Industrie Services Tertiaire

# Bilan Cert-IST des failles et attaques de 2018

Publié en Mars 2019

# 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 2018 (cf. chapitre 2), puis nous analysons les éléments les plus significatifs (cf. chapitre 3). Au-delà de ces faits d'actualité, nous rappelons ensuite les problèmes récurrents sur lesquels il faut rester vigilant (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 et permettre une remise en service opérationnelle et sécurisée.

# 2. Cela s'est passé en 2018

Le tableau ci-dessous récapitule des événements marquants de 2018. Nous y retrouvons les événements qui se sont distingués, soit parce qu'ils ont été fortement médiatisés (parfois sans réalité technique, comme par exemple le cas des puces espionnes sur les cartes mère Supermicro en octobre 2018), soit plus généralement parce que ce sont des marqueurs de la progression de la menace cyber.

| | |
|---|---|
| Janvier 2018 | Les vulnérabilités **Spectre et Meltdown** sont publiées. Pendant 3 mois les correctifs vont se succéder (processeurs, OS, navigateurs web) mettant en évidence la difficulté du traitement de ces failles de bas niveau. Nous approfondissons ce sujet au chapitre 3.3. |
| Janvier 2018 | L'application mobile **Strava**, qui permet d'enregistrer des activités sportives via GPS, a permis de géolocaliser des bases militaires américaines. |

| | |
|---|---|
| Février 2018 | GitLeaks (outil de recherche de clés d'accès pour AWS - ou autres - dans GitHub) & BuckHacker.com (moteur de recherche de serveurs AWS S3 vulnérables) : les outils visant les **espaces Cloud mal protégés** se multiplient. Amazon rend gratuit son outil « S3 Bucket Permissions Check tool ». |
| Février 2018 | Le malware **Olympic Destroyer** perturbe (légèrement) l'ouverture des jeux d'hiver en Corée du Sud. Il est surtout le 1er exemple d'un malware embarquant des **faux indices sophistiqués** (false flags) visant à tromper les analystes dans l'attribution de l'attaque. |
| Février 2018 | Une nouvelle technique d'**attaque DDOS par amplification** via des serveurs **Memcached** mal protégés a permis de générer un flux DDOS record de 1.3 Tbps contre GitHub.com et OVH. |
| Mars 2018 | **www.cert.org** (aka CERT/CC) c'est fini ! C'était le 1er CERT, créé en 1988 suite au ver de Morris. Animé par le SEI, il était passé au second plan avec l'arrivée de l'US-CERT (en 2006). |
| Mars 2018 | **Trustico** (vendeur de certificats SSL) se discrédite en révélant qu'il a conservé une copie des clés privées des certificats numériques de ses clients. |
| Mars 2018 | Surfant sur la vague Spectre/Meltdown, la société CTS-Labs publie un rapport alarmiste sur les **vulnérabilités des processeurs AMD** ainsi qu'un site web dédié : AMDflaws.com. La communauté sécurité critique fortement cette communication de CTS-Labs. |
| Mars 2018 | Les techniques d'attaques pour **tromper les systèmes d'IA** se multiplient. |
| Mars 2018 | Le malware **Triton** découvert fin 2017 et qui visait les automates de sûreté industrielle Schneider Triconex aurait été conçu pour provoquer une explosion sur une installation pétro-chimique en Arabie Saoudite. Après avoir tout d'abord pointé l'Iran, les analystes ont indiqué plus tard (octobre 2018) que les russes pourraient être à l'origine de cette attaque. |
| Mars 2018 | Le ransomware **SamSam** réclame $50 000 (6 bitcoins) à la mairie d'Atlanta. Le modèle du ransomware change : plutôt que des attaques au hasard pour une rançon de 0,1BTC, les escrocs attaquent des entreprises (ou organisations) pour de fortes rançons. Cette tendance s'accentue à partir de la mi-2018 avec l'apparition du malware **Ryuk**, dont une variante (**LockerGoga**) a touché la société Altran début 2019. |
| Mars 2018 | **Facebook** fait face à un premier scandale avec l'affaire **Cambridge Analytica** (campagne électorale de 2016 aux USA). En septembre, ce sera **le bug « Voir en tant que »** qui aurait pu permettre de pirater près de 50 millions de comptes Facebook et en décembre le bug de l'accès aux photos privées.<br><br>Voici un aperçu en anglais et en français récapitulant les autres événements de cette année bien difficile pour Facebook… |
| Avril 2018 | « Don't mess with our elections … » : C'est le message que des **hackers américains patriotes** affichent sur 200 000 équipements réseaux Cisco mal protégés, principalement en Iran et en Russie. C'est probablement la vulnérabilité Cisco Smart Install (SMI), aussi citée ci-dessous par l'US-CERT, qui a été utilisée. |

| | |
|---|---|
| Avril 2018 | L'US-CERT publie l'alerte TA18-106A à propos d'**attaques systématiques par les Russes sur des routeurs** mal protégés. Le CERT pointe en particulier les vulnérabilités connues de Cisco Smart Install (SMI) et les accès SNMP mal protégés. |
| Avril 2018 | **Drupalgeddon2** (Drupal Armageddon 2) : deux failles critiques corrigées dans le CMS Drupal vont donner lieu dans les mois suivants à des attaques massives contre les serveurs web Drupal non mis à jour. |
| Mai 2018 | Vulnérabilités **EFAIL** dans **OpenPGP**, S/MIME et les clients de messagerie. |
| Mai 2018 | **MEWkit** (MyEtherWallet-Kit) : une **attaque par détournement BGP** qui pendant quelques heures a détourné le trafic destiné aux serveurs DNS Amazon Route 53. |
| Mai 2018 | Cisco TALOS publie en avance ses recherches sur **VPNFilter**, un malware qui infecte les équipements réseaux mal protégés. Cisco pense que VPNFilter est Russe et pourrait être utilisé dans une cyber-attaque imminente contre l'Ukraine. |
| Mai 2018 | Le **RGPD** entre en vigueur dans tous les pays de l'UE. Au 16/10/2018 la CNIL avait reçu 742 notifications (en 7 mois), soit près de 7 par jour. On a vu aussi apparaitre en parallèle des arnaques aux RGPD (voir le chapitre 4.1). |
| Juin 2018 | **Attaques Docker** : des images malveillantes hébergées sur Docker Hub permettent d'attaquer des environnements Docker mal protégés. Voir notre article bulletin sur ce sujet. Ce type d'attaque a été de nouveau observé en octobre. |
| Juin 2018 | La Commission Européenne cite l'anti-virus **Kaspersky** comme un exemple de **logiciel malveillant à éviter**. La crainte est que les services secrets russes utilisent Karpersky dans des opérations d'espionnage. Les Etats-Unis avaient fait des recommandations similaires en septembre 2017. |
| Juillet 2018 | Vague d'escroqueries de type « **Sextorsion** » : un pirate demande une rançon par mail à ses victimes en prétendant les avoir filmées lorsqu'elles visitaient des sites pornographiques. Ces escroqueries seront vues de nombreuses fois au cours du second semestre 2018 (voir ce rapport Cisco Talos). |
| Juillet 2018 | Recrudescence des **attaques « SIM swap »** (ou « SIM hijack »), qui permettent de prendre le contrôle de comptes (Instagram, Twitter, etc…) en volant le numéro de téléphone de la victime. Cela met aussi en défaut l'authentification 2FA si celle-ci est basée sur la réception de codes par sms. |
| Juillet 2018 | Une **cyber-attaque contre l'hôpital SingHealth à Singapour** est révélée : 1,5 millions de données personnelles sont concernées, y compris les prescriptions médicales du premier ministre. La sophistication de l'attaque fait penser à une attaque d'un état étranger. Le rapport final a été publié en janvier 2019. |
| Septembre 2018 | **British Airways** a été victime d'une attaque **MageCart** qui a infecté le système de paiement de son site web et volé 380 000 cartes bancaires en 2 semaines (du 21 août au 5 septembre). Depuis plusieurs mois, les attaques "MageCart" se multiplient. Parfois ce sont des sites de fournisseurs qui sont visés, de façon à infecter tous les sites marchands utilisant le produit en question, comme dans le cas de l'incident |

