Industrie Services Tertiaire

Bilan Cert-IST 2017 des failles et attaques

Publié en Mars 2018

Table des matières

1. Introduction

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

Nous présentons dans un premier temps une rétrospective de l'actualité de l'année 2017 (cf. chapitre 2), puis en tirons les principales tendances technologiques de l'année (cf. chapitre 3). Au-delà de ces faits d'actualité, il se dégage aussi des domaines où une vigilance accrue semble nécessaire dans les années à venir (cf. chapitre 4).

Nous fournissons ensuite un récapitulatif des différentes productions du Cert-IST au cours de cette année (cf. chapitre 5).

La conclusion (cf. chapitre 6) donne une synthèse du paysage actuel de la cyber-menace et des challenges auxquels les entreprises doivent faire face.

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

2. Cela s'est passé en 2017

Le tableau de la page suivante récapitule des événements marquants de 2017. **L'actualité majeures de l'année sont les infections WannaCry (mai 2017) et NotPetya (juin 2017)**. D'une part elles ont généré des crises majeures dans les entreprises qu'elles ont touchées. Et d'autre part elles contiennent de nombreux éléments techniques représentatifs de l'évolution actuelle de la menace :

- Elles marquent le **retour des vers** (infections de poste en poste),
- Les techniques utilisées (**ransomware, wiper, piégeage de logiciels légitimes**) sont tout à fait caractéristiques de 2017,
- Elles utilisent des **outils d'attaques volés à la NSA** (phénomène de « prolifération » que nous analysons au paragraphe 3.5),
- Elles ont été **attribuées officiellement** par les Etats Unis et leurs alliés à des états (**la Corée du Nord** pour WannaCry, **et la Russie** pour NotPetya), ce qui montre l'importance sans précédent qu'ont pris les attaques cyber sur l'échiquier géopolitique mondial.

Nous revenons sur plusieurs de ces aspects dans le chapitre 3 (sur les aspects techniques) ainsi que dans la conclusion (pour les aspects géopolitiques).

Janvier 2017	La société « St. Jude Medical » annonce la sortie d'un correctif de sécurité pour ses Pacemakers cardiaques, après la publication d'une alerte par la FDA (Food and Drug Administration) américaine. En août 2017 un programme de rappel est organisé pour que la mise à jour soit effectuée lors de la prochaine visite annuelle de contrôle : 800 000 patients sont affectés.
Janvier 2017	Le site sulfureux **LeakedSource** a été fermé par les autorités judiciaires. Il proposait de vendre les bases données de mots de passe qui avaient été publiées sur Internet. Nota : Le site Have I Been Pwned rend un service comparable, mais sans publier les mots de passe. Il est considéré comme un service utile et non frauduleux.
Mars 2017	Wikileaks publie **Vault7,** une série de documents volés à la CIA qui décrivent les outils d'espionnage (iPhone, Android, smart TVs) et les 0-days (Cisco par exemple) utilisés par l'agence américaine. Wikileak continuera ses publications sur Vault7 tout au long de l'année, et lancera en novembre 2017 une nouvelle série baptisée **Vault8**.
Mars 2017	Le groupe de hackers Turkish Crime Family a réclamé à Apple l'équivalent de 75 000 dollars en monnaie virtuelle pour ne pas supprimer des centaines de millions de comptes **iCloud**. Cette menace semble avoir pris fin avec l'arrestation fin mars par la police britannique d'un membre de la Turkish Crime Family.
Avril 2017	Kaspersky publie un rapport montrant que le **groupe Lazarus** (Corée du Nord) a effectué de nombreuses attaques visant les banques, les casinos ou les places de marchés de crypto-monnaies. Ce serait un moyen de financer l'économie de la Corée du Nord.
Mai 2017	Une première vulnérabilité dans **Intel ME et AMT** (un composant embarqué sur certaines cartes mères Intel) est découverte (CVE-2017-5689). Une seconde série sera ensuite révélée en novembre 2017 par Intel.
Mai 2017	Le 12/05/2017, le ransomware **Wannacry** utilise une vulnérabilité SMB dans Windows et infecte 200 000 ordinateurs dans le monde.
Mai 2017	L'équipe de campagne d'Emmanuel Macron explique qu'elle a utilisé des techniques de « cyber-deception » (envoi de fausses données à l'attaquant) pour contrer les attaques qu'elle a subies pendant la campagne électorale française.
Mai 2017	Le groupe **ShadowBrokers**, qui avait publié en mars 2017 le code d'exploitation volé à la NSA, que WannaCry a utilisé, annonce qu'il lance un **« Monthly Dump Service »** accessible sur abonnement. Cette action ne semble pas avoir eu de suite, et on spécule toujours sur l'identité et les motivations des acteurs du groupe ShadowBrokers (exemple 1 et 2).
Juin 2017	Le 27/06/2018 **NotPetya** bloque des milliers d'entreprises en Ukraine (principalement) et dans le monde.
Juillet 2017	Les **marketplaces AlphaBay et Hansa** sur le **Dark Web** sont démantelées lors d'une large opération coordonnée baptisée **« Opération Bayonet »**. En août 2017,

