1) Introduction

Comme chaque année, le Cert-IST fait 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 tout d'abord les événements les plus marquants de 2014 (cf. chapitre 2) et la nécessité de ré-évaluer les risques face à des attaques cyber plus fréquentes et plus perfectionnées, ou le phénomène des attaques cryptographiques.

Nous passons ensuite en revue les principales failles et attaques de 2014 (cf. chapitre 3) en faisant un récapitulatif issu du suivi quotidien par le Cert-IST des vulnérabilités et des menaces. Cela inclut un bilan général de la production du Cert-IST (nombre d'Avis, de Danger Potentiels et d'Alertes), puis un examen des principales menaces ayant donné lieu à des Alertes (ou des Dangers Potentiels) Cert-IST.

La conclusion (cf. chapitre 4) effectue une synthèse du paysage actuel de la cyber-menace et des challenges auxquels l'entreprise doit faire face.

Nota : Les encadrés bleus insérés tout au long du bilan correspondent à des articles ou des annonces qui ont été publiés au cours de l'année dans le bulletin mensuel du Cert-IST.

➢ 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 événements les plus marquants de 2014

L'année 2014 a été riche en événements. Tout d'abord, les entreprises ont dû faire face au quotidien à des attaques liées à la découverte de nouvelles vulnérabilités. Certaines attaques ont généré des situations de crises plus ou moins marquées :

- les attaques Shellshock et HeartBleed contre les serveurs.
- les attaques visant le poste de travail au moyen de nouvelles vulnérabilités dans Internet Explorer, Flash ou etc.
- ou même les vagues d'infections par mail avec des malwares comme CryptoLocker.

Mais au-delà de ces menaces au quotidien (que nous développons au chapitre 3) des phénomènes plus globaux se dégagent de l'actualité. Nous les passons en revue ci-dessous.

2.1 Des attaques plus sophistiquées qui changent la nature du risque

Il y a eu en 2014, un grand nombre de rapports décrivant des attaques "sophistiquées". Par exemple :

- L'attaque « Havex » (dans le cadre d'opérations de cyber-espionnage nommée « Energetic Bear » ou « Dragonfly ») tente de compromettre des systèmes industriels en infectant des programmes d'installation légitimes sur les sites web des constructeurs de ces logiciels SCADA.
- L'attaque « Zombie Zero » parvient à compromettre une société de logistique et transport, en livrant à la société visée des douchettes lecteurs de code-barres infectées spécifiquement.
- La chaine de distribution américaine Target subit (fin 2013) une intrusion sévère dans son système d'information qui résulte en l'installation de logiciels espions sur les terminaux de paiement de la chaine de magasins et le vol des données de cartes de paiement de millions de clients.
- La société Sony Pictures Entertainment subit (fin 2014) une intrusion d'ampleur qui résulte en la divulgation de données internes, le report de la sortie du film « The Interview » et une escalade diplomatique entre les USA et la Corée du Nord.
- …

Pour un spécialiste, aucune de ces attaques n'est réellement sophistiquée. Les techniques utilisées sont relativement simples et les failles exploitées connues depuis longtemps (il n'y a même parfois pas de faille mais simplement des faiblesses chroniques comme par exemple des infrastructures mal cloisonnées, des utilisateurs piégés par des techniques d'ingénierie sociale, etc…). Par contre ces attaques étaient jusqu'à présent très ponctuelles, et aucun rapport n'était publié à leur propos. La multiplication des cas d'incidents publiés montrent que ces temps ont changé : désormais ce type d'attaques est beaucoup plus commun. Il semble même que la situation crée des émules :

- Avant 2010, seuls certains états (et certaines sociétés privées spécialisées ?) procédaient probablement à ce type d'attaques informatiques
- En 2010, le phénomène des APT est devenu public (avec les révélations de Google sur l'attaque "Aurora"), et tous les états ont dû se poser la question de se doter également de cette capacité.
- Aujourd'hui, le cas Target (et sans doute aussi Sony) montre que les cybercriminels aussi, ont adopté les techniques de cyber-espionnage pour prendre le contrôle des systèmes d'information de leurs victimes.

Incident majeur dans la chaine de magasins Target
(extrait du bulletin Cert-IST de janvier 2014)

Mi-décembre 2013, il a été découvert que la chaine de magasins Target avait été victime d'un incident majeur qui aurait permis à des attaquants de voler les données de 40 millions de cartes bancaires. De nombreux articles ont été publiés depuis cette date sur cet incident, au fur et à mesure de la progression de l'enquête. En résumé, les attaquants seraient entrés dans le système informatique de l'entreprise en utilisant un compte de télé-maintenance pour le système de climatisation, et auraient infecté les caisses enregistreuses de la chaine de magasins. Il s'agit d'une opération sophistiquée qui montre que les attaques par infiltration ne sont pas réservées au domaine du cyber-espionnage stratégique. Il met aussi en évidence que les malwares visant les caisses enregistreuses sont devenus fréquents en 2013. Cet article de Brian Krebs (parmi beaucoup d'autres) donne plus d'informations sur cet incident.