| | |
|---|---|
| | TicketMaster en juillet 2018. Cette actualité illustre 2 phénomènes marquant de 2018 : les attaques bancaires (cf. chapitre 3.4) et les attaques via les fournisseurs (cf. chapitre 3.6). |
| Septembre 2018 | Découverte de **LoJax** : le premier cas d'un **rootkit UEFI** utilisé dans une attaque réelle. Il s'agirait d'une attaque du groupe russe APT28 (Sofacy). |
| Septembre 2018 | Dans la cadre de la **directive européenne NIS**, la France publie les règles de sécurité applicables aux OSE (Opérateurs de Services Essentiels). Une première liste identifiant 122 OSE est établie début novembre. Elle devrait contenir à terme plusieurs centaines d'organismes. |
| Octobre 2018 | Le journal Bloomberg publie un article à propos de **puces espionnes ajoutées par la Chine à des cartes mères Supermicro** dans le but d'infecter les ordinateurs de sociétés américaines telles qu'Apple ou Amazon. Tout le monde dément. Sur le fond, l'ajout d'une puce espionne ne parait pas une prouesse technologique, mais le piégeage à large échelle de composants électroniques serait une première. |
| Octobre 2018 | L'US-CERT publie une note pour mettre en garde contre **les attaques APT passant par l'infrastructure des infogérants**. Dans un webinaire intitulé « Chinese Cyber Activity Targeting Managed Service Provider », l'US-CERT précise que ces attaques baptisées **Cloud Hopper** sont apparues en 2014, sont montées en flèche en 2016 et se poursuivent depuis. |
| Novembre 2018 | Plus de 50 000 imprimantes mal protégées se mettent à imprimer un flyer promouvantla chaine YouTube de **PewDiePie**. Selon l'auteur de cette blague, c'est au total 800 000 imprimantes qui auraient pu être attaquées. |
| Novembre 2018 | **Le téléphérique de Moscou** est interrompu suite à une infection par un rançongiciel. |
| Novembre 2018 | Les **hôtels Marriott** annoncent une fuite de données massive sur la base de données de réservation de sa filiale **Hotels Starwood** : 500 millions de réservations, pour un incident qui dure depuis 2014 . |
| Décembre 2018 | **Shamoon**, un malware destructeur découvert en 2012 en Arabie Saoudite (incident Saudi Aramco), réapparait dans plusieurs pays en Europe avec une V3 : en Italie (incident Saipem), au Pays-Bas et en France. |
| Décembre 2018 | Amnesty International publie un article qui décrit pour la première fois des attaques réelles mettant en défaut le 2FA (attaques par relayage, appelées aussi MiTM - Man In The Middle). **Elles visent le 2FA sms mais aussi les 2FA à base d'OTP** comme Google Authenticator, Authy, Duo, etc.. |
| Décembre 2018 | Plusieurs rapports sur la société russe IRA (**Internet Research Agency**, appelée ironiquement la « boite à Troll » du gouvernement Russe) décrivent les campagnes de désinformation russes, via les réseaux sociaux, pour influencer les élections américaines de 2016. |

# 3. Analyse des phénomènes les plus marquants de 2018

## 3.1. Ils se sont particulièrement distingués cette année

Dans ce premier chapitre, à la façon d'une remise de prix, nous distinguons les vulnérabilités et les malwares qui ont été les plus présents dans l'actualité de 2018.

- **Nouveauté de l'année : Meltdown & Spectre**

Nous développons ce point au chapitre 3.3 car les vulnérabilités Meltdown et Spectre publiées en janvier 2018 sont pour nous un des événements majeurs de l'année.

- **Botnet de l'année : Emotet**

Emotet (aussi connu sous les noms Geodo et Feodo) a été le botnet le plus présent en 2018. Ce malware existe depuis 2014 et était à l'origine un malware bancaire (un « banker ») qui infecte l'ordinateur de particuliers pour leur voler des données bancaires. Emotet a évolué depuis, pour devenir un "downloader" (on parle aussi de MDS : "Malware Distribution System" ou "Malware Delivery Service"), c'est à dire que les cybercriminels qui contrôlent l'ensemble des machines infectées par Emotet vendent à d'autres cybercriminels le service de propager d'autres malwares (en organisant des campagnes de spam envoyant des mails infectés) ou même d'installer des malwares directement sur les machines du botnet.

- **Payload de l'année : Le Crypto-mineur**

Pour gagner de l'argent, un cybercriminel doit définir son business-model : il peut décider de vendre du service à d'autres cybercriminels, par exemple avec le service de MDS que nous avons décrit pour Emotet. Il peut aussi décider de voler de l'argent aux utilisateurs qu'il a infecté. Dans cette catégorie, on avait vu en 2016 les attaques par crypto-ransomwares : le pirate chiffre les données de l'utilisateur et réclame une rançon. En 2018, le modèle le plus répandu a été celui des crypto-mineurs. Nous détaillons ce phénomène au chapitre 3.8.