	OxyMonster, l'administrateur de **« Dream Market »** (un autre site majeur du Dark Web) est arrêté.
Septembre 2017	**Equifax** annonce avoir subi une intrusion, de mi-mai à juillet 2017, ayant entrainé la compromission des données personnelles de 145 millions de citoyens américains. Sa communication maladroite sur cette crise est citée en exemple pour illustrer ce qu'il ne faut pas faire en cas de crise.
Septembre 2017	La société **Deloitte** annonce que son système de mails (solution Cloud Office 365) pour Deloitte US a été piraté.
Septembre 2017	Des pirates (supposés chinois) ont introduit une backdoor dans CCleaner pour tenter d'infecter des entreprises Hightech.
Septembre 2017	Une série de vulnérabilités baptisée « BlueBorne » permet d'infecter via le Bluetooth des terminaux Android, IoS, Windows, Linux, etc…
Octobre 2017	L'antivirus de Kaspersky aurait permis à des hackers russes de dérober des outils d'espionnage à la NSA. Plusieurs gouvernements recommandent de ne plus utiliser cet Antivirus sur des systèmes sensibles.
Octobre 2017	La vulnérabilité **KRACK** (Key Reinstallation Attacks) dans le protocole Wifi WPA2 permet de casser le chiffrement WPA2.
Octobre 2017	**Infineon** : la vulnérabilité **ROCA** dans la bibliothèque Infineon RSA permet de casser dans un temps raisonnable les clés RSA de moins de 2018 bits générées avec cette bibliothèque. Les cartes d'identité numériques en Espagne et en Estonie sont affectées.
Octobre 2017	**Bad Rabbit** : Ce nouveau crypto-ransomware a fait peur, car il était visuellement très proche de NotPetya, mais il s'agissait d'une attaque « drive-by » classique et d'une ampleur limitée.
Novembre 2017	La société **UBER** révèle qu'elle s'est fait voler en 2016 les données de 57 millions de clients et 600 000 chauffeurs, et qu'elle a payé les voleurs pour acheter leur silence.
Décembre 2017	**ROBOT** Attack (Return Of Bleichenbacher's Oracle Threat) : Une nouvelle attaque SSL qui permet de décrypter des communications HTTPS spécifiquement visées.
Décembre 2017	**SCADA** : FireEyes et Dragos découvrent **« Triton »**, un malware qui vise les systèmes de sureté industrielle Schneider Triconex. L'attaque rappelle Stuxnet car elle semble viser spécifiquement des installations industrielles (au Moyen-Orient). L'administration américaine publie un rapport sur ce malware en le baptisant « HatMan »
Décembre 2017	Les USA accusent la Corée du Nord d'être à l'origine de WannaCry.

3. Analyse des phénomènes les plus marquants de 2017

3.1. Le retour des vers

Si WannaCry et NotPetya ont été des crises majeures dans les entreprises touchées, c'est parce que l'attaque s'est propagée d'ordinateur en ordinateur une fois entrée dans l'entreprise. Nous n'avions plus vu ce phénomène depuis 2009, lors de la propagation du ver Conficker.

Rappel : lorsqu'une vulnérabilité touchant un composant très répandu est découverte, il peut se produire deux types d'attaques massives :

- L'attaque "en étoile" : l'attaque est lancée depuis un point central vers de multiples cibles. C'est le cas le plus courant. Dans ce cas les machines exposées à l'attaque sont uniquement celles qui sont visibles depuis Internet.
- L'attaque "par un ver" : l'attaque se propage de poste en poste. Dans ce cas, l'attaque n'est pas cantonnée aux serveurs exposés sur Internet : elle se propage aussi en interne, sur tous les postes vulnérables.

Même si ce type d'attaques est rare, le scénario d'une attaque "par un ver", doit rester une préoccupation majeure pour les entreprises. C'est un des scénarios d'attaques que nous identifions au chapitre 4.1, et contre lesquels les entreprises doivent se préparer.