Target montre les limites de la sécurité traditionnelle
(Une du bulletin Cert-IST de Mars 2014)

La cyber-attaque subie par la chaîne de magasins « Target » fin 2013 (cf. la rubrique « Attaques du mois » de notre bulletin de janvier 2014) servira sans doute désormais de « cas d'école » pour améliorer la sécurité. Elle démontre, si cela était encore nécessaire, que :

- Une certification de sécurité (PCI-DSS dans ce cas) ne suffit pas pour empêcher un incident majeur. Deux banques ont déposé plainte en mars contre la société qui avait effectué la certification PCI-DSS de Target, mais ont finalement annulé cette action.
- Les outils techniques de détection (Symantec et FireEye dans ce cas) ne suffisent pas s'ils ne sont pas correctement configurés et exploités (ou s'ils ne sont pas exploitables). Lors de son audition auprès du Sénat américain en mars, Target a indiqué sur ce point que les alertes générées avaient été noyées dans le flot des centaines d'alertes générées chaque jour.

Le rapport préparé pour le Sénat donne une analyse intéressante de la cyber-attaque subie par Target, et pointe les insuffisances des systèmes de sécurité en place. Cet incident majeur montre avant tout que la supervision de sécurité est désormais un élément clé de la maîtrise de la sécurité.

Du fait de cette évolution, il est nécessaire de reconsidérer le risque de "cyber-intrusion" : il faut considérer désormais que toutes les attaques théoriquement possibles ne sont pas que théoriques. Voici quelques exemples des risques théoriques que l'on ne peut plus ignorer :

- Ecoute sur une liaison réseau qui sort du périmètre de l'entreprise sans être chiffrée,
- Attaque MiTM (Man In the Middle) sur un flux applicatif,
- Propagation interne d'une intrusion sur un réseau interne non segmenté ou sans politique stricte de limitation des comptes à privilèges,
- Attaque d'utilisateurs mobiles via des faux points d'accès Wifi,
- Attaque utilisant des vulnérabilités déjà identifiées lors de tests d'intrusion, mais qui n'ont pas été corrigées.
- …

De façon un peu provocante, on peut dire également que si 100% des audits intrusifs qu'une entreprise a réalisés se sont conclus par une intrusion, alors il y a 100% de "chance" qu'un attaquant réel puisse réussir une intrusion s'il s'intéresse à un système qui n'a pas été audité ou qui a été audité mais non corrigé..

Dans notre bilan 2011 sur les failles et attaques, nous disions que la vague d'attaques APT vue cette année-là, montrait un risque nouveau (ou un risque dont le niveau devait être réévalué à la hausse) et qu'elle correspondait très probablement au début d'un cycle de renforcement de la sécurité. L'actualité 2014 confirme clairement ce phénomène : **Il est nécessaire de renforcer la sécurité des entreprises ou au moins de ré-évaluer son niveau de sécurité face à la menace actuelle.**

2.2 Beaucoup d'attaques visant la cryptographie

L'année 2014 a été marquée par une série d'événements relatifs à la cryptographie :

- Nombreuses failles découvertes dans SSL et TLS,
- Arrêt du logiciel de chiffrement Truecrypt,
- Attaques visant à briser l'anonymat TOR.

La cryptographie est aujourd'hui un élément essentiel pour la sécurisation des Systèmes d'Informations, et ces événements montrent que cette brique centrale est très activement attaquée. 2014 est la première année où cette tendance est clairement visible.

- **Nombreuses failles découvertes dans SSL et TLS**

Au cours de l'année, une série de vulnérabilités graves ont été découvertes dans les protocoles SSL et TLS (TLS est le successeur du protocole SSLv3 ;la version la plus récente est TLSv1.2). Nous les résumons dans le tableau ci-dessous.

Vulnérabilité Date	**Constructeur** Commentaire
GotoFail Mars 2014	**Apple** Permet de contourner la vérification de la validité du certificat numérique.
CVE-2014-0092 (aka « Bool is not Int ») Mars 2014	**Unix-Linux/GnuTLS** Permet de contourner la vérification de la validité du certificat numérique.
HeartBleed Avril 2014	**Unix-Linux/OpenSSL** Lecture à distance de portions de mémoire sur la machine vulnérable.
Poodle Octobre 2014	**Indépendant constructeur** (faille protocolaire) Une faiblesse dans SSLv3 permet à un attaquant MiTM de déchiffrer les flux.
Schannel Novembre 2014	**Microsoft** Exécution de code à distance.

On peut voir ici que tous les constructeurs sont affectés (Apple, Linux, Microsoft).

Il n'est pas rare que des failles SSL soient découvertes (chaque année le Cert-IST publie une dizaine d'avis de sécurité sur ces sujets), mais les failles listées ici sont plus graves que d'ordinaire. Il n'y a pas vraiment d'explication au fait qu'autant de failles graves aient été découvertes. Par exemple, il n'existe pas à notre connaissance de nouvelle technique de recherche de faille (« fuzzer »). Nous pensons donc que ces découvertes sont dues au fait que les chercheurs en sécurité sont de plus en plus pointus dans leur domaine : lorsqu'ils remarquent un comportement anormal, ils l'analysent en profondeur l'anomalie jusqu'à trouver certaines fois des vulnérabilités graves. On peut remarquer aussi que les chercheurs sont également très compétents en ce qui concerne l'exploitation des vulnérabilités découvertes. Par exemple dans le cas de HeartBleed, il n'était pas du tout évident au moment de son annonce que la faille pourrait être mise en pratique avec autant de "succès" : car entre une faille qui permet une fuite mémoire, et le vol de la clé privée d'un serveur il y a bien des difficultés (d'implémentation) à résoudre. Cloudflare avait lancé sur ce sujet un challenge … qui a été gagné en moins de 24h ! (voir cette explication sur le blog de Cloudflare).