- **Vulnérabilité de l'année : la dé-sérialisation Java**

La dé-sérialisation est une opération permettant d'importer un objet Java dans une application. Si cette application est vulnérable (bug de dé-sérialisation), un objet Java malveillant peut forcer le moteur de dé-sérialisation à exécuter un code arbitraire. Ce type de vulnérabilités a été découvert en 2006, mais il est devenu très populaire en 2017 et en 2018. La dé-sérialisation est d'ailleurs listée au 8eme rang dans le TOP-10 de l'OWASP, et est répertoriée CWE-502 dans le dictionnaire Mitre. Cette vulnérabilité n'affecte pas que Java : PHP, .NET et même Ruby sont également affectés.

Voici des exemples d'applications web vulnérables ; on y retrouve presque tous les grands noms des applications web Java (et autres) : CVE-2018-15957 (**ColdFusion**), CVE-2018-1567 (**WebSphere**), CVE-2018-3245 (**WebLogic**), CVE-2018-14667 (**JBoss**), CVE-2018-8421 (**SharePoint**).

## 3.2. Le RGPD peut-il endiguer les incessantes fuites de données ?

Depuis plusieurs années, le nombre d'attaques et le volume des données volées est en constante augmentation. A tel point que l'on ne s'étonne plus à l'annonce d'une nouvelle fuite de données, sauf si celle-ci dépasse en volume les fuites précédentes. Si l'on cherche les causes de ces fuites de données (qu'elles soient accidentelles ou le résultat d'une attaque), on peut les classer en trois catégories :

- Les données n'étaient pas assez protégées (défaut de protection),
- Les données étaient protégées mais une vulnérabilité a été découverte dans les mécanismes de protections,
- Une attaque élaborée a permis de contourner les protections.

Il arrive parfois que des données ne soient pas du tout protégées. Mais il est plus courant que les protections qui ont été mises en place au démarrage du système se révèlent vulnérables quelques années plus tard. Le maintien du niveau de sécurité est donc un élément clé de la sécurité, pour prendre en compte :

- les vulnérabilités découvertes (a-t-on appliqué les correctifs de sécurité ?)
- mais aussi l'évolution des technologies et de techniques d'attaques (par exemple nos serveurs Amazon S3 sont-ils correctement configurés ?)

L'entrée en vigueur du RGPD va améliorer le niveau de sécurité des applications qui gèrent des données personnelles (c'est-à-dire presque toutes les applications). On peut donc espérer que cela aura un impact à termes pour diminuer les fuites de données, mais il est bien sûr difficile d'évaluer à quel horizon.

## 3.3. Spectre et Meltdown : il faut apprendre à patcher les firmwares

En janvier 2018, les attaques **Spectre** et **Meltdown** ont fait apparaitre une nouvelle classe d'attaques : l'attaque du mécanisme **d'exécution spéculative** dans les micro-processeurs. Ces attaques visent directement le fonctionnement interne des processeurs et nécessitent une mise à jour de leur firmware (micro-code). Ce n'est pas la première fois que des attaques de bas niveau nécessitent ce type de mises à jour (voir par exemple Intel AMT en mai 2017 ou Row Hammer en 2015) mais cette fois le produit visé est très répandu (les processeurs Intel). La mise à jour d'un firmware est une opération complexe dans un contexte d'entreprise car les outils de déploiement sont peu rôdés à ce type d'opération. Elle reste donc une opération exceptionnelle.

Dans le cas de Spectre et Meltdown, on retiendra :

- La **complexité des correctifs** (3 niveaux de correctifs ont été publiés : correctifs au niveau des navigateurs web, correctifs pour le système d'exploitation et correctifs au niveau des processeurs) et l'instabilité de certains correctifs (incompatibilité avec certains antivirus, manque de fiabilité de certains correctifs Intel, impacts éventuels sur les performances).
- La **difficulté pour déterminer l'urgence** pour le déploiement des correctifs. Au départ, à la vue de la gravité des vulnérabilités, le déploiement des correctifs semblait urgent. L'absence d'attaques réelles et la complexité de déploiement des correctifs a amené à réviser ce jugement.

La gestion des vulnérabilités reste une activité complexe où il faut composer avec des correctifs incomplets et un risque d'attaques difficiles à prévoir et souvent surmédiatisées. Il est important de disposer des informations les plus factuelles possibles et c'est ce que nous cherchons à fournir au travers des publications du Cert-IST. Dans le cas de Meltdown et Spectre, nous avons évalué les vulnérabilités à un risque moyen (car l'impact est "uniquement" le vol de données) et le risque d'attaques est resté au

niveau jaune (le plus faible des 3 niveaux d'alertes). Nous utilisons pour ces évaluations des métriques pilotées par des arbres de décisions. Même si cela est perfectible, cette approche a l'intérêt d'être rationnelle, ce qui permet de modérer l'emballement médiatique qu'une actualité peut produire.

## 3.4. Les banques ciblées par de nouvelles attaques

De 2010 à 2016, de nouvelles techniques sont apparues pour les attaques visant les banques ou les terminaux de paiement. Nous les présentons ci-dessous, en reprenant un article publié dans notre bulletin mensuel de décembre 2018. L'année 2018 est pour nous une année charnière pour les attaques visant les banques, car :

- Le nombre de ces nouvelles attaques a augmenté de façon significative,
- On observe une extension géographique progressive des cibles. A l'origine, les attaques visaient plutôt les pays satellites de la Russie, l'Asie du Sud-Est et l'Amérique du Sud ; aujourd'hui, elles semblent s'étendre vers le reste du monde et en particulier l'Europe et les Etats-Unis.

*Extrait de l'article publié dans le bulletin Cert-IST de décembre 2018*

- **Jackspotting :**

  Cette technique consiste à attaquer les distributeurs automatiques de billets (DAB) de façon à leurs « faire cracher » leur réserve de billets. Un scénario typique est celui où un attaquant se présente devant le distributeur, perce un trou dans la façade, et branche une clé USB malveillante sur le PC qui pilote le distributeur. Il peut alors utiliser cette clé USB pour prendre le contrôle du PC (par exemple avec une attaque de type « Rubber Ducky ») et faire éjecter les billets de banque .