3.2. Le piégeage de logiciels légitimes

C'est un phénomène que nous avions déjà vu en 2014 avec l'attaque Dragonfly/Havex, mais qui gagne en ampleur, puisqu'il a été vu à nouveau plusieurs fois en 2017 :

- Piégeage du logiciel MeDoc : L'attaque **NotPetya** a été déclenchée par le logiciel **MeDoc** ; un des 2 logiciels utilisés par les entreprises en Ukraine pour déclarer leurs taxes. Ce logiciel avait été préalablement piégé par les auteurs de NotPetya, qui avaient pour cela pris le contrôle du serveur officiel distribuant les mises à jour de MeDoc.
- Piégeage du logiciel CCleaner : la Chine est soupçonnée d'avoir piégé le logiciel CCleaner (qui permet de nettoyer et d'optimiser une installation Windows) pour s'introduire dans des entreprises High-Tech qui utilisent ce logiciel.
- Piégeage de 5 logiciels de NetSarang : 5 produits de la société **NetSarang** pour la gestion des serveurs et réseaux ont été piégés à l'insu du fournisseur en y ajoutant la backdoor **ShadowPad**.

Dans chacun de ces cas, il s'agit d'attaques visant la chaine des fournisseurs : l'attaquant compromet d'abord l'infrastructure du fournisseur et piège les fournitures qui sont ensuite envoyées légitimement à l'entreprise ciblée. Ce type d'attaques est extrêmement difficile à empêcher, et l'on est ici au-delà du constat que « la sécurité de l'entreprise dépend de celle de ses fournisseurs » puisque c'est tout ce qu'utilise l'entreprise qui peut être ainsi piégé (clé USB, logiciels, matériels). A défaut d'empêcher ce type d'attaque, il faut sans doute plutôt augmenter la capacité de l'entreprise à détecter et limiter les conséquences d'une compromission pour améliorer sa résilience.

3.3. Les failles matérielles

La recherche de vulnérabilités matérielles est un sujet actif depuis plusieurs années. Après les attaques DMA en 2011, les failles IPMI/BMC en 2013 ou Row Hammer en 2015, l'année 2017 a fourni plusieurs nouveaux exemples de failles matérielles.

Février 2017	ALSR on the Line : Contournement de la protection ASLR via une vulnérabilité du composant MMU (Memory Management Unit) Message Cert-IST : • **VulnCoord-2017.005 :** *Menace*: Vulnérabilité dans plusieurs microprocesseurs
Mai 2017	Vulnérabilité Intel AMT (Active Management Technology) Messages Cert-IST : • **CERT-IST/AV-2017.0489** : Vulnérabilité dans les micrologiciels AMT, SBT et ISM d'Intel
Octobre 2017	Vulnérabilité Roca dans la génération de clés RSA sur les matériels Infineon Message Cert-IST : • **VulnCoord-2017.024 :** *Menace* Vulnérabilité dans les modules TPM et cartes à puces utilisant la bibliothèque Infineon RSA
Novembre 2017	Vulnérabilité Intel ME (Management Unit) Messages Cert-IST : • **VulnCoord-2017.027** : *Menace*: Vulnérabilités dans les firmwares Intel • CERT-IST/AV-2017.1260 : Vulnérabilités dans les micrologiciels ME, SPS et TXE d'Intel

Cette actualité montre que le matériel, tout comme le logiciel, peut être vulnérable. Le plus souvent, il est possible de corriger ces vulnérabilités en mettant à jour les micro-logiciels (firmware) qui pilotent ces matériels. Mais le déploiement de correctifs de ce type est bien moins habituel, et bien moins rôdé que ce que les entreprises savent faire au niveau des logiciels et des systèmes d'exploitation, ce qui rend cette tâche difficile.

Nous pourrons bien sûr à nouveau parler de ce domaine l'an prochain avec les vulnérabilités Spectre et Meltdown révélées début janvier 2018 …

3.4. Les attaques « Fileless »

La généralisation des attaques sans fichier (« fileless attacks ») est un des événements marquants de 2017. Mais le terme « Fileless Attack » est trompeur et l'on devrait plutôt parler « d'attaque furtives ». Il y a en effet deux aspects qu'il faut distinguer dans cette classe d'attaques :

- Les attaques « tout en mémoire » : l'attaquant utilise ici un code qui s'installe uniquement en mémoire et n'utilise pas de fichier.
- Les attaques sans exécutable (i.e. sans « virus ») : Au lieu d'utiliser un malware classique (un virus) l'attaquant utilise des fichiers ordinaires, comme par exemple des scripts PowerShell, qu'il est difficile de différencier des fichiers légitimes. L'attaquant peut même ne pas utiliser de fichiers du tout, en insérant son script directement en argument d'une simple commande PowerShell ou WMI.