La faille HeartBleed
Une du bulletin d'avril

La faille HeartBleed dans OpenSSL (cf. **CERT-IST/DG-2014.004**) est la faille la plus grave vue pour l'instant cette année. Outre sa dangerosité intrinsèque (elle permet de voler à distance des données sur les serveurs vulnérables, par exemple des mots de passe ou des certificats), elle impacte un composant de sécurité largement déployé (sur les serveurs web, mais aussi sur tous les autres logiciels embarquant la librairie OpenSSL). Elle a donc déclenché dans toutes les organisations, de larges campagnes de recensement et de mise à jour des parcs informatiques. Nous décrivons plus en détail au chapitre Attaques du mois la chronologie de cet événement et son traitement par le Cert-IST.

Menace HeartBleed dans OpenSSL
Extrait de la rubrique « Attaques du mois » du bulletin d'avril

Il s'agit d'une vulnérabilité critique dans la fonction de « heartbeat » de la librairie OpenSSL. Elle permet à un attaquant distant de lire des portions de la RAM d'un serveur OpenSSL vulnérable. Elle peut être utilisée par exemple pour lire des portions mémoire d'un serveur HTTPS vulnérable. Ces portions de mémoire contiennent potentiellement des données sensibles : mots de passe, cookies, données applicatives sensibles, etc. Il a été démontré par exemple (via le challenge lancé par CloudFlare) qu'il était possible de récupérer par ce moyen, la clé privée d'un serveur web HTTPS.
Cette vulnérabilité a été rendue publique le 7 avril, avec la publication par OpenSSL du correctif qui résout le problème. Elle avait été découverte le 21 mars 2014 par des chercheurs de Google et conservée secrète jusqu'au 7 avril (voir cet article pour plus de détails sur cette chronologie).
Le Cert-IST a publié le 08/04/2014 l'avis **CERT-IST/AV-2014.0266**, puis Le Danger Potentiel **CERT-IST/DG-2014.004** le 09/04/2014. A cette date, le Danger potentiel avait un risque « Moyen » car si la dangerosité théorique de la vulnérabilité était indéniable, l'efficacité effective lors d'attaques réelles semblait encore plus discutable. En parallèle, nous avons ouvert la menace [Heartbleed] dans le Hub de Crise Cert-IST afin de tenir au courant les abonnés à ce service de l'évolution de cette menace.
Le 15/04/2014 nous avons ré-émis le Danger Potentiel avec un niveau de risque à « Elevé » car les outils mis à disposition sur Internet pour cette vulnérabilité (et en particulier la démonstration du vol de la clé privée d'un serveur web HTTPS) rendaient désormais possible une exploitation massive sur Internet.
En termes de dangerosité, cette vulnérabilité HeartBleed est très grave car elle donne accès à distance (en lecture) à la mémoire des serveurs web vulnérables. Plusieurs cas d'attaques ont été rapportés. Par exemple :

- L'agence gouvernementale canadienne du revenu (Canada Revenue Agency) a suspendu son site web le 14/05/2014 suite à des tentatives d'attaque ayant abouti au vol de données personnelles de contribuables (voir cet article).
- Le 18/04/2014 la société Mandiant a indiqué avoir détecté des attaques HeartBleed ayant abouti au vol de jetons de sessions VPN (voir cet article de DarkReading.com). Plus inquiétant encore, ces attaques se seraient produites dès le 08/04/2014, c'est-à-dire le lendemain de l'annonce initiale de la vulnérabilité par OpenSSL.

- **Arrêt du logiciel de chiffrement Truecrypt**

2014 est aussi l'année où l'équipe qui développait le logiciel de chiffrement open-source "TrueCrypt" a soudainement annoncé (fin mai) qu'elle stoppait le projet. Aucune explication claire n'a été donnée pour cet arrêt. On peut penser qu'il est dû à des pressions secrètes de la NSA sur l'équipe de développement ; la seule échappatoire pour s'en soustraire étant alors pour eux de stopper brutalement le projet.

- **Attaques visant à briser l'anonymat de TOR**

On a vu aussi en 2014 plusieurs attaques visant le réseau TOR :

- Attaque de chercheurs insérant des **faux nœuds TOR** (voir cet article de Freedom-To-Tinker.com)
- **Opération Onymous** (par des forces de police) ayant conduit à la neutralisation de serveurs illégaux (voir cet article du blog officiel du projet Tor ou cet article 01Net.com)
- Etude de chercheurs utilisant **Netflow** pour établir une corrélation de trafic (voir cet article du blog officiel ou cet article ZDNet – ou cet article TheRegister.co.uk).