  Cette technique est connue depuis 2010 où elle avait été démontrée lors de la conférence de sécurité BackHat USA par Barnaby Jack. Les attaques réelles sont apparues quelques années plus tard. Il existe sur le marché underground des kits, appelés des « **black box** », pour réaliser ce type de piratage. Selon Europol (cf. cette annonce de mai 2017), 15 incidents blackbox ont été répertoriés en Europe en 2015 et 58 en 2016, ce qui montre la progression importante de ces attaques. Les médias grands publics (cf. cet article de LCI) indiquent que le phénomène touche également la France depuis 2017. Enfin, les services secrets des Etats-Unis ont émis en janvier 2018 un avertissement public sur de possibles attaques en préparation aux Etats-Unis. Il existe donc visiblement un déplacement des attaques, depuis leurs pays d'origine (par exemple Roumanie, Moldavie, Russie et Ukraine) vers l'Europe de l'Ouest et les Etats-Unis.

- **Intrusions avancées (APT)**

  Il s'agit ici de « cyber-casses » : des pirates entrent illégalement sur les systèmes informatiques internes d'une banque (typiquement au moyen d'une attaque de type spear-phishing), s'y installent (pour surveiller l'activité interne, collecter des informations et attendre le moment le plus opportun), puis réalisent des malversations comme des virements interbancaires (par exemple SWIFT). Ces attaques sont similaires aux attaques APT vues depuis 2010 dans d'autres secteurs d'activités (espionnage industriel). Dans le monde bancaire elles sont apparues en 2014 avec **Carbanak** et sont devenues significatives en 2016 avec l'attaque de la banque centrale du Bangladesh. En 2018, on notera l'attaque de la banque PIR en Russie (juillet 2018, attribuée à des cybercriminels isolés) et l'attaque de la banque Cosmos en Inde (août 2018, aujourd'hui attribuée à la Corée du Nord).

Ces attaques semblent pour le moment toucher des établissements financiers de petites tailles dans lesquels les mesures de sécurité sur les systèmes informatiques sont sans doute moins importantes que dans des établissements plus grands. Les attaquants sont visiblement très aguerris, à la fois dans le fonctionnement internes des banques (connaissance du métier) et dans les techniques d'attaques informatiques.

- **Form-jacking (et Skimmers logiciels)**

Il s'agit d'une attaque visant les sites web marchands. Si un pirate trouve une vulnérabilité sur un site marchand, il peut y installer un petit code JavaScript invisible qui attend que l'internaute vienne sur la page de paiement du site ; le script vole alors une copie des informations de paiement saisies dans cette page (numéro de carte de paiement, code CVV, etc.). On appelle ces attaques du « Server-side Form-jacking », ou du « Form grabbing » et on parle aussi de « software skimmer ». Ces attaques existent depuis 2015 (le « client-side Form-jacking » existe lui depuis 2007), mais elles ont énormément augmenté en 2018, avec en particulier l'attaque du site de billetterie **TicketMaster** (de février à juin 2018) et l'attaque de **British Airways** (380 000 données de cartes bancaires volées en 2 semaines en août 2018).

**Conclusion**

Les banques sont depuis toujours des cibles de choix pour les cybercriminels. Mais ces dernières années de nouveaux types d'attaques sont apparus. La première réponse qui vient à l'esprit pour empêcher ces attaques est de renforcer la sécurité des installations :

- Les PCs qui pilotent les distributeurs automatiques semblent insuffisamment protégés (protection contre le branchement des périphériques externes, renforcement de la sécurité des OS utilisés ou de la robustesse des logiciels de protection déjà installés sur ces PCs).
- Les banques attaquées par des APT semblent avoir un niveau de sécurité informatique (et de surveillance) limité et trop faible par rapport aux normes recommandées.
- Les sites web devraient isoler plus strictement les formulaires de paiement de l'ensemble du code du site (et du code externalisé) pour ainsi éviter l'ajout du skimmer, invisible dans la masse du code du site.

On peut aussi noter que les attaquants sont plus aguerris. Une certaine connaissance des métiers et des systèmes informatiques des banques est nécessaire pour réaliser les 2 premières attaques. Certaines attaques peuvent sans doute être réalisées par des équipes très réduites (un développeur et un pen-testeur), mais il est probable qu'elles incluent aussi des spécialistes ayant travaillé dans le domaine bancaire. On dit souvent que la menace interne est la plus dangereuse (par le préjudice en cas d'attaque), mais la connaissance métier croissante des attaquants change également la donne.

## 3.5. Les Etats sont devenus un des acteurs les plus visibles dans le paysage de la menace

La Cyber-Défense (au sens large de la défense des intérêts d'un Etat) est omniprésente dans l'actualité. Les medias grand-public abordent souvent ce sujet lorsqu'un groupe agissant pour le compte d'un Etat attaque une entreprise ou un autre Etat (attaques chinoises contre un secteur industriel, attaques russes visant à influencer une élection, etc.). C'est donc dans un premier temps l'aspect offensif qui prédomine. Cependant les Etats travaillent aussi au niveau du renforcement de leurs défenses : par des actions de fond (par exemple les obligations vis-à-vis des OIV français et la directive NIS européenne), mais aussi par

des opérations de communication : il faut faire savoir à l'ennemi qu'il va être détecté et que l'on sait riposter.

Sur cette thématique, **en 2018 les Etats-Unis ont annoncé de façon déterminée les pays qui les attaquent (politique du « Name to Shame »),** en nommant :

- La **Corée du Nord** (première nation citée par les Etats-Unis), qu'ils désignent sous le nom de code Hidden Cobra. Selon eux, la Corée du Nord est passée en 2017 du statut de « puissance mineure » sur le plan cyber (avec par exemple l'attaque de Sony Picture Entertainment en 2014) à celui d'acteur majeur (auteur supposé de Wannacry). En 2017 et 2018, la Corée du Nord a été accusée principalement d'attaques financières.
- Puis la **Russie**, désignée sous le nom de code Grizzly Steppe. La Russie a été l'acteur le plus souvent nommé en 2018 par les Etats-Unis avec en particulier des attaques visant les infrastructures réseaux (alerte TA18-106A sur Cisco Smart Install – SMI) et les attaques visant les entreprises américaines de l'énergie (alerte TA18-074A).
- Et plus récemment la **Chine** (voir cette page web de l'US-CERT). La Chine avait été beaucoup mise en cause en 2010 pour des attaques de cyber-espionnage visant les entreprises, mais avait quasiment disparu du paysage fin 2015 au moment de la mise en place d'un accord de non-agression entre la Chine et les Etats-Unis. La Chine fait donc en 2018 un retour dans l'actualité avec des attaques ciblant les fournisseurs : voir l'alerte TA18-276B sur les attaques au travers de l'infrastructure d'infogérance.

