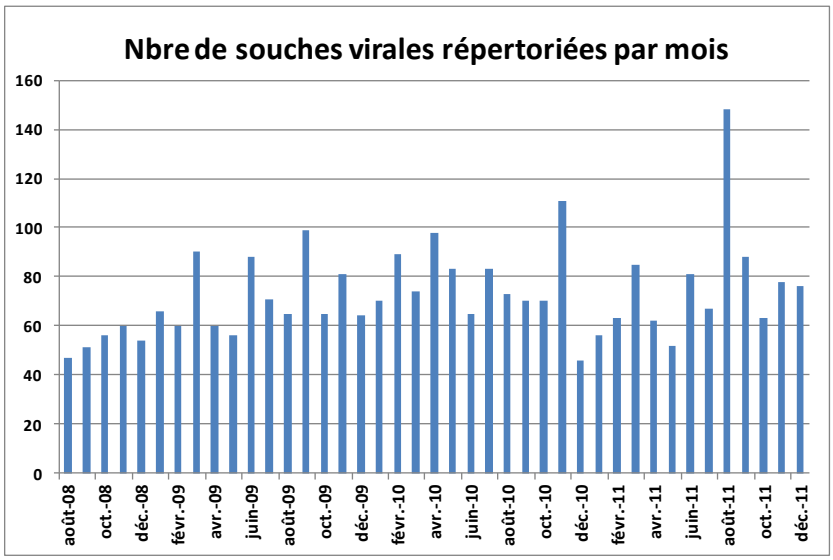
- **0 Alerte, 8 Dangers Potentiels et 31 messages "Vuln-coord"**. Les Alertes du Cert-IST sont utilisées pour les menaces majeures nécessitant un traitement prioritaire. La dernière Alerte émise par le Cert-IST était Conficker (fin 2008). Les Dangers Potentiels décrivent des menaces significatives mais 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. En termes d'attaques, les chiffres 2011 sont en baisse par rapport aux années précédentes (cf. le nombre de Dangers et d'Alertes dans l'histogramme de la page suivante). Cependant, comme vu précédemment la menace a changé de nature : les attaques sont moins nombreuses mais leurs conséquences sont potentiellement plus graves.





➢ Les virus en 2011

Le Cert-IST suit de façon continue les nouvelles menaces virales, en se basant sur les données publiées par les principaux éditeurs antivirus. Cette analyse se fait sur les souches virales, sans prendre en compte les variantes de chaque virus. L'histogramme ci-dessous donne un aperçu de cette activité. On y voit que si l'on écarte les épiphénomènes (les pics qui apparaissent sur l'histogramme) la courbe globale reste relativement stable (aux alentours de 60 souches par mois).
Dans le même temps, le nombre de variantes répertoriées par les éditeurs antivirus a explosé. Il suffit pour s'en convaincre de visiter la page de McAfee ou de Sophos listant les dernières variantes virales répertoriées pour s'en rendre compte : alors qu'il y a 3 ans les virus s'appelaient "Virus.B" (variante B du virus), ils ont maintenant des noms tel que "Generic.dx!12536D125737" (variante "12536D125737" d'un comportement générique considéré comme malveillant).



2.3 Les attaques médiatisées en 2011

Le tableau ci-dessous donne une synthèse des attaques et vulnérabilités les plus médiatisées de l'année 2011.

Evénement	Description
Attaque contre le **ministère de l'Economie et des Finances** – Bercy (Mars 2011)	Début mars 2011, le ministère de l'Economie et des Finances annonce avoir subi une attaque visant à voler des documents relatifs au G20. L'attaque aurait débuté en décembre par la compromission silencieuse de plusieurs postes de travail et aurait nécessité des travaux de ré-installation et de sécurisation sans précédents pour s'assurer que tous les éléments touchés avaient été totalement désinfectés.
Attaque contre **RSA** et vol de données SecurID. (Mars 2011)	En mars 2011 RSA annonce qu'il a subi une attaque et que des données relatives aux calculettes d'authentification SecurID lui ont été volées. Ces données seront en particulier utilisées fin mai 2011, pour tenter d' attaquer l'entreprise Lockheed Martin. Il s'agit au niveau international de l'exemple le plus démonstratif des nombreuses attaques APT annoncées en 2011 (cf. la liste donnée au chapitre 3.1.2), dont l'attaque de Bercy (mentionnée ci-dessous) ou cette de la société Areva (en septembre) sont également des exemples
Mac Defender : un faux antivirus qui vise Mac-OSX (Mai 2011)	Début mai 2011, la société Intego a mis à jour un logiciel malveillant se faisant passer pour un anti-virus MacOS X. Il piège les utilisateurs utilisant des moteurs de recherche en leur signalant qu'un virus a été détecté sur leur système et en leur proposant d'installer le logiciel anti-virus Mac Defender. Une fois installé, ce dernier va collecter des données sensibles (informations bancaires) sur le poste de l'utilisateur. Très classique dans le monde Windows, le faux anti-virus fait donc en 2011 son apparition sur MacOS.
Attaques **Lulzsec** et **Anonymous**	Depuis la fin d'année 2010, de nouvelles formes de cyber-activisme ont vu le jour, avec notamment les actions menées par les groupes Anonymous et Lulzsec. Parmi les actions les plus médiatisées, l'on retiendra Paypal, Visa, MasterCard et Sony du côté des Anonymous, le Sénat américain et la CIA pour Lulzsec. En juin 2011, ces deux groupes auraient fusionné et fondé le mouvement appelé Opération AntiSec, visant cette fois les gouvernements réduisant la liberté d'expression sur Internet.
Attaques contre **Sony** (Avril 2011)	Survenue entre les 17 et 19 avril 2011, une attaque historique contre les jeux en ligne Sony (PlayStation Network) a entrainé la mise hors service mondiale du site. Ce dernier n'a en effet pu être redémarré que le 15 mai 2011. Durant cette attaque, des millions de données personnelles ont été dérobées.
Outils d'attaques DOS contre Apache : "**Apache killer**" (Août 2011)	En août un programme baptisé "Apache killer" est diffusé sur Internet. Il utilise la fragmentation HTTP (entête "Range:") pour saturer un serveur Apache.
Outils d'attaques DOS contre SSL : **THC-SSL-DOS** (Octobre 2011)	En octobre 2011 le groupe THC publie un outil qui exploite la fonction SSL de "re-négociation" pour saturer un serveur utilisant SSL (par exemple un serveur HTTPS).
Ver **Morto** (Août 2011)	Ver qui se propage en cherchant des machines Windows disposant d'un accès RDP et en essayant, via RDP, une série de mots de passe triviaux. C'est le premier cas de ver RDP recensé. Il a connu une propagation assez faible (voir ce bilan publié par Microsoft).
Compromission d'Autorités de Certification (AC) **Comodo** (mars 2011) et **DigiNotar** (septembre 2011)	En mars 2011, la société de certification Comodo a annoncé avoir été victime d'une intrusion informatique ayant permis la génération de neuf certificats SSL frauduleux. Ces derniers peuvent permettre à une personne malveillante d'usurper l'identité d'un site web légitime et de réaliser des actions nuisibles sur un système vulnérable (vol d'identifiants de connexion ou d'informations sensibles etc.). Le 30 août 2011, c'est au tour de Google