Il est clair que TOR abrite beaucoup de trafics illégaux et que briser l'anonymat qu'il apporte est une préoccupation majeure des entités légales de beaucoup de pays. Briser l'anonymat de TOR permet aussi aux pays totalitaires de garder sous surveillance sa population. Si la surveillance est exercée sans contrôle d'une entité de régulation, elle ouvre alors la porte à des risques de dérive..

2.3 Cyber-espionnage : les états à la pointe des attaques cybers

Depuis 2010 et la médiatisation progressive des attaques par infiltration (attaques appelée « APT » : Advanced Persistent Threat), les états – ou les agences privées commanditées par les états – apparaissent comme étant les plus avancés dans les techniques de cyber-intrusions et de cyber-espionnage.

Nous en avons déjà souvent parlé dans nos bilans annuels. Et 2014 ne fait que renforcer ce constat. A titre d'illustration, nous listons ci-dessous les affaires de cyber-espionnage qui ont été révélées en 2014. La plupart correspondent à des opérations démarrées depuis plusieurs années et qui n'ont été découvertes que récemment.

Date de publication	Noms de l'opération de cyber-espionnage	Pays supposé à l'origine
Février	Uroburos Autres noms : Epic Turla, Snake	Russie
Février	Careto/The Mask	Espagne
Mars	Siesta	Chine
Mars	Snowglobe Autre nom : Babar	France
Mai	Clandestine Fox	Chine
Juin	Energetic Bear Autres noms : Crouching Yeti, Dragonfly	Russie
Juin	Putter Panda	Chine
Juin	Pitty Tiger	Chine
Juillet	CosmicDuke	
Août	Machete	
Août	Poisoned Hurricane	
Octobre	SandWorm / BlackEnergy2	
Octobre	Axiom	
Novembre	DarkHotel	Corée du Sud
Novembre	Regin	USA

Dans les années 2000, lors de la généralisation du web, Internet est apparu comme une terre de liberté (ou même de non droit !) avec un esprit fort de partage et de démocratie (le « village global »). Les états ont semblé alors absents (dépassés ?) de ce territoire. En fait, il n'en est rien. Les états ont visiblement compris il y a plusieurs années la puissance que pouvait leur apporter l'Internet en termes de surveillance ou de cyber-espionnage, et ont développé silencieusement des capacités techniques

sur ce terrain. Aujourd'hui, ces pratiques deviennent visibles au grand jour, probablement parce qu'elles sont utilisées de plus en plus largement.

Il y a bien sûr une légitimité des états à pratiquer de la surveillance des activités terroristes, ou même une nécessité a être capable de pratiquer l'espionnage. Mais ces techniques cyber ont aussi tendance à se généraliser et à déborder la sphère étatique.

2.4 Des escroqueries florissantes

Dans le domaine des activités cyber-criminelles, nous avons en particulier relevé en 2014 les phénomènes suivants :

- Escroqueries de type « Faux Ordres de Virement » ou « Arnaques au président »
- Crypto-ransomware,
- Vague d'attaques des terminaux de paiement aux USA

Il n'y a pas ici de nouveauté technique. Par contre l'ampleur des attaques observées est étonnante.

Faux ordres de virement et arnaque au président : Nouveaux cas d'escroqueries d'ampleurs touchant des entreprises françaises
Extrait de la rubrique « Attaques du mois" »du bulletin de Janvier 2014

Deux nouveaux cas de l'attaque baptisée « Francophoned » par Symantec ont été révélés dans la presse en janvier :

- Une entreprise située de Pyrénées-Atlantiques s'est fait dérober 800 000 euros (voir cet article de Undernews),
- Une entreprise de la Manche s'est fait dérober 200 000 euros (voir cet article de Ouest-France).

Nous avions mentionné ce type d'attaques dans nos Unes des bulletins de mai et de septembre 2013. Elles consistent à :

- Infecter des postes internes d'une entreprise (par exemple le poste d'une assistante de direction) pour obtenir des informations sensibles,
- Envoyer par mail de fausses demandes de virements en se faisant passer pour un dirigeant de l'entreprise,
- Appeler au téléphone la personne visée pour la convaincre de réaliser ces virements.

Pour plus d'informations, reportez vous à cet article de Symantec ou à cette version francisée.

Les crypto-ransomware
Une du bulletin de juin 2014

Les virus qui chiffrent les données puis réclament une rançon existent depuis longtemps (voir par exemple PgpCoder en 2005), mais « CryptoLocker » a été, en octobre 2013, le premier virus « chiffrant » à se répandre à grande échelle (cf. notre Danger Potentiel **CERT-IST/DG-2013.012**). Depuis, plusieurs autres virus de ce type ont été identifiés : CryptorBit (décembre 2013), CryptoDefense (février 2014, également dénommé CryptoWall, très actif en juin avec une campagne de mails intitulés « Incoming fax report »), ou même Simplocker sur Android (juin 2014). Contrairement à un ransomware classique (où il suffit de ré-installer le poste), ces « crypto-ransomware » chiffrent les données utilisateurs, et s'il n'existe pas de sauvegarde, l'alternative est alors de payer ou d'abandonner les fichiers. Comme ce type d'arnaques semble assez lucratif, il n'y a

pas de raison que cela s'arrête. Il est donc recommandé de rappeler aux utilisateurs de faire régulièrement des sauvegardes de leurs fichiers importants.