**En termes d'attaques, les 2 événements les plus importants en 2018 sont :**

- **VPNFilter** : attaque russe infectant des réseaux mal protégés, pour en faire des agents dormants que l'on peut réutiliser ultérieurement dans le cadre d'autres attaques.
- **TRITON** : l'attaque industrielle la plus préoccupante depuis Stuxnet. Il s'agit d'une attaque ratée, qui visait les systèmes de sûreté Schneider Triconex d'une installation industrielle en Arabie Saoudite. Si l'attaque avait réussie elle aurait sans doute causé une catastrophe industrielle. L'attaque TRITON (aussi appelée Trisis ou Hatman) a été rendue publique fin 2017, mais les détails et la portée de l'incident n'ont été connus qu'au cours de 2018 (cf. la section « Mars 2018 » au chapitre 2).

## 3.6. Les attaques via les fournisseurs ou les partenaires

L'attaque via les fournisseurs (« supply-chain cyber attack ») est un sujet qui inquiète depuis plusieurs années. Il peut prendre 3 formes distinctes :

- Les attaques par rebond via des partenaires
- Le piégeage de logiciels tiers
- Le piégeage du matériel

• **Les attaques par rebond via des partenaires**

Dans le monde industriel, le premier cas publiquement connu est celui de la cyber-attaque ayant touché RSA Security en 2011 (pour attaquer des industriels de la défense américaine). Aujourd'hui, les attaques de sites industriels débutent très souvent par l'envoi d'emails piégés (attaque de type spear-phishing) **provenant d'un partenaire connu par la victime**. Ce partenaire (un fournisseur par exemple) a en fait été lui-même attaqué et c'est depuis un poste infecté de celui-ci que le mail est envoyé par les attaquants. En 2018, le webinaire du NCCIC (organisme américain intégrant l'US-CERT et l'ICS-CERT) sur les **attaques Russes contre des infrastructures industrielles américaines en 2017** (attaques baptisées **Dragonfly** par

Symantec) présente ces attaques par rebond : le NCCIC appelle les victimes intermédiaires les « staging targets », par opposition aux « intended targets » qui sont les cibles finales visées (voir cet article de l'ARC advisory group).

- **Le piégeage de logiciels tiers**

Ce type d'attaques a été particulièrement médiatisé en 2017 (voir par exemple le chapitre 3.2 de notre bilan annuel de l'an dernier) avec les attaques ayant utilisé des versions piégées des logiciels MeDoc (attaque NotPetya), NetSarang et CCleaner. En 2018, nous avons eu avec l'attaque MageCart sur le site TicketMaster un autre exemple de piégeage d'un logiciel tiers. Cette fois le malware a été introduit dans le code du service de chat-bot vendu par la société Inbenta et utilisé sur le site web de TicketMaster.

- **Le piégeage du matériel**

Cette dernière catégorie est différente des deux précédentes car elle préoccupe avant tout les Etats, plutôt que les entreprises. Il s'agit de la possibilité que certains matériels soient piégés lors de leur fabrication de façon à pouvoir espionner leurs futurs utilisateurs. Ce risque existe depuis toujours pour des attaques ponctuelles par des services d'espionnage. Par contre ces dernières années, les gouvernements ont des craintes que ces attaques puissent être réalisées à grande échelle, en particulier par la Chine puisque cette dernière est l'usine du monde pour les technologies informatiques. On a beaucoup parlé de ces sujets en 2018, avec en particulier :

- Les craintes aux Etats Unis et en Europe à propos des constructeurs Huawei et ZTE (cf. le projet de loi des Etats-Unis pour les interdire dans leurs administrations), qui se focalise désormais sur la technologie 5G,
- Du possible piégeage des cartes mères SuperMicro démenti depuis (voir la section « Octobre 2018 » au chapitre 2).

On peut également inclure dans cette catégorie, la mise à l'index de l'antivirus de Kaspersky (en septembre 2017 par les USA, puis en juin 2018 par le parlement Européen).

## 3.7. Les TTPs des attaquants évoluent et l'attribution devient encore plus difficile

- **Les faux indices pour tromper l'adversaire**

Une fois qu'une attaque est découverte, un des buts de l'équipe de réponse sur incident est d'identifier qui sont les attaquants. En 2010, on se contentait parfois de l'adresse IP (localisation géographique de la machine attaquante) ou la langue et de la disposition du clavier pour attribuer un malware à un pays. Plus récemment, on cherchait les similitudes entre les codes binaires des malwares (recherche de sections de codes identiques). Mais **l'attaque « Olympic Destroyer »** (pendant les jeux Olympiques d'hiver 2018 en Corée du Sud) marque la fin de ces approches. Cette attaque est considérée comme **l'exemple le plus avancé où des « faux indices »** (voir cet article de Kaspersky) ont été insérés dans le code d'attaque pour tromper les enquêteurs sur l'origine réelle des attaquants. On a d'abord soupçonné la Chine (avec des indices plutôt faibles), puis le Corée du Nord (avec des indices qui se sont révélés par la suite être des leurres) et finalement la Russie. Comme l'attaque a été beaucoup moins destructrice qu'elle n'aurait pu l'être, certaines personnes pensent qu'il s'agit en réalité d'une démonstration visant à prouver aux services secrets du monde entier que l'attaquant était capable de frapper fort et de faire accuser un autre pays.

- **Rester invisible grâce à l'utilisation d'outils standards**

Les attaquants préfèrent désormais utiliser lors des attaques des outils standards déjà disponibles plutôt que des binaires développés spécifiquement (malwares). Il s'agit d'une part d'outils standards

d'administration (comme Power-Shell sur Windows) ou d'outils utilisés par tous les attaquants (quelle que soit leur nationalité). Cette approche a deux intérêts pour l'attaquant :

- Il est difficile de détecter les attaques si les outils utilisés sont aussi utilisés pour les tâches légitimes d'administration des plates-formes.
- Il est difficile d'attribuer l'attaque à un groupe particulier si tous les groupes d'attaquants utilisent les mêmes outils.

Nota : Ces attaques qui n'utilisent pas de binaires spécifiques sont souvent appelées « fileless attack » (voir sur ce sujet le chapitre 3.4 de notre bilan de l'an dernier). En 2018, Symantec a inventé le terme **« Live off the land »** (vivre de la terre) pour désigner cette tactique.