	d'alerter sa communauté au sujet d'un certificat frauduleux émis par l'autorité de certification hollandaise DigiNotar (à son insu) et usurpant l'identité de "google.com". L'enquête réalisée sur cet incident (voir ce rapport rédigé par FoxIT) montre que la compromission de DigiNotar remonte à début juillet 2011 et que la sécurité de l'organisme DigiNotar est très largement défaillante, ce qui, pour une société de type "Autorité de Confiance" (organisme critique pour la sécurité des certificats émis) est un comble. Les pirates ayant pris la main sur les moyens de gestion des certificats, ont pu générer plus de 250 certificats frauduleux de sites web incontournables de l'Internet dont google.com, microsoft.com, twitter.com, facebook.com, etc. Suite à cet incident la société DigiNotar cesse son activité et se déclare en faillite.
Vulnérabilité "**The Beast**" visant SSL (Septembre 2011)	Deux chercheurs en sécurité (Juliano Rizzo et Thai Duong) ont réussi à exploiter une faille dans SSL/TLS 1.0. Ils en ont fait la démonstration (via un programme de démonstration baptisé BEAST : Browser Exploit Against SSL/TLS) à Buenos Aires le 23 septembre 2011, lors de la conférence Ekoparty.
Malware **DuQu** (octobre 2011)	Le malware DuQu (dont le nom fait référence au préfixe « ~DQ » des fichiers qu'il crée) a été annoncé initialement comme étant sans doute le successeur de Stuxnet parce que les codes des 2 malwares se ressemblent et que DuQu semblait viser les sociétés du monde industriel. Ces 2 constats ont été démentis par la suite. DuQu semble avoir été utilisé ponctuellement (pas de propagation automatique) contre un petit nombre de sociétés (probablement choisies par l'attaquant). Il pourrait donc s'agir d'attaques de type "APT".
Ver **JBOSS** (octobre 2011)	JBOSS est un serveur web de type J2EE. Ce ver JBOSS utilise une vulnérabilité connue et corrigée depuis plus d'un an pour se propager de serveur JBOSS à serveur JBOSS. Des cas d'infections en France nous ont été signalés.

3) Analyse des événements les plus marquants

3.1 Attaques par infiltration (APT) : La menace majeure en 2011

Le terme anglo-saxon de « APT » (Advanced Persistent Threat) existe depuis au moins 2007, mais est devenu vraiment populaire à partir de 2010. Il est utilisé pour désigner les attaques informatiques par infiltration qui consistent à :

- Infecter un composant interne du système d'information,
- Rester invisible et survivre le plus longtemps possible sur le système infecté,
- Effectuer des actions malveillantes, le plus souvent en étant téléguidé par un attaquant distant.

Nous avons déjà parlé de ces attaques dans notre bilan 2010, mais 2011 renforce notre constat 2010 : les attaques par infiltration sont devenues une préoccupation majeure pour les entreprises.

- De nombreuses attaques de ce type ont été rendues publiques en 2011.
- Elles visent le plus souvent des éléments stratégiques pour l'entreprise : vol de données (espionnage industriel) ou cyber-sabotage.

L'attaque qu'a subie RSA en mars 2011 est un exemple typique d'attaque par infiltration, et nous la détaillons donc ci-dessous.