La première classe est la plus ancienne (c'est à elle que l'on pense en premier quand on utilise le terme de « fileless attack ») et plutôt rare. Il s'agit d'une technique d'attaque avancée.

La seconde est plus récente et est en forte progression depuis 3 ans. En fait, **depuis 2017 on peut considérer qu'elle est devenue la norme** et que la majorité des attaques utilisent désormais cette technique**.** Par exemple NotPetya utilise ces techniques « Fileless » pour se propager d'un ordinateur à l'autre au moyen de commandes Windows comme PsExec ou WMI.

3.5. Les effets d'imitation

Nous parlons « d'imitation », mais on pourrait aussi parler « d'effet boule de neige » ou plus justement « d'effet de diffusion » des techniques d'attaques.

On constate en effet que les techniques d'attaques se diffusent :

- Verticalement : Les cybercriminels réutilisent des outils, des techniques ou des tactiques vues initialement dans des attaques de pointes telles que celles réalisées par des états. Par exemple, les outils EternalBlue et DoublePulsar volés à la NSA en 2016 par le groupe Shadow Brokers ont été utilisés en 2017 par WannaCry (puis NotPetya). On a, à cette occasion, parlé **d'armes de guerre utilisées par des cybercriminels**.
- Horizontalement : Une fois qu'un groupe cybercriminel a utilisé une première fois une technique d'attaque, très rapidement de nombreux autres groupes se mettent à les utiliser également. Par exemple, de nombreux autres malwares ont imité WannaCry en intégrant le même modèle de propagation de poste en poste : **Adylkuzz** (crypto-miner), **Uiwix** (crypto-ransomware), **EternalRocks**, **Trickbot** (Banker), **Emotet** (Banker), **EngineBox** (Banker), …

Ce phénomène d'imitation n'est pas spécifique à 2017 mais l'attaque WannaCry l'illustre parfaitement. Globalement, au cours des années, les techniques d'attaques se diffusent et le risque d'attaque se généralise :

- De 2010 (affaire Aurora) à 2013 (affaire Snowden) tous les états ont pris conscience que les attaques cyber étaient une arme géostratégique qu'il fallait maîtriser.
- En parallèle, les cybercriminels ont fait évoluer leurs attaques en utilisant des scénarios plus évolués, similaires aux attaques APT réalisées par les états. C'est le cas par exemple dans l'attaque des magasins Target fin 2015 ou de la Banque du Bangladesh en 2016.
- De mêmes, les « arnaques aux présidents » (qui ne sont pas à proprement parler les cyber-attaques mais plutôt de l'ingénierie sociale) utilisent désormais couramment des outils d'intrusion pour compromettre les ordinateurs de leurs victimes et mieux les manipuler.

3.6. Le cryptojacking

Depuis l'été 2017, de plus en plus d'attaques ont pour but d'installer sur les systèmes infectés un logiciel de crypto-minage, qui fonctionne en tâche de fond, et dont les bénéfices générés sont versés à l'attaquant. **On appelle "crypto-jacking" ce type d'attaque** (hijacking de CPU pour générer de la crypto-monnaie). Ces attaques visent :

- soit directement les internautes : un logiciel de minage est installé illégalement sur le poste des internautes infectés,
- soit des sites web compromis : un code de minage (par exemple JavaScript) est ajouté aux sites web et l'internaute l'exécute lorsqu'il les visite.

C'est la crypto-monnaie "Monero" qui est le plus souvent utilisée (le Bitcoin étant trop difficile et cher à miner), et ces attaques sont souvent réalisées aux moyens d'outils tels que :

- xmrig : un logiciel open-source de crypto-minage
- CoinHive.com : un site qui propose le code de minage à insérer sur les sites web.

Ces deux services sont généralement considérés comme légaux : ce qui est illégal c'est d'installer ces codes de minage à l'insu de l'internaute ou du propriétaire du site web.

3.7. Les botnets IOT

L'absence totale de sécurité des « petits équipements raccordés à Internet » (que l'on appelle désormais les IOT) n'est plus à démontrer. Il est souvent trivial de les pirater, par exemple en utilisant les mots de passe par défaut avec lesquels ces équipements ont été configurés. Par conséquence, ces équipements sont très souvent piratés à distance (s'ils sont visibles depuis Internet) et enrôlés dans des botnets. Ce phénomène est apparu en octobre 2016 avec le botnet Mirai. Il s'est poursuivi en 2017, en améliorant progressivement les méthodes de compromissions utilisées (utilisation de failles connues, ou même de 0-day, plutôt que de mots de passe par défaut) avec des botnets tels que Hajime, Reaper, Satori ou Okiru.