• **Modéliser les tactiques des attaquants au moyen du modèle ATT&CK**

En 2018, le projet ATT&CK par MITRE a gagné en visibilité et est devenu la référence pour modéliser les attaquants. ATT&CK est un catalogue qui répertorie les attaquants connus et leurs techniques d'attaques. Ce modèle offre deux perspectives intéressantes :

- il devient théoriquement possible de reconnaitre un attaquant par les techniques qu'il utilise, et non plus uniquement par des marqueurs (IOC),
- cela permet aux entreprises de travailler prioritairement sur les techniques d'attaques les plus utilisées.

## 3.8. Une année de Crypto-mineur mania

En 2017, le cours des crypto-monnaies (tel que le Bitcoin) a explosé, entrainant ainsi l'explosion d'attaques appelées « crypto-jackings ». Ces attaques consistent à installer sur une machine (à l'insu de son propriétaire), un logiciel de crypto-minage qui fonctionne en tâche de fond et qui génère de la crypto-monnaie au profit de l'attaquant. C'est donc un détournement des tâches effectuées par les processeurs (d'où le terme de « crypto-hijacking »).

La crypto-monnaie la plus utilisée pour ces attaques (et plus généralement pour toutes les activités illégales) est le Monero (dont le symbole est XMR) car cette monnaie est difficilement traçable et relativement facile à miner. Si le crypto-jacking Monero existe depuis la création du Monero en 2014, son usage a explosé à la mi-2017, au moment où le cours de toutes les crypto-monnaies a augmenté de façon vertigineuse. Une baisse significative du cours s'est produit fin 2017, mais le nombre d'infections par crypto-jacking est resté très fort tout au long de 2018. En nombre d'incidents, le crypto-jacking est passé en fin 2017 et en 2018 devant les incidents de crypto-ransomware (qui avaient été les types d'infections les plus courants en 2015 et surtout 2016). Il semble cependant que ce phénomène soit désormais en baisse en ce début 2019.

Le crypto-jacking est un marché très attractif pour les cyber-escrocs (du fait de la flambée du cours des crypto-monnaies) mais le marché n'est apparemment lucratif que pour les gros acteurs. Une étude universitaire récente estime que :

- l'ensemble des campagnes de crypto-jacking étudiées représente 4,32 % de tout le marché du Monero,
- ces 4,32 % ont généré en tout 57 millions d'USD,
- **99% des campagnes ont généré moins de 100 XMR** (= $4500) chacune alors que la meilleure campagne a généré à elle seule 18 millions de dollars en 2,5 ans (et les 10 meilleures ont généré un total cumulé de 34 millions de dollars).

# 4. Points de vigilance

Dans ce paragraphe, nous mettons en avant des menaces qui ne sont pas vraiment nouvelles mais qui pour autant continuent à être très présentes. Il s'agit donc d'un rappel à la vigilance, pour ne pas oublier ces problèmes récurrents qui nécessitent une attention particulière.

## 4.1. Les arnaques aux présidents (et au RGPD)

Nous parlons de ces attaques depuis 2014 (voir le chapitre 2.4 de notre bilan 2014, ou 2.8 du bilan 2016) mais ces attaques restent très présentes. Par exemple, en mars 2018 les cinémas Pathé se sont fait escroquer 19 millions d'euros parce que des attaquants se faisant passer pour la direction du groupe ont demandé à la filiale Pathé au Pays-Bas de réaliser des virements pour une prétendue acquisition à Dubaï.

Nota : ces arnaques sont aussi appelées escroqueries aux Faux Ordres de Virement International (FOVI) ou « Business E-mail Compromise scam » (BEC scam) aux Etats Unis. Le FBI a recensé de 2013 à 2018 plus de 40 000 victimes aux Etats-Unis avec une perte totale de de près de 3 milliards de dollars.

A une échelle de coûts plus modeste, on peut noter cette année l'apparition des **arnaques au RGPD** : des sociétés envoient de fausses mises en demeure à des PME/PMI pour les obliger à faire appel à leurs services pour une mise en conformité RGPD (la CNIL a publié un avertissement sur ce sujet).

## 4.2. Accès distants et authentification 2FA

L'authentification au moyen d'un simple mot de passe est aujourd'hui une mesure de sécurité obsolète pour un service accessible depuis Internet. En effet, on ne compte plus les cas de fuites de données (vol de la liste des comptes d'un site web) ou de vol de mot de passe par phishing.

L'utilisation d'une authentification forte, par exemple 2FA (2-Factors Authentication), est donc indispensable lorsqu'on accède à des services externalisés dans le Cloud, comme par exemple une messagerie Office 365 ou même un service extranet comme un simple webmail.

Nota : Tous les mécanismes 2FA ne se valent pas. Le 2FA sms (réception d'un code par SMS) et les 2FA à base d'OTP (comme les Apps Google Authenticator, Authy, ou Microsoft Authenticator) ne sont plus considérés comme sûrs. Pour les systèmes grands publics, à ce jour, seuls le 2FA FIDO (U2F ou FIDO2) est considéré comme sûr.

## 4.3. La sécurité du Cloud

Il ne fait plus de doute aujourd'hui que le Cloud est un élément incontournable des infrastructures IT des entreprises. Si les esprits sont convaincus, la mise en œuvre est parfois beaucoup plus périlleuse. On observe en effet de plus en plus d'incidents de sécurité impactant des environnements Cloud :

- Fuites de données Amazon AWS S3,
- Compromission d'infrastructures mail Microsoft Office 365,
- Attaques via des informations récoltées sur GitHub,
- Installation de crypto-miners illégaux dans des infrastructures Docker,
- Etc.

Les fournisseurs de solutions Cloud sont conscients de cette situation et depuis 2017 ont largement renforcé leurs offres pour implémenter et superviser la sécurité. Il est assez probable d'ailleurs que **les incidents de sécurité constatés viennent le plus souvent de projets déployés trop vite** qui n'ont pas pris le temps d'analyser la sécurité de la solution Cloud qu'ils déployaient. Il ne faut pas oublier que le fournisseur Cloud n'assure la sécurité que sur les couches de son domaine de responsabilité. **Pour les couches plus hautes, la sécurité reste sous la responsabilité du projet** et c'est sans doute là où se trouvent les défauts de sécurité qui ont rendus possible les incidents constatés. Ainsi, pour le Cloud, le mot d'ordre doit être : « Attention aux solutions déployées trop vite et sans sécurité ! ».