3.1.1 Une APT typique : l'attaque de RSA et de Lockeed Martin

En mars 2011, la société RSA (très connue pour ses produits cryptographiques et sa calculette d'authentification "SecurID") a été attaquée par des pirates. Voici le scénario de l'attaque, telle que décrite par RSA (dans l'annexe du document Anatomy of an Attack) :

- Un email piégé est envoyé par les pirates à certains employés de RSA. L'email contient en attachement un fichier Excel embarquant un contenu flash malveillant qui utilise la vulnérabilité 0-day CVE-2011-0609 pour infecter les postes de ces collaborateurs (vulnérabilité corrigée depuis, et décrite dans l'avis **CERT-IST/AV-2011.151**).
- Une variante de l'outil d'administration à distance Poison Ivy est alors automatiquement installée sur les postes compromis. Elle est ensuite utilisée par les pirates pour agir à distance sur le poste cible.
- Les attaquants progressent au sein du système d'information de RSA, y collectent des données confidentielles et exfiltrent ces données à l'extérieur de RSA, en les envoyant sur des serveurs FTP.

Les données volées à RSA sont relatives aux calculettes d'authentification "SecurID". Bien que RSA n'ait jamais confirmé cette information, il pourrait s'agir des couples "(Numéro de série, Clé secrète)" des calculettes SecurID (ou d'un sous ensemble de ces calculettes) que RSA a vendu à ses clients. Ces données sont très sensibles car elles permettent à l'attaquant de créer de fausses calculettes SecurID. L'attaquant peut ensuite utiliser ces fausses calculettes pour obtenir un accès sur les infrastructures d'un client RSA. Il doit cependant pour y parvenir collecter des informations complémentaires (par exemple le nom du compte d'accès protégé par SecurID, le PIN de l'utilisateur, etc…) ce qui rend l'attaque non triviale.

Deux mois plus tard (fin mai 2011), la société Lockeed Martin (une des principales sociétés américaines du domaine de la défense) annonce avoir repoussé des tentatives d'attaques informatiques et que ces attaques ont utilisé les données volées chez RSA et relatives aux tokens RSA SecurID. Cette information sera ultérieurement confirmée par RSA (voir cette annonce de RSA) qui propose alors de remplacer l'intégralité des calculettes SecurID compromises lors de l'attaque de mars 2011.

Ces attaques contre RSA et SecurID montrent :

- d'une part qu'une entreprise leader dans le domaine de la sécurité peut subir une attaque sévère, qui pénètre en profondeur ses réseaux et aboutit au vol de données très confidentielles.
- d'autre part, que les attaquants n'agissent pas au hasard. Ils élaborent des plans minutieux, avec des visées à long terme. Les données volées à RSA ont ainsi permis à l'attaquant de mettre en place les attaques qui ont ensuite été tentées contre la société Lockeed Martin.

En octobre 2011, lors de la conférence annuelle de RSA, l'un des dirigeants de cette société a indiqué à l'occasion de son discours que l'attaque qu'a subi sa société a très certainement été orchestrée par un état (sans préciser s'il s'agit ou non de la Chine, qui est le pays le plus souvent évoqué pour les attaques de ce type).

3.1.2 Les autres attaques par infiltration découvertes en 2011

L'attaque qui a visée RSA n'est pas la seule survenue en 2011 dans la catégorie des attaques par infiltration. Voici un inventaire non exhaustif des attaques de ce type publiquement annoncées en 2011.

Attaques « Night Dragon » (février)	McAfee publie en février 2011 un rapport pour des attaques par infiltration datant de fin 2009 visant des entreprises du monde de l'énergie, des hydrocarbures et de la pétrochimie
NASDAQ	En février 2011, le FBI a annoncé que la bourse américaine du NASDAQ a été victime d'une intrusion informatique. Des fichiers suspects ont en effet été découverts sur les serveurs du groupe NASDAQ OMX et le logiciel de transactions en ligne "Directors Desk" a été affecté suite à cette attaque (voir cet article publié par clubic.com).
Le ministère de l'Economie et des Finances – Bercy (mars)	Le ministère de l'Economie et des Finances annonce avoir subi une attaque visant à voler des documents relatifs au G20. (voir cet article publié par Le Monde)
La Commission Européenne	La Commission Européenne annonce qu'elle a subi une attaque sérieuse. La nature de l'attaque n'est pas détaillée (voir cet article publié par Le Monde et celui-ci publié par ComputerWorld)
Le Parlement australien (mars)	Les postes du premier ministre australien et de plusieurs membres du gouvernement ont été victimes d'un piratage. Cette attaque, qui aurait débuté en février 2011, aurait visé 10 ministères australiens et permis d'accéder à des milliers d'e-mails (voir cet article d'undernews.fr).
Areva (septembre)	Le groupe nucléaire français Areva a été la cible d'un piratage qui l'a conduit à prendre des mesures de sécurité d'urgence. Ces attaques qui, selon les dirigeants de l'entreprise, n'auraient impacté que des informations non critiques, dureraient depuis plusieurs années.
Mitsubishi Heavy Industries (septembre)	Cette société japonaise du domaine de la défense annonce qu'elle a été l'objet de cyber-attaques (voir cet article Reuters). Des données sur des équipements militaires et des centrales nucléaires auraient été volées (voir cet article Reuters)
Attaques « Lurid » (septembre)	Série d'attaques ciblées utilisant le malware "Lurid" et ayant contaminés quelque 1465 ordinateurs de diplomates, ministères, agences de recherche et entreprises dans le bloc de l'ex-Union soviétique. Découverte par TrendMicro, cette attaque serait une combinaison de plusieurs attaques exploitant des failles dans des logiciels populaires (Adobe, Microsoft) et utilisant des serveurs de type "Command & Control".
Attaques « Nitro » (octobre)	Cyberattaque, dévoilée par Symantec, visant de grands noms de l'industrie chimique et de la défense. Elle s'est déroulée de fin juillet à septembre 2011 et a utilisé une technique simple mais efficace : envoie d'e-mails malveillants afin d'installer le cheval de Troie "Poison Ivy" sur les postes des victimes.