Il s'agit de piratages faciles (pas de difficulté technique), mais qui génèrent des nuisances certaines (attaque DDOS, atteinte potentielle à la vie privée) du fait de la multiplication des objets non sécurisés qui sont maintenant connectés à Internet.

4. Points de vigilance

Les attaques vues en 2017 permettent d'identifier des domaines où il faut que les entreprises fassent preuve d'une vigilance accrue afin de limiter les crises possibles ou de mieux s'y préparer.

4.1. Les scénarios types d'attaques

En 2017, trois types d'attaques ont particulièrement marqués l'actualité, et il faut que les entreprises évaluent leur capacité de résistance et leur plan de secours face à ces cas :

- **La propagation d'un ver dans l'entreprise** : Nous avons déjà évoqué ce point en parlant de WannaCry et du retour des attaques qui se propagent de poste en poste. Le scénario d'attaque le plus réaliste est le cas où, après l'infection d'un premier poste au sein de l'entreprise (par exemple au moyen d'un mail piégé ouvert depuis ce poste), l'infection se propage ensuite automatiquement de poste en poste au moyen des partages réseaux. Le point clé ici est de mettre en place des mécanismes d'isolation qui pourront limiter la propagation de l'infection.
- **Les attaques de sabotage** : dans ce scénario, de plus en plus classique (cf. TV5Monde en 2015, ou NotPetya en 2017) l'attaquant, après avoir infecté un grand nombre d'ordinateurs dans l'entreprise, décide de déclencher une procédure de destruction des ordinateurs infectés (typiquement en effaçant les disques). Cette fois, c'est la capacité de l'entreprise à faire face à une attaque mettant hors service une grande partie de son système d'information qui est mise en question.
- **Les attaques par crypto-ransomware** (qui ont culminé en 2016 et début 2017). Ici le but des attaquants est de bloquer des ressources critiques de l'entreprise (chiffrer les données), afin d'obtenir le paiement d'une rançon.

Une des façons de se préparer face à ce type d'événement peut être d'organiser des exercices de simulation de crise. On peut noter dans ce domaine l'initiative du CLUSIF qui a organisé en 2017 un exercice de cyber-crise baptisé « ECRAN 2017 », qui simulait une crise de type crypto-ransomware dans le milieu hospitalier, et dont nous avons publié un compte-rendu dans notre bulletin mensuel de septembre 2017. Il est aussi souvent possible d'éviter les crises en identifiant leurs prémices et en appliquant régulièrement les correctifs de sécurité. Par exemple, pour l'attaque WannaCry, le Cert-IST a émis un avis deux mois avant et un Danger Potentiel un mois avant.

4.2. La sécurité du cloud

Les entreprises s'appuient aujourd'hui de plus en plus sur des infrastructures externalisées. Il peut s'agir de choix d'entreprise (par exemple en externalisant sa messagerie), mais aussi de décisions projets (conception d'une solution Amazon AWS, développements hébergés sur GitHub, etc.) ou mêmes d'initiatives individuelles (utilisation d'espaces de partages documentaires GoogleDoc, échanges de données PasteBin, etc.).

L'année 2017 a donné de nombreux exemples des problèmes sécurité que cela peut induire, et nous en listons quelques exemples ci-dessous.

Swedish Government Blamed for Mega Data Leak - infosecurity-magazine.com – 24/07/2017

Le gouvernement Suédois a été accusé de négligence pour avoir confié à IBM la gestion de son infrastructure informatique sans avoir imposé de clauses d'habilitation sur le personnel autorisé à manipuler les données.

Source: Deloitte Breach Affected All Company Email, Admin Accounts - KrebsOnSecurity.com - 25/09/2017

La société de conseil Deloitte s'est fait pirater sa messagerie hébergée sous Office 365 : apparemment, les accès administrateurs se faisaient par simple mot de passe, sans utiliser d'authentification à double facteur.

Dow Jones Leaks Personal Info of 2.2 Million Customers - infosecurity-magazine.com - 17/07/2017

La société financière Dow Jones a mal protégé des données internes stockées dans un bucket Amazon AWS S3, ce qui permettait à n'importe quelle personne ayant un compte Amazon AWS d'y accéder depuis Internet.

Hundreds of companies expose PII, private emails through Google Groups error - ZDNet - 24/07/2017

Selon la société RedLock.io, un grand nombre d'entreprises utilisant les groupes Google (comme outil de discussion entre employés) ne configurent pas correctement les permissions de l'outil ce qui rend certaines discussions visibles sur Internet.