# 5. Productions du Cert-IST en 2018

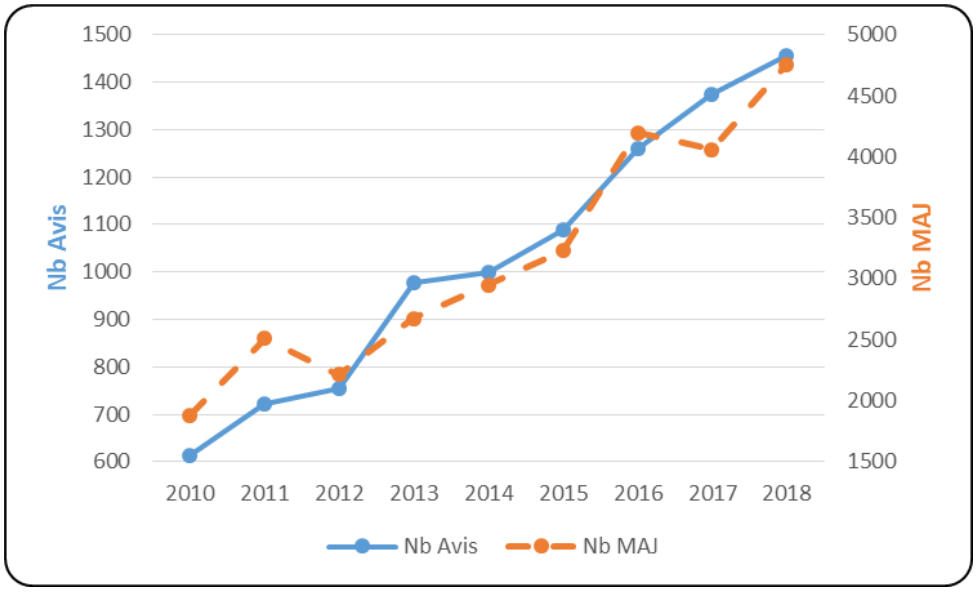
## 5.1. Veille sur les vulnérabilités et les menaces

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.

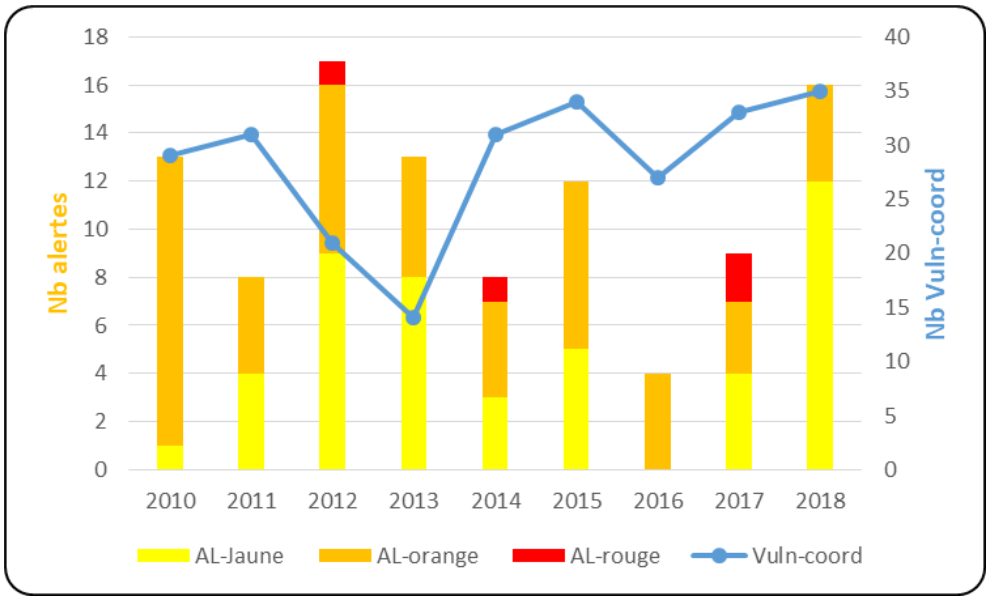
Le Cert-IST émet ainsi plusieurs types de publications :

- **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 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 une analyse 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 leur probabilité d'être utilisées dans des attaques).
- 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).

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

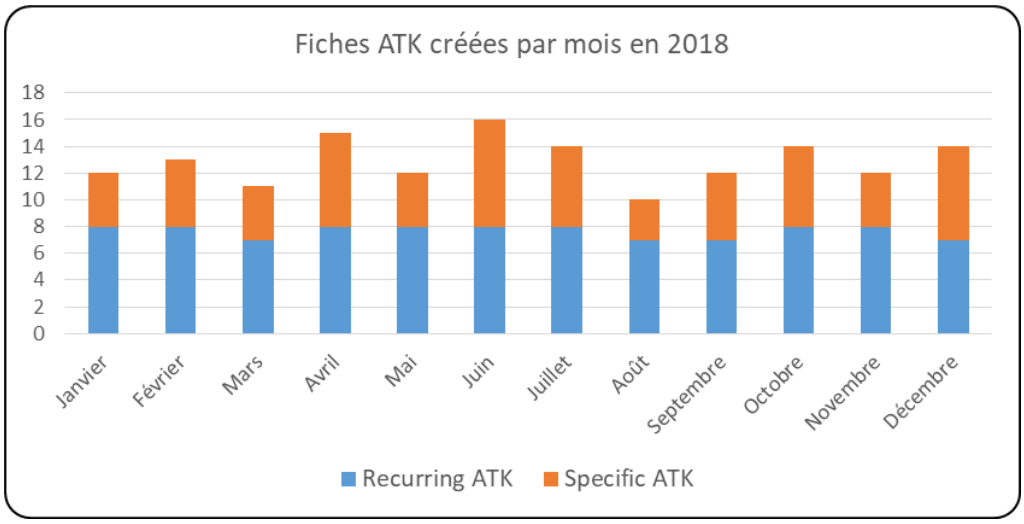



Nombre d'avis de sécurité publiés par an




Nombre d'alertes publiées par an

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




Nombre de fiches attaques publiées par mois

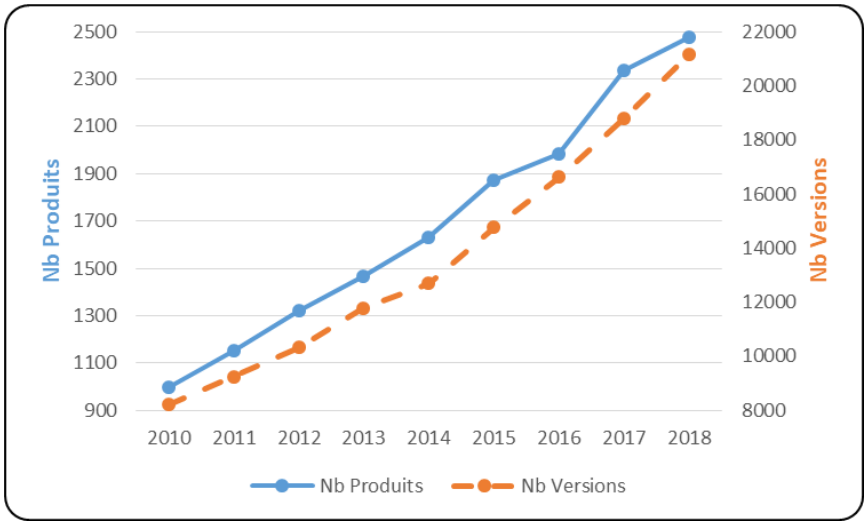
Nota : le service ATK (et IOC) est disponible depuis juillet 2016