Attaques de sociétés norvégiennes du domaine énergie et défense (novembre)	Le gouvernement norvégien annonce en novembre 2011 qu'au moins une dizaine de sociétés norvégiennes auraient été victimes au cours de l'année de cyber-espionnage. (voir cet article du WashingthonPost)

3.2 Des réseaux insuffisamment sécurisés

Certaines des attaques vues en 2011, par exemple celles subies par RSA ou DigiNotar, posent de sérieuses questions sur l'efficacité de la sécurité au sein de ces organisations :

- Dans le cas RSA, comment la compromission de 2 postes de travail peut-elle permettre à un attaquant de se déplacer à l'intérieur de l'organisation jusqu'à atteindre et voler des données très sensibles (les données d'authentification des calculettes SecurID vendues par RSA à ses clients) ?
- Dans le cas de DigiNotar, comment un attaquant externe a-t-il pu s'infiltrer au sein du système d'information et générer plus de 500 faux-certificats numériques. Une autorité de certification (comme DigiNotar) est a priori un organisme pour lequel on attend un niveau de sécurité irréprochable. Cette attaque montre que c'est loin d'être le cas pour DigiNotar.

De même, il est troublant de voir le nombre de sites web "de confiance" qui ont subi une compromission en 2011 :

- SourceForge.net (janvier 2011)
- Wordpress.com (avril 2011)
- Kernel.org (août 2011)
- MySQL.com (septembre 2011)

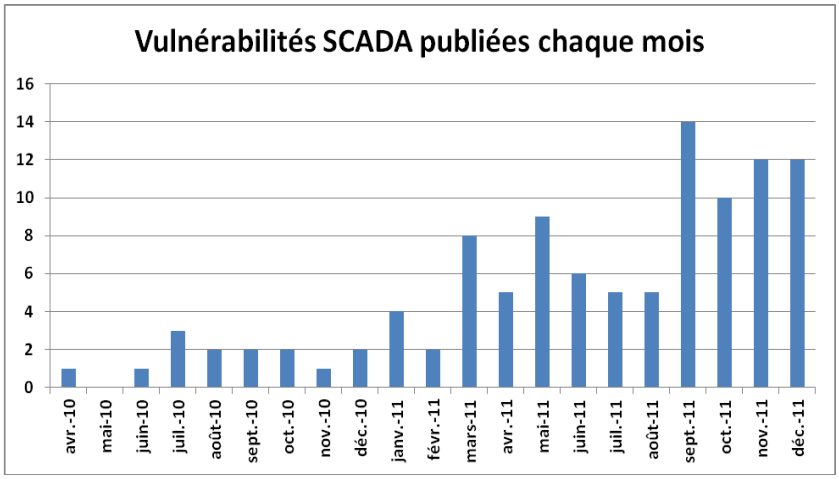
Plusieurs éléments peuvent expliquer ce constat :

- Le facteur humain. Assez souvent les compromissions de ce type s'appuient sur une faiblesse du maillon humain. Par exemple, l'utilisateur a le même mot de passe pour de multiples comptes différents (par exemple son compte FaceBook et son compte d'accès sur un serveur).
- La faiblesse des architectures sécurités mises en place. Dans certains cas, les architectures de securité au sein des entreprises semblent insuffisantes. Les contraintes économiques, la recherche d'une efficacité maximum poussent souvent à une sécurité "low cost" incompatible avec l'exposition croissante aux menaces du système d'information de l'entreprise.
- Des attaquants plus audacieux. Les attaques récentes montrent que les attaquant n'hésitent pas à attaquer une entreprise, et parfois dans des attaques allant profondément dans le système d'information visé. L'attaque informatique est désormais un outil courant, dans l'arsenal à la disposition des groupes activistes (aspect développé au chapitre 3.4) ou d'espionnage (par des concurrents ou des états) qui veulent viser une entreprise particulière.

3.3 SCADA : la menace de demain ?

En 2010, le ver Stuxnet, qui avait été conçu pour attaquer certains systèmes SCADA, a mis en évidence le danger auquel les systèmes de l'informatique industriel sont exposés. Stuxnet a été le révélateur d'une menace latente, que les entreprises connaissaient, mais que personne ne pouvait imaginer voir se produire dès maintenant. Il a été sans aucun doute un accélérateur pour les travaux de sécurisation déjà en cours sur ces infrastructures industrielles.

L'année 2011 montre que les chercheurs de failles (qui ont pour certains découverts le monde de l'informatique industrielle avec Stuxnet) s'intèressent désormais beaucoup au SCADA. La courbe ci-dessous montre l'évolution du nombre de vulnérabilités SCADA publiées chaque mois (données extraites du bulletin "Securité Scada" publiées chaque mois par le Cert-IST) : en 2011 plus de 70 vulnérabilités ont été annoncées, soit 5 fois plus que pour l'année précédente.



