Cert IST

Industrie Services Tertiaire

Bilan Cert-IST des failles et attaques de 2019

Publié en Février 2020

Table des matières

1. Introduction 3
2. Cela s'est passé en 2019 3
3. Analyse des phénomènes les plus marquants de 2019 8
   3.1. BlueKeep : L'attaque attendue n'est pas (encore) arrivée 8
   3.2. Vagues de ransomwares visant spécifiquement les entreprises et les organismes 10
   3.3. Les attaques cybercriminelles reviennent au premier plan de l'actualité 12
   3.4. Les attaques étatiques restent très présentes 13
   3.5. Avec ATT&CK et Open-CTI l'analyse et la réponse aux attaques gagne en maturité 15
   3.6. Fuites de données : 9 milliards de mots de passe ; et après ? 16
4. Points de vigilance 18
5. Productions du Cert-IST en 2019 20
   5.1. Veille sur les vulnérabilités et les menaces 20
   5.2. Veille technologique 22
6. Conclusions 23

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 2019 (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 cybermenace 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 2019

Le tableau ci-dessous récapitule des événements marquants de 2019, qui se sont distingués soit parce qu'ils ont été fortement médiatisés, soit parce que ce sont des marqueurs de la progression de la menace cyber.

Janvier 2019	**Collection #1, Collection #2, …, Collection #5** : L'année 2019 débute par la publication (gratuite) de 5 lots de plusieurs giga de données contenant des listes de comptes et de mots de passe. Ensuite, de février à avril un autre hacker nommé **Gnosticplayers** mettra en vente sur le Blackmarket près de 1 milliard de comptes récemment volés en piratant plus de 40 sociétés. Nous analysons ce phénomène au paragraphe 3.6
Janvier 2019	**Modlishka** : c'est le nom d'un nouvel outil open-source permettant de réaliser des attaques de phishing contre les systèmes **2FA** (authentification à double facteur).

Janvier 2019	**FaceTime bug** : Les médias révèlent qu'un bug dans l'application FaceTime d'Apple permet d'écouter son correspondant avant qu'il ne décroche. Ce bug fera la Une de l'actualité et sera corrigé par Apple une semaine plus tard. Il a été découvert par hasard par un adolescent de 14 ans, en jouant à Fortnite.
Janvier 2019	**LockerGoga** : Le ransomware LockerGoga attaque ALTRAN. C'est la première victime française d'une longue série qui se produira tout au long de l'année, que l'on désigne sous le terme de « **Big-game hunting** ». Nous analysons ce phénomène au paragraphe 3.2
Février 2019	**Bug 'PrivExchange' dans Microsoft Exchange** : Ce bug permet d'attaquer l'Active Directory en tirant parti des privilèges d'Exchange dans l'AD.
Février 2019	**Docker RunC** : une vulnérabilité critique dans la commande RunC permet à un attaquant qui serait « root » dans un conteneur, de passer « root » sur la plate-forme hôte.
Mars 2019	La NSA publie **GHIDRA**, un outil de reverse-engineering que l'agence américaine utilise en interne. Cet outil est assez populaire et est parfois comparé à l'outil commercial (beaucoup plus avancé) IDA pro.
Mars 2019	**10KBLAZE :** La société Onapsis publie 10KBLAZE, un outil d'attaque visant SAP. Il s'agit d'attaques anciennes exploitant des défauts bien connus de configuration ou d'architecture **SAP**.
Mars 2019	Microsoft lance **Azure Sentinel** : une solution de SIEM fonctionnant dans le Cloud Microsoft (article ZDnet).
Mars 2019	**Norsk Hydro** est attaqué à son tour par le ransomware LockerGoga (comme Altran en janvier), et se distingue par sa communication très active.
Mars 2019	**ShadowHammer** : Kaspersky a découvert une attaque visant le logiciel « ASUS Live Update » qui est pré-installé sur les ordinateurs ASUS. L'attaque semble très ciblée puisqu'elle ne se déclenche que sur certains postes très précis (reconnus par leur adresse MAC). Par la suite, Kaspersky a indiqué que cette attaque semblait avoir des liens avec les attaques (chinoises ?) de 2017 visant **CCleaner** et **NetSarang**.
Mars 2019	**WinRAR** : Une vulnérabilité découverte dans WinRAR est immédiatement utilisée, à l'occasion du sommet de Hanoï entre la Corée du Nord et les Etats-Unis, sans doute pour réaliser des attaques de cyber-espionnage. Elle sera très utilisée tout au long de l'année dans d'autres attaques.
Avril 2019	**Dragonblood** est le nom donné à une série de vulnérabilités dans le très récent protocole WIFI **WPA3**. Ce nom fait référence au protocole cryptographique Dragonfly. En Septembre, les mêmes chercheurs publieront 2 vulnérabilités supplémentaires.
Avril 2019	**Julien Assange** est arrêté par la police britannique à la porte de l'ambassade de l'Equateur à Londres où il s'était réfugié en 2012.
Avril 2019	**WIPRO** : Cette société indienne d'infogérance est touchée par une attaque cybercriminelle qui viserait en fait les clients de WIPRO. Nous analysons ce phénomène des attaques par rebond au paragraphe 3.3.