Ainsi, en 2018, le Cert-IST a publié :

- **1 456** avis de sécurité (dont **73** avis SCADA), **4 613** mises à jour mineures et **141** mises à jour majeures.
  Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec une augmentation de **6%** par rapport à 2017. Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène en constante croissance. 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.

- **16** alertes et **35** messages "Vuln-coord". Les dernières alertes rouges ont été émises en 2017 (Wannacry et NotPetya). Globalement l'activité dans cette catégorie a augmenté de façon importante, pour revenir à des maxima comparables à 2012 (année des attaques Java).
- **155** fiches attaques ont été publiées en 2018, avec dans la base de données MISP **1 929** évènements qui ont été enrichis, et **173 720** marqueurs (IOC) utilisables.

Concernant les produits et les versions suivis par le Cert-IST, fin 2018 le Cert-IST suivait **2 476** produits et **21 138** versions de produits. 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 (revue de presse)** 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'actualités 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

• **La menace cyber est toujours dans une phase croissante**

Cette année encore, on constate une augmentation des cyber-attaques :

- **en nombre.** Chaque mois de nouveaux cas de vols de données, de plus en plus volumineux, sont annoncés. Chaque semaine, des nouveaux rapports décrivant des attaques ciblées (cyber-espionnage d'état, vol de données industrielles ou action malveillantes de cyber-gangs) sont publiés.
- **en sophistication**, avec par exemple les attaques visant le domaine bancaire (cf. chapitre 3.4), les attaques étatiques contre les équipements réseaux mal protégés (cf. VPN-Filter au chapitre 3.5), ou les attaques via les fournisseurs et partenaires (cf. chapitre 3.6).

• **Les Etats occupent une place de plus en plus importante dans le paysage de la menace**

Les cyber-attaques sponsorisées par des Etats ont commencé à être médiatisées en 2013. Depuis, ce phénomène a pris de l'ampleur et les attaques russes, chinoises ou nord-coréennes font désormais couramment la une de l'actualité. 2018 poursuit cette trajectoire montante. Après la Corée du Nord en 2017, les Etats-Unis ont cette année plusieurs fois nommé la Russie comme responsable d'attaques visant leurs infrastructures.

Si les Etats occupent le premier plan de l'actualité, les cyber-gangs sont eux aussi toujours là. Mais il est vital pour eux de rester discrets pour ne pas attirer l'attention sur leurs activités. Ici, de gros acteurs très organisés côtoient sur le terrain une forêt de petits malfrats. Par exemple, dans le domaine du crypto-jacking et des crypto-mineurs (un des phénomènes de 2018) les gros acteurs accumulent des sommes considérables en crypto-monnaies alors qu'une foule de petits acteurs semblent avoir des gains très modestes (cf. chapitre 3.8).

• **Le renforcement des défenses demeure donc une nécessité**

Face à ce paysage de la cyber-menace, il est important pour les entreprises de maintenir des défenses fortes. Au-delà des mesures techniques (hygiène de la sécurité, défense en profondeur), c'est aussi le point de vue d'analyse qui doit évoluer. Par exemple, il faut penser dès la conception d'un système aux questions telles que :

- Que se passera-t-il lorsqu'une intrusion réussira ?
- Comment peut-on limiter la propagation de cet incident ?
- Quel sera l'impact de la fuite de données ?

On rejoint ici certaines des préoccupations du RGPD (cartographie des systèmes). Il est clair que l'entrée en vigueur du RGPD est un événement majeur de 2018. Après des préoccupations techniques (axe moteur de la sécurité dans les années 2000), puis l'arrivée des approches de conformité (ISO 27000), le RGPD montre que la sécurité a désormais besoin d'un renforcement du cadre législatif. S'il est encore trop tôt pour en mesurer les effets, on voit clairement que l'initiative européenne du RGPD intéresse les autres pays et qu'elle donnera surement lieu à des initiatives similaires ailleurs dans le monde.

• **Au-delà des défenses il faut développer la capacité de l'entreprise à répondre aux intrusions**

Aucune défense n'étant infaillible, l'entreprise a intérêt à optimiser ses actions en équilibrant défense et réaction. En effet, une fois le socle de défense mis en place il est souvent plus productif de surveiller son environnement et de réagir aux menaces lorsque celles-ci apparaissent, plutôt que de continuer à renforcer le socle.

Cette surveillance implique :

- la **mise en place d'une supervision de sécurité**, avec comme objectif de réduire le « Mean Time To Detect » (c'est-à-dire le temps moyen pour détecter un incident),
- la **capacité à traiter les incidents**, pour stopper rapidement l'intrusion et surtout d'empêcher sa propagation.

On dit souvent qu'en cyber-sécurité l'attaquant a l'avantage sur le défenseur parce qu'il lui suffit d'une seule faille pour réussir son attaque, alors que le défenseur doit se préoccuper de tous les composants du système d'information (toute la surface d'exposition). Seulement, un orateur de la conférence Botconf-2018 a récemment proposé un autre point de vue: dans une attaque par infiltration (APT) **c'est le défenseur qui a l'avantage**, en effet, il lui suffit de trouver une seule trace laissée par l'attaquant (et il est difficile de ne laisser aucune trace) pour se rendre compte de sa présence et se lancer à sa poursuite.

Pour lutter efficacement, il est aussi important de bien connaitre les menaces :

- au moyen d'une veille de sécurité,
- mais aussi en partageant avec les autres entreprises de son secteur, les TTPs (Tactiques, Techniques et Procédures) des attaques que l'on a traitées.

Le Cert-IST est dans ce domaine un partenaire privilégié des entreprises.

Association Cert-IST

3 quai du point du jour
92100 Boulogne-Billancourt
France

info@cert-ist.com

https://www.cert-ist.com

05.34.39.44.88