Thousands of Elasticsearch installs compromised to host PoS Malware - SecurityAffairs.co - 14/09/2017

Plusieurs milliers de serveurs ElasticSearch hébergés sur AWS étaient installés sans sécurité (aucune option de sécurité n'avait été activée, probablement parce qu'il s'agissait de tests du produit, sans objectif de mise en production). Ces configurations non sécurisées ont pu alors être facilement piratées, et ont servi dans ce cas à héberger des malwares.

Uber quits GitHub for in-house code after 2016 data breach – TheRegister.co.uk – 07/02/2018

La société Uber s'est fait voler en 2016 des codes d'accès Amazon AWS S3 qui étaient stockés dans un espace GitHub mal protégé. Le schéma d'attaque probable est le suivant : vol des logins et mots de passe GitHub (ou mot de passe trivial ?), recherche de jetons d'authentification AWS dans les sources GitHub, intrusion dans l'espace AWS et vol des données Uber.

4.3. SCADA : Industrial-IOT et Entreprise 4.0

L'arrivée de nouvelles technologies (le Cloud, l'Intelligence Artificielle, et l'IOT) est annoncée comme une révolution pour l'usine du futur, que l'on appelle désormais l'Entreprise 4.0. On imagine bien les perspectives énormes d'évolution que toutes ces technologies pourraient amener à une unité de production. Mais la demande d'ouverture et d'agilité que cette révolution implique est clairement inquiétante si la cyber-sécurité n'est pas prise en compte.

5. Productions du Cert-IST en 2017

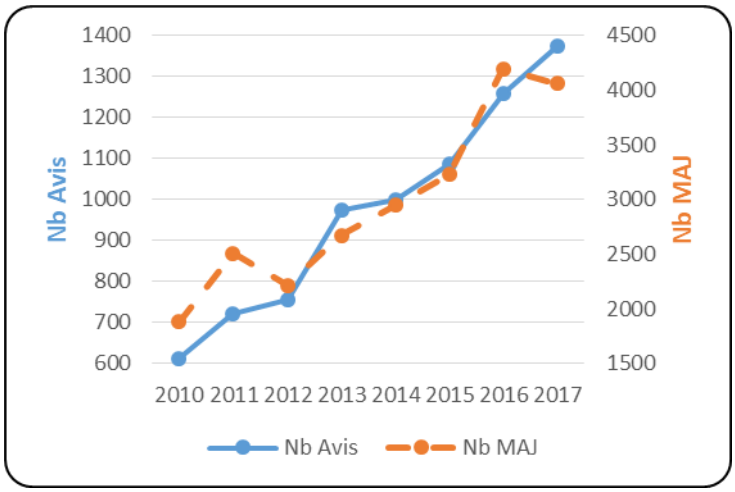
5.1. Veille sur les vulnérabilités et des menaces

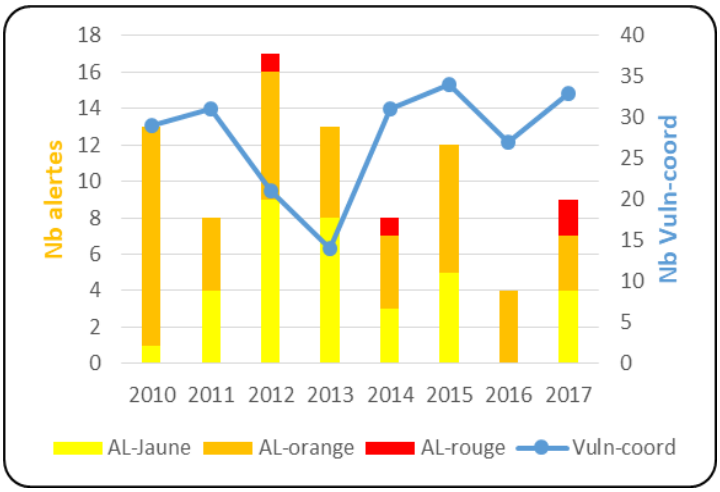
Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST suit de façon continue, différentes sources d'informations (annonces constructeurs, blogs sécurité, mailing-lists, échanges entre CERTs, etc.) afin d'être informé des nouvelles vulnérabilités. Ces informations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

Le Cert-IST émet ainsi plusieurs types de publications :