La grande majorité des vulnérabilités découvertes en 2011 sont des vulnérabilités « faciles » à découvrir. En effet, la plupart des systèmes industriels aujourd'hui en fonction ont été conçus sans se préoccuper réellement de la sécurité des systèmes informatiques utilisés (au sens de la résistance aux attaques volontaires) et incluent en conséquence de nombreuses failles classiques (mots de passe par défaut, programmation non défensive, débordements mémoire, etc…). Avec la panoplie des outils de test de vulnérabilités disponibles dans le monde de l'informatique général, il est aujourd'hui plus facile pour un chercheur de failles de découvrir ces failles classiques et de faire « tomber » des outils SCADA déployés dans le monde industriel. Ces failles ne sont en général exploitables que par un attaquant se trouvant déjà à l'intérieur de l'installation industrielle.

En 2011, certains chercheurs ont ainsi publié des « packs de vulnérabilités » :

- En mars 2011, le chercheur italien Luigi Auriemma a publié un pack de 34 vulnérabilités touchant 4 produits SCADA (comptabilisées comme 4 vulnérabilités multiples dans l'histogramme ci-dessous). Il l'a complété depuis en ajoutant 15 nouvelles vulnérabilités en septembre (concernant cette fois 10 produits) puis 5 en octobre, etc.. On voit bien ici l'intérêt du chercheur pour le monde SCADA (19 produits SCADA testés) et le nombre important de vulnérabilités trouvées (54 vulnérabilités en 2011).
- En mars 2011, la société Gleg a publié un pack (baptisé « Agora SCADA+ exploit pack ») regroupant 18 vulnérabilités déjà connues et 5 nouvelles vulnérabilités (selon le décompte fait par l'ICS-CERT). Ce pack est mis à jour régulièrement et annonce regrouper toutes les vulnérabilités déjà publiées par ailleurs (y compris celles publiées par Luigi Auriemma).

On le voit, la recherche de failles dans le monde SCADA est un domaine en pleine ébullition. Les experts de la sécurité SCADA indiquent cependant que la grande majorité des failles publiées actuellement se contentent de reproduire dans le monde SCADA les vulnérabilités déjà connues dans l'informatique généraliste (les vulnérabilités Windows). Les « vraies » vulnérabilités SCADA sont donc encore largement inexplorées : il s'agit des vulnérabilités dans les équipements spécifiques au SCADA (les PLC).

3.4 Cyber-activisme : faut-il s'en inquiéter ?

2011 est aussi l'année où les **hacktivistes** (mot construit par contraction de « hacker » et « activiste », désignant les personnes qui utilisent des outils de hackers pour promouvoir des mouvements protestaires) ont pris une importance médiatique.

Le groupe « **Anonymous** » est le plus représentatif aujourd'hui de ce mouvement hacktiviste. Ce groupe est devenu visible pour le grand public en décembre 2010 lorsqu'il a pris la défense de Wikileak et invité tous ses sympatisants à participer à une attaque en déni de service pour bloquer les sites de Paypal, Visa et MasterCard. Le blocage effectif de MasterCard et Visa a alors démontré la puissance que pouvait avoir un mouvement collaboratif de ce type.

Aujourd'hui les mouvements de protestation similaires à ceux lancés par le groupe Anonymous, représentent une nouvelle menace pour les entreprises : quelques milliers de sympatisants, prêts à installer sur leur PC un outil d'attaque diffusé par le groupe hacktiviste, sont en effet capables de bloquer par leur action concertée la plupart des sites web institutionnels. En 2011, l'attaque informatique est devenue un outil de protestation (au même titre que d'autres actions comme la pétition ou le seating) à la portée de n'importe quel mouvement de protestation.

Face à cette situation, les entreprises doivent donc se préparer et considérer cette dernière comme un nouveau type de risques à prendre en compte. Elles doivent notamment définir les mesures techniques à déployer, préparer la mise en œuvre d'une cellule de crise et définir le type de communication qu'elles feraient en cas d'attaques. Les attaques des groupes hacktivistes ne sont généralement pas d'un haut niveau de technicité par rapport aux attaques ciblées qu'une entreprise pourrait subir.

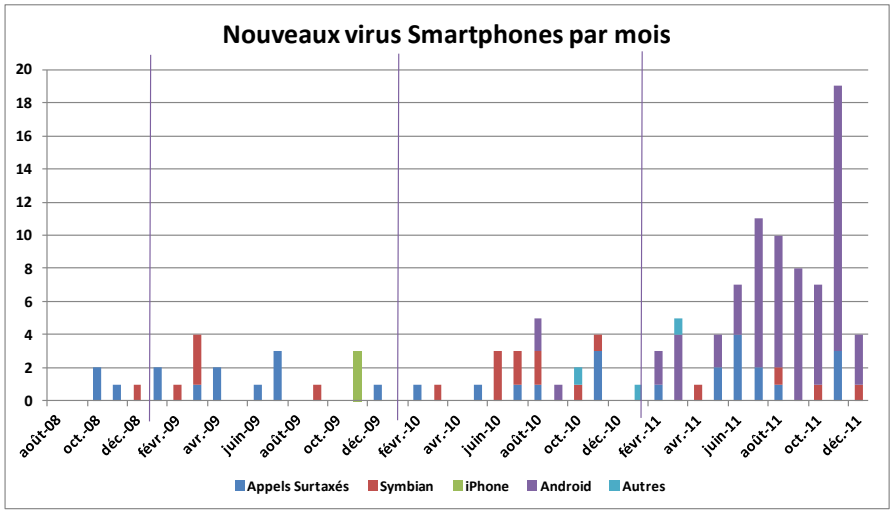
Il est difficile de savoir le sérieux qu'il faut apporter à ces groupes hacktivistes. Entre amusement, recherche de notoriété, volonté de déstabilisation ou forme moderne de protestation, les motivations de ces groupes ne sont pas claires. Les groupes hackivistes qui ont le plus fait parler d'eux en 2011 sont Anonymous et Lulzsec. :