Vague d'attaques contre les terminaux de paiements aux USA
Extrait de la section « Attaques du mois » du bulletin mensuel Cert-IST pour Août 2014

Au cours du mois d'août, il y a eu une forte médiatisation **d'incidents visant les terminaux de paiement aux USA**. Au cours de l'été, une série de chaines de magasins (et de restaurants) ont en effet annoncé avoir détecté des attaques visant leurs terminaux de paiement : UPS Stores, SuperValu, Home Depot, Goodwill Stores, Jimmy John sandwich restaurants. Ce type d'incident avait également été largement médiatisé en début d'année, avec l'attaque visant les magasins Target (voir notre rubrique Attaque du bulletin de janvier, puis la Une du bulletin de mars), puis les restaurants PF Chang (voir notre rubrique Attaque du bulletin de juin).

Ces attaques utilisent un malware spécialisé (un Ram scrapper) qui capture les informations relatives à la carte de paiement, au moment où elles sont présentes en RAM sur le terminal de paiement (qui fonctionne sous Windows). Le nombre des incidents « Ram Scrapper » a fortement augmenté en 2013, d'abord sans médiatisation, puis dans des attaques publiquement annoncées (l'attaque Target de la fin 2013 a été le premier cas vraiment médiatisé). L'US-CERT a publié en juillet et août plusieurs alertes à propos du « Ram Scrapper » nommé « Backoff » (en particulier une description de Backoff puis une alerte sur les attaques en cours). Le PCI council a également émis des recommandations sur ce sujet.
Nota : D'autres malwares de ce type existent, comme par exemple JackPOS, Decebel, Soraya ou BrutPOS : cet article de Net-Security.org, et l'étude Trend Micro qui y est citée, donnent plus de détails sur ce sujet.
Une solution à ces attaques multiples semble être de remplacer les cartes de paiement ordinaires en usage aux USA (cartes à pistes magnétiques) par des cartes à puces (système EMV en usage en Europe). EMV n'empêche pas les attaques par « RAM Scraper » (cf. cet article de l'IEEE-USA), car les informations volées par ces malwares sont uniquement des informations générales (par exemple : titulaire, No carte bleu, code CVV) et non le code confidentiel. Par contre elle rendra plus complexe ces escroqueries et la fabrication de fausses cartes.

3) Revue des failles et attaques de 2014

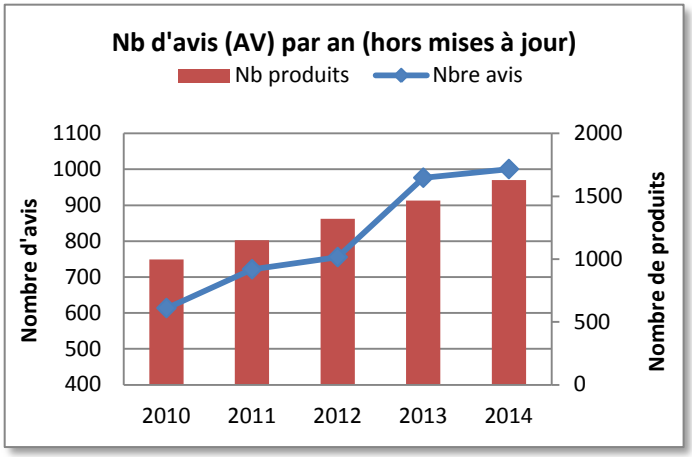
3.1 La production du Cert-IST en 2014

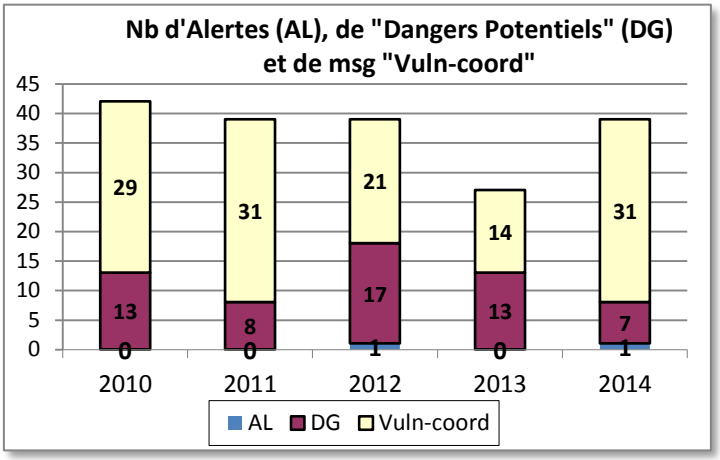
3.1.1 Veille sur les vulnérabilités et des menaces

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 privés entre CERT, 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 nécessitant un traitement prioritaire. L'émission d'une alerte est un événement rare : par exemple le Cert-IST a émis en 2014 une alerte sur la vulnérabilité Shellshock. 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 (quelque soit leurs probabilités d'être utilisées dans des attaques).