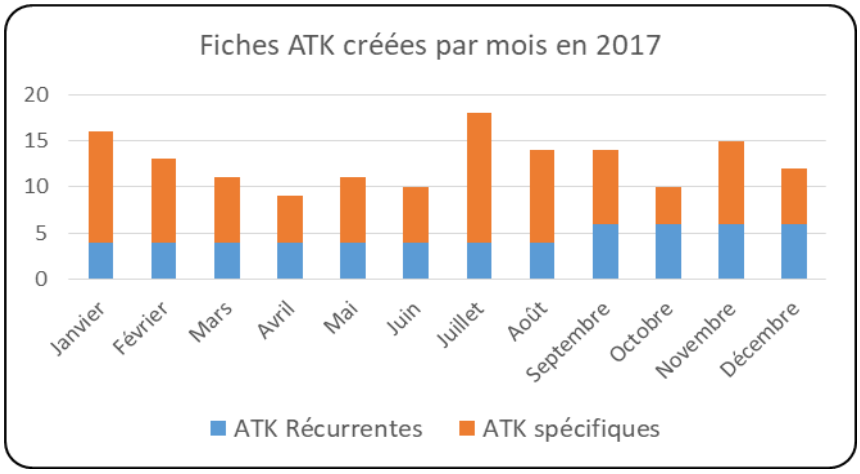
- **Les Avis de sécurité (AV)** : ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis sont enrichis de façon continue avec des mises à jour mineures ou majeures. Ces dernières correspondent typiquement au cas où des programmes d'attaques – des "exploits" – sont publiés.
- Des **Alertes (AL)**, qui sont émises lorsqu'il y a un risque spécifique d'attaque, et les **messages "Vuln-coord",** qui permettent d'apporter un commentaire sur des vulnérabilités particulières (par exemple médiatisées) mais d'une dangerosité immédiate plus faible. Ces 2 catégories sont axées sur les risques d'attaques alors que les avis de sécurité répertorient eux de façon systématique toutes les vulnérabilités (quelle que soit leurs probabilités d'être utilisées dans des attaques et leur dangerosité).
- Des **Fiches Attaques (ATK)** et des **indicateurs de compromission** (IOC) à travers une base de données MISP. Elles répertorient les attaques majeures, qu'il s'agisse de menaces récurrentes (MalSpam, Exploit-Kit, Ransomware), ou de cas de cyber-espionnages (attaques APT). Ce nouveau service est opérationnel depuis juillet 2016.

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





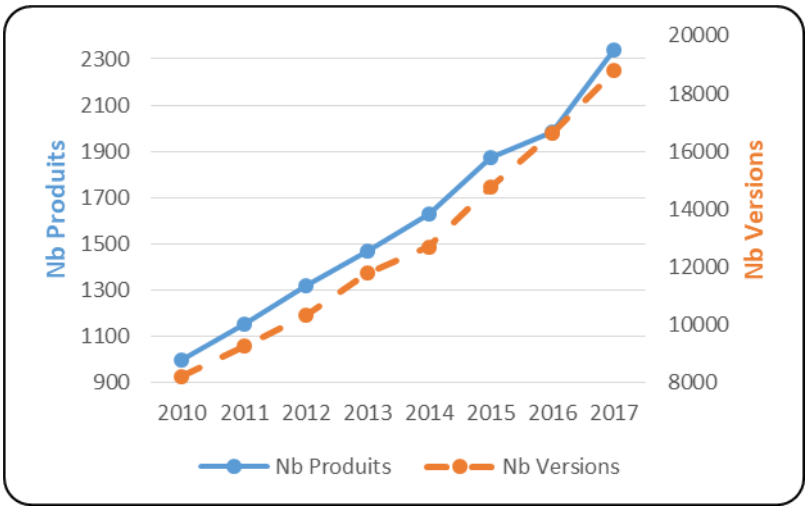
Nota : les Alertes jaunes et les Alertes orange correspondent à ce qui était appelé antérieurement les DanGers Potentiels (DG).



Ainsi, en 2017, le Cert-IST a publié :

- **1 374** avis de sécurité (dont 81 avis SCADA), **4 060** mises à jour mineures et **138** mises à jour majeures. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec une augmentation de **9%** par rapport à 2016. Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène en constante augmentation. Le maintien du niveau de sécurité passe donc encore et toujours par une application régulière des correctifs de sécurité sur les produits présents dans le système d'information.
- **9** alertes, dont 2 alertes rouges (Wannacry et NotPetya) et **33** messages "Vuln-coord". Globalement l'activité dans cette catégorie a augmenté de façon significative par rapport à 2016, pour revenir à des valeurs comparables à 2014 ou 2015.
- **153** fiches attaques ont été publiées en 2017, avec dans la base de données MISP **2 154** évènements qui ont été enrichis, et **178 242** IOC utilisables comme signatures.

Concernant les produits et les versions suivis par le Cert-IST, fin 2017 le Cert-IST suivait **2 338** produits et **18 780** versions de produit. Le graphique suivant montre l'évolution du nombre des produits et des versions qui sont suivis par le Cert-IST.