- Lulzsec (ce nom viendrait de "LoL Sec" ce qui peut être traduit par "La sécurité pour rire") est un groupe qui semble chercher avant tout la notoriété médiatique et qui attaque des sites mal protégés mais ayant un certain prestige.
- Anonymous est plus difficile à cerner car le mouvement est multi-forme (de nombreux groupes indépendants se revendiquent comme étant des « anonymous »). Il n'y a pas vraiment de cohésion du groupe autour d'une revendication ou d'un objectif et le groupe semble plutôt chercher les causes qu'il pourrait défendre.

Ces groupes (nous considérons dans ce rapport uniquement ceux qui mettent en avant leurs compétences pour les attaques informatiques) s'inscrivent dans un contexte social de protestation plus large : mouvement des indignés en Espagne, Occupy Wall Street, etc…

3.5 Smartphone

Au cours de 2011, nous avons observé une augmentation importante du nombre d'applications malveillantes visant les smartphones, et plus particuliérement Android (cf. l'histogramme ci-dessous). La première raison de cette augmentation est sans doute le fait qu'Android est un système ouvert et facilement abordable. Par exemple, il est assez facile de construire une application malveillante en clonant une application légitime et de lui ajouter une fonction malveillante invisible.



L'explosion du nombre de malwares visant les téléphones mobiles pose la question de la nécessité d'équiper les téléphones mobiles de logiciels antivirus. Les experts semblent plutôt sceptiques sur la qualité des antivirus aujourd'hui disponibles pour ces plates-formes et des tests récents ont même jugé les logiciels antivirus gratuits actuels totalement innefficaces (cf. cet article).

La plupart du temps, ces applications malveillantes sont mises à disposition sur Internet dans des espaces autres que le site officiel d'Android (l'Android Market) et il y a peu de risques qu'un utilisateur lambda aille les télécharger (car ce sont plutôt les utilisateurs aguerris qui utilisent un « Market » non officiel). Il arrive aussi que des applications malveillantes soient publiées sur le « Market » officiel (voir par exemple ce cas à propos du malware DroidDream) mais dans ce cas ces applications sont otées du « Market » (et des terminaux sur lesquels elles ont été installés) dès qu'elles sont identifiées comme malveillantes (suite à des plaintes d'utilisateurs). Bien sûr il s'agit d'un système réactif qui a clairement des limites (voir par exemple cet article qui montre comment une application malveillante peut réapparaitre très rapidement après avoir été suspendue par Google).
Nota : Ce principe d'un espace contrôlé (le « Market »), où sont mises à dispositions les applications, est appelé un « walled garden » (le jardin clos). Il introduit un nouveau modèle de sécurité (où l'espace de distribution des applications est contrôlé par le concepteur du téléphone : Android Market, iPhone Apps Store, Blackberry App World, Phone7 MarketPlace).

Au dela de la multiplication de ces applications malveillantes, l'attaque la plus classique (la plus répandue) dans le monde du mobile reste les appels vers des numéros surtaxés. Il peut s'agir d'un simple SMS incitant le destinataire à rappeler un numéro surtaxé, ou d'une application maveillante qui génére automatiquement l'envoie d'un SMS vers un numéro surtaxé.

Les malwares les plus inquiétants (les plus spectaculaires) dans le monde des smartphone restent en 2011 ceux des familles ZitMO (Zeus in the mobile) et SpitMO (SpyEye in the mobile). Découverts pour la première fois en septembre 2010, ces malwares s'installent sur tout type de smartphones (des versions existent pour Windows Mobile, Symbian, Blackberry et Android) et ont pour objectif principal d'intercepter les SMS envoyés par les banques lors d'un virement (voir par exemple cet article de

Kaspersky et celui-ci de McAfee). En effet, lorsqu'un virement par Internet est demandé, certaines banques envoient sur le téléphone mobile du propriétaire du compte bancaire un code que ce dernier doit fournir dans le formulaire de demande de virement. Cela permet d'éviter que quelqu'un d'autre que le propriétaire du compte bancaire réalise un virement par Internet.

4) Conclusions

➢ Les attaques par infiltration deviennent une menace majeure

L'année 2011 marque une étape significative dans l'évolution de la menace pour les entreprises.
Si l'on regarde rétrospectivement les catégories d'attaques que l'on a vues depuis les années 2000 on peut schématiquement identifier 3 vagues successives :

- Les attaques virales qui saturent les infrastructures (tels les vers vus au début des années 2000).
- Les attaques contre les équipements d'infrastructure (par exemple attaque DOS) ou les sites institutionnels (défacement de serveurs web),
- Les attaques visant les postes de travail, avec comme objectif premier la constitution de botnets.