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





Ainsi, en 2014, le Cert-IST a publié :

- **1000 avis de sécurité**, suivis de façon continue au cours de l'année avec 2931 mises à jour mineures et 68 mises à jour majeures. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), et ce phénomène s'est fortement accentué en 2013 (+29% par rapport à 2012). Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène qui ne se tarit 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 forcément par une application régulière des

correctifs de sécurité sur ces produits. Au 31/12/2013 le Cert-IST suivait les vulnérabilités concernant 1 655 produits et 13 010 versions de produits.

- **1 Alerte, 7 Dangers Potentiels et 31 messages "Vuln-coord".** Nous donnons un aperçu de ces publications 2014 au chapitre 3.2 ci-dessous.

3.1.2 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.

3.2 Les Alertes et Dangers Potentiels émis par le Cert-IST

Le tableau ci-dessous liste les menaces les plus importantes pour l'année 2014 (par ordre décroissant), et les publications Cert-IST associées.

On trouve en tête les attaques massives qui ont visé les serveurs web : **Shellshock et HeartBleed**. Ensuite, nous avons regroupé dans une seule catégorie (ligne 3) toutes les attaques visant à infecter **le poste de travail de l'utilisateur** au moyen de documents (reçus par mail) ou de site web piégés. On pourra noter dans le reste de ce « top 10 » :

- en ligne 5 les **vulnérabilités Kerberos et Active Directory** affectant Windows : nous analysons ce phénomène au paragraphe 3.3.
- L'importance des **failles cryptographiques** dans l'actualité : HeartBleed (rang 2), Windows/SChannel (rang 6), Poodle (rang 8) et TrueCrypt (rang 10). Nous avons analysé ce phénomène au paragraphe 2.2

1	**ShellShock**	
		Alerte **CERT-IST/AL-2014.001 :** Risque d'attaque des serveurs web sur Unix/Linux via la vulnérabilité "Bash/Shellshock" **- 25/09/2014**
		Message **VulnCoord-2014.020 :** Vulnérabilité dans Bash sur Unix/Linux (ShellShock) **(25/09/2014)**
2	**HeartBleed**	
		Danger **CERT-IST/DG-2014.004** : Risque d'exploitation de la vulnérabilité " Heartbeat/Heartbleed " dans OpenSSL **- 09/04/2014**
3	**Attaques ciblées via des documents ou sites web piégés**	
	Internet Explorer	
		Danger **CERT-IST/DG-2014.001** Risque d'attaques via une vulnérabilité 0-day (CVE-2014-0322) dans Internet Explorer 9 et 10 **(14/02/2014)**
		Message **VulnCoord-2014.008** Nouvelle vulnérabilité dans Internet Explorer 8 (CVE-2014-1770 / ZDI-14-140) – **22/05/2014**
		Message **VulnCoord-2014.006** Exploitation de la vulnérabilité CVE-2014-1776 dans Internet Explorer – **28/04/2014**
	Flash	
		Danger **CERT-IST/DG-2014.002** Risque d'attaques via la vulnérabilité CVE-2014-0502 dans Adobe Flash – **21/02/2014**
	Word	
		Danger **CERT-IST/DG-2014.003** Risque d'attaques via une vulnérabilité 0-day (CVE-2014-1761) dans Microsoft Word – **25/03/2014**
	0-days : PowerPoint, IE et Windows(TTF)	
		Message **VulnCoord-2014.024** Point sur les 0-days Microsoft et la vulnérabilité Poodle de SSLv3 – **16/10/2014**
	PowerPoint	
		Message **VulnCoord-2014.026** Nouvelle vulnérabilité dans la gestion des objets OLE sur Microsoft Windows (3010060) – **23/10/2014**
4	**Web : CMS Drupal**	
		Danger **CERT-IST/DG-2014.005** Risque d'attaques automatisées contre les serveurs Drupal 7 (CVE-2014-3704) – **30/10/2014**
5	**Windows : Authentification Kerberos et Active Directory**	
	PyKEK	
		Danger **CERT-IST/DG-2014.007** Risque d'attaque pour la vulnérabilité Kerberos (CVE-2014-6324) sur les systèmes Windows (MS14-068) – **19/12/2014**
	Pass-the-Ticket	
		Message **VulnCoord-2014.015** Vulnérabilité dans le mécanisme d'authentification de Microsoft Active Directory – **16/07/2014**

6	**Windows : Schannel**	
		Danger **CERT-IST/DG-2014.006** Risque d'attaques via une vulnérabilité "Schannel" dans Microsoft Windows (MS14-066) – 18/11/2014 *Nota : Cette menace est décrite à la fin du § 3.3*
7	**Crypto-Ransomware**	
		Message **VulnCoord-2014.029** Campagne de diffusion du malware Cryptolocker – **04/12/2014**
8	**Poodle (faille SSLv3)**	
		Message **VulnCoord-2014.024** Point sur les 0-days Microsoft et la vulnérabilité Poodle de SSLv3 – **16/10/2014**
9	**Windows (Escalade de privilèges)**	
		Message **VulnCoord-2014.025** Programme d'exploit XP pour MS14-062 – **17/10/2014**
10	**Divers**	
	Arrêt de TrueCrypt	
		Message **VulnCoord-2014.010** Arrêt du logiciel TrueCrypt – **02/06/2014**
	Mouchard Computrace	
		Message **VulnCoord-2014.009** Fonction cachée "Computrace/Lojack" embarquée dans certains BIOS – **22/05/2014** *Nota : Cette menace est décrite à la fin du § 3.3*

3.3 Zoom sur quelques failles et attaques

- **Kerberos et ActiveDirectory**

Depuis 2012, on voit apparaitre des publications à propos de Microsoft sur:
- la compromission de l'Active Directory,
- les vulnérabilités dans les mécanismes d'authentification Kerberos.