5.2. Veille technologique

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

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

6. Conclusions

- **Un champ d'exploration de plus en plus large pour la recherche de vulnérabilités**

Depuis plus d'une dizaine d'années, les compétences et le nombre de chercheurs en vulnérabilités se sont multipliés, ce qui a amené ces derniers à explorer progressivement de nouveaux domaines technologiques. Au-delà de la traditionnelle recherche de vulnérabilités sur Windows ou sur les logiciels applicatifs, on a vu alors apparaitre de nouvelles recherches : Android d'abord (et les smartphones en général), mais aussi la cryptanalyse, les cartes à puces, la sécurité matérielle, les signaux radios, le SCADA, l'automobile, l'IoT, le biomédical etc… Ces nouveaux champs d'investigations semblent se multiplier à l'infini.

De plus, le déplacement des données et des traitements dans le Cloud a induit de nouveaux risques de fuites de données. S'il y a quelques années ces fuites étaient souvent dues à des vulnérabilités SQL dans des sites web, en 2017 elles sont de plus en plus souvent dues aussi à des données déposées sans protections dans des services cloud accessibles sur Internet : mots de passes ou tokens d'authentification volés dans Github, accès non protégé sur des espaces Amazon S3, etc…

Face à cette évolution permanente des risques, l'entreprise doit maintenir une veille active afin d'identifier ces nouvelles menaces, évaluer son exposition et décider des mesures de protection à mettre en place.

- **Les états accusés d'être à l'origine des crises cyber**

Depuis plusieurs années, les états sont régulièrement soupçonnés d'être impliqués dans des cyber-attaques ayant des visées économiques ou politiques. **2017 marque une progression significative dans ce domaine** puisque les Etats Unis et leurs alliés du « Five Eyes » accusent désormais ouvertement des pays comme la Corée du Nord (pour Wannacry) ou la Russie (pour NotPetya) d'être à l'origine des crises majeures qui ont marquées 2017. En parallèle, les USA semblent avoir trouvé un terrain d'entente avec la Chine en passant des accords de non-agression cyber pour le domaine économique.

S'il y a sans doute un fond technique dans ce type d'accusation, on se doute bien qu'il y a aussi une large part de stratégie diplomatique et de manipulation de l'information. On peut constater par exemple que la **Corée du Nord** est soudainement passée en 2017 du statut de « puissance mineure dans le domaine cyber » (image donnée fin 2014 au moment de l'attaque destructrice ayant visé Sony Pictures Entertainment aux USA) à celui d'expert aguerri impliqué dans le piratage à grande échelle et les attaques visant les crypto-monnaies.

- **Des attaques faciles à mettre en œuvre**

Avec la diffusion d'outils volés à la NSA (comme « EternalBlue » utilisé par WannaCry) ou les attaques triviales des objets connectés non sécurisés (botnets IOT), certaines des attaques majeures de 2017 étaient en fait faciles à mettre en œuvre. Il est également étonnant de voir comment les attaquants adoptent vite les nouvelles techniques d'attaques. Par exemple, au cours de l'été 2017, les crypto-ransomwares (qui étaient l'attaque dominante depuis 2 ans) ont soudain cédé la place aux attaques de crypto-jacking (voir § 3.6). Cela montre une capacité de mutation très rapide de la part des cybercriminels.

- **RGS, LPM, RGPD, NIS : le cadre réglementaire/législatif pousse à la sécurisation des infrastructures**

Depuis plusieurs années, les autorités françaises ont entrepris des actions de sécurisation en mettant en place successivement des référentiels de sécurisation pour les administrations (via le RGS : Référentiel Général de Sécurité), puis les OIV (Opérateurs d'Importance Vital), et maintenant les OSE (Opérateur de Services Essentiels, avec la transposition en cours en France de la directive européenne NIS - Network Information Security).

Ces actions, bien que contraignantes, sont largement nécessaires pour limiter la vulnérabilité des installations. La France est d'ailleurs considérée comme un exemple à suivre sur ce point par les autres pays européens.

- **Globalement les entreprises restent largement exposées aux risques d'attaques**

Comme nous l'avons vu tout au long de ce rapport, les menaces restent très présentes et évoluent en permanence. L'entreprise ne peut clairement pas laisser l'informatique se développer sans contrôle, et doit surveiller les nouveaux usages afin de détecter les pratiques dangereuses.

Recenser les équipements et les pratiques, segmenter les réseaux, appliquer les correctifs de sécurité et superviser la sécurité sont aujourd'hui des clés pour conserver le contrôle sur la sécurité des systèmes d'information.

Association Cert-IST
126 rue de Gallieni
92643 Boulogne-Billancourt cedex France
info@cert-ist.com
https://www.cert-ist.com
05.34.39.44.88