Ces menaces avaient pour objectif premier d'attaquer des équipements informatiques (pour les mettre hors service, pour en prendre le contrôle, ou pour en voler le contenu). Par opposition, en 2011 un grand nombre d'attaques par infiltration ont été découvertes. Pour ces attaques, que l'on appelle souvent des « APT » (Advanced Persistent Threat) la prise de contrôle des équipements informatiques n'est plus une fin en soin, il est le moyen pour pénétrer au sein de l'entreprise de façon à atteindre ensuite un objectif précis (vol de document confidentiel, cyber-espionnage, voire sabotage).

Contrairement aux menaces précédentes, les attaques par infiltration n'ont pas pour objectif d'attaquer le Système d'Information de l'entreprise (ce n'est pas leur but) ; elles ont comme but d'attaquer le patrimoine de l'entreprise (ses secrets ou ses organes vitaux).

Les attaques en 2011 contre le ministère de l'Economie et des Finances (Bercy), la société RSA ou d'Areva sont des exemples de ces attaques ciblées.

Bien sûr le risque d'une intrusion au sein du système informatique existe depuis toujours, et les attaques ciblées, à caractère d'espionnage industriel, ne datent pas de 2011. On peut par exemple citer en 2004 l'affaire Titan rain à propos d'attaques supposées chinoises contre des sites militaires américains, ou l'affaire Michaël Haephrati qui a mis en évidence l'utilisation de chevaux de Troie pour l'espionnage industriel. Mais **le grand nombre d'attaques ciblées survenues en 2011 montre que ce phénomène a changé d'échelle : il est passé d'un phénomène marginal (un risque théorique) à un phénomène majeur que l'on doit impérativement prendre en compte.**

Comme l'a indiqué M. Pailloux (Directeur de l'ANSSI) lors de notre journée Forum 2011, la question n'est plus aujourd'hui de savoir si une entreprise sera touchée ou non par une attaque de cyber-espionnage (du type de celle qui a touché Bercy début 2011), elle est de savoir quand cette attaque arrivera et combien de temps il faudra à l'entreprise pour la détecter et la contrer.

La Chine et la Russie sont souvent pointées comme étant à l'origine de ce type d'attaque (cf. le rapport publié par le gouvernement américain) mais il serait illusoire de penser que ces deux pays sont les seuls à agir sur ce terrain. Les cyber-attaques sont aujourd'hui une composante à part entière de l'arsenal de l'espionnage, que celui-ci vise les entreprises ou les gouvernements.

➢ Ces attaques marquent le début d'un nouveau cycle de renforcement de la sécurité

Depuis la disparition des attaques virales massives (du type CodeRed et Nimda en 2001, Slammer en 2003, Sasser en 2004), les entreprises n'ont plus subi d'attaques perturbant de façon importante de leurs systèmes informatiques. Comme nous le disions dans notre bilan annuel 2006 la vie des RSSI pouvait alors semblait plus tranquille. Nous montrions aussi que ce n'était pas vraiment le cas parce que la menace était en fait devenue plus pernicieuse. Conficker (fin 2008) a montré d'ailleurs que le risque d'attaque massive ne pourrait jamais être définitivement écarté.

Mais globalement, après 2004, les gens qui n'étaient pas impliqués directement dans la sécurité ont pu considérer que la menace d'attaque avait diminuée et que l'on était dans un cycle de relâchement progressif des contraintes sécurités.

Pendant ce temps la menace a continué à évoluer :

- Apparition des "fuzzers" pour rechercher de façon systématique les failles,
- Débouchant sur le phénomène des 0-days, et l'industrialisation du marché des failles,
- Provoquant l'arrivée des cyber-criminels avec des attaques visant principalement le grand public (phishing, vol de données bancaires et escroqueries).

Globalement, de 2004 à 2010 les techniques d'attaques se sont considérablement améliorées, et ces techniques se tournent maintenant vers l'entreprise en prenant en particulier plusieurs formes :

- Les attaques par infiltration,
- Les attaques SCADA.

Parallèlement à cette évolution de la menace, les contraintes économiques, ou la recherche d'une efficacité maximum, ont pu pousser vers une sécurité "low cost" qui est aujourd'hui incompatible avec cette nouvelle menace.

L'entreprise se trouve face à un risque nouveau (ou un risque dont le niveau doit être réévalué à la hausse) et doit adapter ses défenses à ce nouveau contexte. Il est très probable que cela marque le début d'un cycle de renforcement de la sécurité.

➢ Il faut y répondre en renforçant les défenses

Pour répondre à la menace croissante l'entreprise doit agir sur 3 axes :

- **Renforcer ses défenses**. Le maintien à jour des équipements (et en particulier des postes de travail des utilisateurs, qui sont aujourd'hui les cibles privilégiées en cas d'attaque par infiltration) est une composante essentielle de défense, car les nouvelles vulnérabilités qui sont découvertes chaque jour créent de nouvelles faiblesses qui en s'accumulant dégradent notablement le niveau de résistance en cas d'attaque. Aujourd'hui, la plupart des attaques exploitent des vulnérabilités anciennes, pour lesquelles des correctifs sont déjà disponibles auprès des constructeurs. L'objectif ici n'est pas d'appliquer 100% des correctifs de sécurité sur l'ensemble du parc dans un délai donné. Il est plutôt de mettre en place un processus maitrisé permettant d'atteindre un "niveau de patch" adapté au besoin de sécurité de chaque sous système de l'entreprise (serveurs frontaux en DMZ, serveurs internes, postes de travail, etc…). La veille sur les vulnérabilités, l'évaluation du niveau de risque de chacun et la capacité à déployer les correctifs de sécurité au sein de l'entreprise, sont donc des éléments clés de la maîtrise de la sécurité.