Ces deux composants (Active Directory et Kerberos) sont fortement liés et sont les éléments centraux des mécanismes d'authentification de Windows :
- Kerberos est le mécanisme natif d'authentification dans les environnements Active Directory.
- Active Directory stocke toutes les clés de chiffrements utilisées pour implémenter l'authentification Kerberos (et en particulier la clé secrète des machines et du KDC).

Le sujet des compromissions est également logique puisque suite à la vague d'attaques par infiltrations apparue en 2010 (cf. le phénomène des APT déjà évoqué aux chapitres 2.1 et 2.3) l'analyse de la compromission des AD est devenue une question récurrente lors de l'analyse d'incidents.

Voici les éléments principaux que l'on peut retenir sur ce sujet :
- Le modèle de sécurité de Windows a clairement des limites : lorsqu'un compte de domaine est compromis, il est difficile ensuite d'empêcher la compromission progressive de toutes les ressources Windows du domaine (voir par exemple cette présentation de la conférence JSSI-2014 : Est-il possible de sécuriser un domaine Windows ?). Ce constat amène les entreprises à mettre en place des solutions de cloisonnement des comptes Windows, en particulier pour les comptes à privilèges.
- L'Active Directory est un composant complexe et la gestion des permissions peut facilement dériver vers une situation non maitrisable. L'audit de cet aspect est une tâche complexe mais elle permet d'identifier et de limiter les dérives.
- Si un AD a été compromis lors d'une attaque, il est impossible de le nettoyer correctement (changer la clé secrète du KDC est aujourd'hui impossible). Il faut donc reconstruire un nouvel AD.
- Kerberos est vulnérable et des failles sont progressivement découvertes dans ce composant.

Sur ce sujet de vulnérabilités Kerberos, on pourra en particulier noter en 2014 :

- La présentation lors de la conférence SSTIC-2014 sur le sujet : Secrets d'authentification épisode II : Kerberos contre-attaque (juin 2014)
- L'attaque Pass the ticket publiée en juillet 2014
- L'attaque PyKEK (MS14-068) publiée en décembre 2014

- **Menace nouvelle : Attaque des Air-gaps**

- Est-il possible de dialoguer secrètement avec une machine si cette machine n'est reliée à aucun réseau (on dit alors que la machine est isolée par un « air gap » - i.e. un « vide d'air ») ?
- Oui : avec des ultra-sons.

Fin 2013, un chercheur renommé (Dragos Ruiu) avait annoncé avoir découvert un malware nommé BadBIOS capable de dialoguer au moyen d'ultra-sons avec un autre ordinateur (voir cet article de ErrataSec d'octobre 2013). Cette affirmation a laissé de nombreux experts sceptiques (y compris le Cert-IST) : si le principe de cacher un signal dans un son est tout à fait possible, la mise en œuvre semblait beaucoup plus problématique. Par exemple, on pouvait douter que le haut-parleur et le micro d'un ordinateur classique étaient suffisamment performants pour le faire.
En 2014, la faisabilité technique a été clairement démontrée. Par exemple lors de la conférence SSTIC 2014, une démonstration a été faite avec une transmission sur une distance d'une douzaine de mètres entre un téléphone portable (diffusant un signal ultrason non audible) et un PC portable (recevant ce son sur son micro standard) : voir la vidéo "J'ai cru voir un grosminet" disponible à la section 7 de la session Rumps de la conférence SSTIC 2014.

- **2014 : année des vulnérabilités des logiciels open-source ?**

Une du bulletin de septembre 2014

Vulnérabilité **Heartbleed** dans OpenSSL, arrêt de **TrueCrypt**, vulnérabilité **Shellshock** : l'année 2014 semble être une année noire pour les logiciels open-source.
Vouloir extrapoler ces événements pour en tirer une tendance est probablement infondé (comme le dit Bruce Schneier). Par contre, ces événements montrent que (bien sûr) il y a des bugs dans les logiciels open-source et que ce n'est pas parce les codes sources sont disponibles que quelqu'un les a (forcement) déjà regardés (voir l'article de Robert Graham).
Globalement, on peut dire que le logiciel open-source :

- Paie la rançon de son succès: il est présent partout et certains composants open-source sont universellement utilisés.
- N'est pas moins buggé que le code « fermé » : mais il est plus malléable, adaptable et permet de construire ses propres solutions (plutôt que s'en remettre à celles d'un fournisseur).
- Dispose de moins de support et a une pérennité plus aléatoire qu'une solution commerciale. La gratuité du logiciel open-source demande donc en contrepartie, un investissement humain pour déployer et maintenir les solutions mises en place.