- **Développer sa capacité de détection et de traitement des intrusions**. Si les IDS, IPS sont des éléments utiles pour assurer la sécurité (ce sont des outils sentinelles, qui permettent de mesurer le niveau de la menace et de stopper les attaques les plus directes), ils ne suffisent

pas pour empêcher toutes les attaques. Une approche complémentaire consiste à rechercher les attaques réussies, avec comme objectif de les stopper le plus tôt possible et d'empêcher qu'elles s'implantent de façon durable au sein de l'entreprise. Cela implique la mise ne place de moyens de détection des anomalies de sécurité (en analysant les logs de sécurité et en apprenant aux utilisateurs à signaler les incidents) et la mise en place d'une équipe de traitement des incidents qui intervient dès qu'un cas suspect est identifié.

- **Ré-évaluer le niveau de sécurité de son infrastructure vis à vis des attaques internes**. De façon complémentaire au point précédent, il est nécessaire d'améliorer les moyens de défense et de détection (souvent tournés vers les attaques externes) à l'intérieur de l'entreprise. Pour cela il faut re-évaluer la résistance du système d'information aux attaques internes, en partant de l'hypothèse que le poste utilisateur sera un jour compromis par un attaquant motivé (qui souvent contournera les protections mises en place en s'appuyant sur la collaboration involontaire des utilisateurs légitimes), et en analysant alors les défenses qui empêcheront la progression de l'attaquant à l'intérieur de l'entreprise. Cette analyse doit permettre d'identifier les faiblesses internes et d'adopter des mesures de sécurité pour les réduire.

➢ L'année 2011 montre aussi que les attaques Cyber-activistes doivent être prises en compte

L'hacktivisme (i.e. le fait que des activistes utilisent des outils de hackers pour leurs actions de protestation) est une menace qui a pris de l'importance en 2011. Les attaques de groupe comme les « Anonymous » (contre PayPal, Sony ou Monsanto) et « Lulzsec » (contre la CIA ou la télévision américaine PBS) ont mis en évidence que des entreprises pouvaient être l'objet d'attaques ciblées par ces mouvements protestataires. Jusqu'à présent, les attaques lancées par ces groupes ont été de deux formes : la divulgation d'informations volées sur des serveurs (documents internes, listes de collaborateurs, etc…) et le déni de service (attaque des sites web par saturation).

Ces cyber-protestations sont une forme modernisée des actions de protestations classiques : appel au boycot, seating, actions médiatisées, etc… D'un point de vue technique, ces attaques sont généralement peu sophistiquées : elles tirent partie de défauts de sécurité classiques (par exemple des vulnérabilités de type "SQL-injection") qui pourraient facilement être détectés par un test d'intrusion, ou utilisent des techniques de saturation d'une ampleur bien plus faible que ce que pourrait déployer un attaquant professionnel. Et **si elles causent aujourd'hui des dégâts c'est, il nous semble, tout d'abord parce que les organisations qu'elles visent ne s'y sont pas préparée**s.

Face à cette menace, les entreprises doivent se préparer et considérer l'hacktivisme comme un nouveau type de risques à prendre en compte. Elles doivent notamment définir les mesures techniques à déployer, préparer la mise en œuvre d'une cellule de crise, et définir le type de communication qu'elles feraient en cas d'attaque.

➢ La sécurité SCADA et la sécurité des Smartphones

Ces deux sujets représentent des menaces latentes et ont occupé une part significative de l'actualité de 2011.

Pour les Smartphones, la menace pour l'entreprise en est encore à ses débuts. Le nombre d'applications malveillantes est certes en augmentation significative (tout particulièrement sur les

téléphones Android), et les possibilités d'attaques au moyen de ce nouveau vecteur se confirment (voir par exemple les malwares bancaires ZitMO et SpitMO). Mais la grande majorité des attaques aujourd'hui restent des escroqueries classiques qui consistent à convaincre les utilisateurs d'installer une application malveillante sur leurs terminaux pour ensuite générer des appels vers des numéros surtaxés. L'efficacité des outils de protection (tels que l'antivirus) pour les smartphones est aujourd'hui un sujet de débats entre experts. Par contre, comme nous l'expliquions dans notre bilan 2010, **l'usage de plus en plus répandu du smartphone induit clairement de nouveaux risques pour l'entreprise**. **Il est donc indispensable que les entreprises analysent ces nouveaux risques et intègrent à leur procédures de gestion de flotte d'équipements mobiles des règles de sécurité** (et par exemple prévoir des procédures d'effacement des données à distance) pour protéger l'entreprise contre les fuites de données via ce vecteur.

De même **dans le monde l'informatique industrielle (le SCADA), on a assisté en 2011 à une explosion du nombre de vulnérabilités découvertes dans les équipements** par des chercheurs de failles. Ce phénomène illustre bien le fait que la plupart de ces équipements n'ont pas un niveau de sécurité suffisant pour se défendre contre des attaques informatiques volontaires. Ces équipements sont heureusement souvent protégés dans des réseaux dédiés, mais le phénomène des attaques par infiltration montre qu'un attaquant motivé peut-être capable de s'infiltrer profondément dans les réseaux d'entreprises jusqu'à atteindre ces cibles. **Il s'agit d'une menace majeure qui nécessite que les travaux de sécurisation déjà en cours sur ces infrastructures soient poursuivis sans relâche**.

Fin du document