- **Fonction "Computrace/Lojack" cachée dans certains BIOS**

Extrait de la section « Attaques du mois » du bulletin mensuel Cert-IST pour Mai 2014

Kaspersky a identifié que certains BIOS d'ordinateurs PC incluent une fonction cachée qui installe, à l'insu de l'utilisateur, un logiciel antivol développé par la société Absolute.com et baptisé "Computrace". Ce logiciel est installé à chaque démarrage de l'ordinateur et il n'existe pas de moyen de supprimer cette fonction BIOS. De plus ce logiciel pourrait être manipulé par un tiers malveillant pour espionner le PC à distance.
Pour plus d'informations, reportez vous à notre message VulnCoord-2014.009**.**

- **Vulnérabilité "Schannel" dans Microsoft Windows - MS14-066**

Extrait de la section « Attaques du mois » du bulletin mensuel Cert-IST pour Novembre 2014

Le 18/11/2014, nous avons émis le Danger Potentiel **CERT-IST/DG-2014.006** (Risque d'attaques via une vulnérabilité "Schannel" dans Microsoft Windows - MS14-066). Il s'agit d'une vulnérabilité dans le composant « S-Channel » de Windows qui implémente les communications sécurisées SSL/TLS.
La vulnérabilité est grave car :

- Schannel est utilisé dans de nombreux services Windows comme IIS, OWA, RDP, Active Directory, etc...
- La vulnérabilité permet une exécution de code à distance et pourrait être utilisée sans authentification dans un certain nombre de cas.

De nombreux articles de presse ont d'ailleurs immédiatement annoncé que cette faille était au moins aussi grave que la vulnérabilité HeartBleed et que des attaques allaient se produire sous peu. Bien que la faille soit effectivement grave, ce type de réaction et d'emportement est excessif et semble plus guidé par le « sensationnalisme » que par une analyse rationnelle et posée de la situation (voir par exemple cet article qui annonçait des attaques dans moins d'une semaine).

Voici les dates clés de l'évolution de cette menace :

- 11/11/2014 : Microsoft annonce la vulnérabilité et publie un correctif dans le cadre de son bulletin MS14-066. Cette vulnérabilité donne lieu à l'avis CERT-IST/AV-2014.873.
- 14/11/2014 : Un programme d'exploitation privé (non disponible sur Internet) a été publié par la société Immunity. Il semble s'agir d'un prototype, disponible uniquement pour les clients de cette société.
- 18/11/2014 : Après avoir observé l'évolution de la menace, nous estimons que d'autres programmes d'attaques pourraient apparaitre et donner lieu à des attaques. Nous émettons le Danger Potentiel, en lui affectant le risque « Moyen ».

La situation n'a pas évoluée de façon significative depuis cette date et aucun cas d'attaque n'a été reporté. Plusieurs chercheurs ont publiés des analyses (comme par exemple ce post sur le blog securitysift.com). **Le danger reste bien réel et des outils d'attaques pourraient apparaitre sous peu**. Comme nous le recommandions dans notre Danger Potentiel, il est donc indispensable de vérifier que les correctifs pour cette vulnérabilité ont été appliqués. Les serveurs web IIS et RDP (Remote Desktop Protocol) semblent les cibles les plus probables pour ces attaques.

Nota : Microsoft a publié le 09/12/2014 une nouvelle version des correctifs pour les plates-formes Vista et Server 2008, car les correctifs initiaux induisaient des dysfonctionnements. L'avis CERT-IST/AV-2014.873 a été mis à jour en conséquence.

4) Conclusions

Les entreprises doivent composer avec une situation complexe.

D'une part :

- l'informatique a pris une place centrale dans la vie quotidienne, aussi bien sur le plan professionnel que sur le plan personnel,
- l'évolution des technologies pousse à disperser l'information (avec par exemple des phénomènes comme le Cloud et le BYOD) et cherche à rendre toujours plus facile l'accès à cette information.

D'autre part le risque d'intrusion a augmenté de façon importante au cours des 5 dernières années. De nouveaux attaquants, visant spécifiquement les entreprises (cyber-espionnage, cyber-sabotage) ont été identifiés.

2014 confirme cette montée du risque :

- Les attaques sont plus fréquentes,
- Le "cyber" est devenu un enjeu stratégique pour les états et on découvre que ces derniers sont très actifs sur les aspects offensifs et mettent en œuvre des attaques que l'on considérait jusqu'à présent comme peu probables.
- La recherche de vulnérabilités et les attaques se tournent désormais vers les solutions de cryptographie et cherchent à les mettre en défaut. Elles s'attaquent ainsi à un élément clé sur lequel sont bâties les solutions de sécurité.

Pour s'adapter à cette situation, l'entreprise a besoin tout d'abord d'être tenue au courant des menaces et de leurs évolutions. Le Cert-IST, au travers de son activité de veille technologique et de ses bilans, lui donne une vision argumentée de la menace.

Face à la montée du risque, chaque entreprise doit aussi :

- évaluer son exposition à ce type d'attaques,
- renforcer ses défenses,
- développer sa capacité de détection et de réaction aux intrusions.

Fin du document