Avril 2019	**Tchap** : Le gouvernement français lance « Tchap », une messagerie chiffrée pour les agents de l'état français. Une vulnérabilité (vite corrigée) est trouvée quelques heures plus tard, et un programme de bug bounty sera lancé ensuite.
Avril 2019	**Sea Turtle** : Cisco TALOS annonce une attaque de cyber-espionnage à base de détournement DNS. Elle est similaire à DNSpionage, mais beaucoup plus sophistiquée. Nous parlons de cette attaque au paragraphe 3.4.
Mai 2019	**Plusieurs médias rapportent qu'Israël a bombardé un immeuble abritant des hackers** Palestiniens. Ce serait le premier cas public de contre-attaque physique (violente) à une attaque cyber.
Mai 2019	0-day **WhatsApp CVE-2019-3568** : WhatsApp annonce avoir corrigé une vulnérabilité qui permettait de faire exécuter du code à distance sur un téléphone Android ou iPhone grâce à un simple appel WhatsApp (même si celui-ci n'est pas décroché). Cette vulnérabilité a été découverte et utilisée par la société NSO Group qui vend des logiciels d'espionnage à des organismes gouvernementaux. Nous parlons de ces attaques visant les téléphones mobiles au paragraphe 3.4.
Mai 2019	**ZombieLoad, RIDL et Fallout :** Ces vulnérabilités des CPU Intel sont similaires à Meltdown et sont baptisées collectivement « Microarchitectural Data Sampling (MDS) vulnerabilities ». En septembre 2019 d'autres attaques visant Intel seront publiées : SWAPGS et NetCAT. Puis **ZombieLoad2** (en novembre) et enfin **PlunderVolt** (en décembre)
Mai 2019	**BlueKeep** : Microsoft annonce avoir corrigé une vulnérabilité dans le service RDP de Windows, qui pourrait donner lieu à des attaques aussi graves que Wannacry (2017). Nous parlons en détail de cette vulnérabilité au paragraphe 3.1.
Juin 2019	**GandCrab shutdown ? :** Les auteurs de ce ransomware annoncent qu'ils arrêtent leurs activités. Un mois plus tard apparait **REvil** (Sodinokibi) qui semble être le remplaçant de GandCrab.
Juin 2019	**RAMBleed** : Cette nouvelle vulnérabilité matérielle utilise la vulnérabilité RowHammer (2015) pour lire des espaces mémoires normalement inaccessibles. RowHammer était une attaque en intégrité (changement accidentel d'un bit mémoire) alors que RAMBleed est une attaque de la confidentialité (fuite mémoire).
Juin 2019	**Have I Been Powned** est à vendre. Troy Hunt, le créateur de cette base de données qui recense les comptes apparaissant dans des listes de comptes volés, annonce qu'il souhaite que ce projet soit repris par un tiers.
Juin 2019	**SIM swapping** : Une série d'attaques de type "SIM swap" frappe à nouveau des utilisateurs pour voler leur portefeuille de crypto-monnaie. Nous avons déjà parlé de ce type d'attaques en 2018. Elles visent aussi les comptes bancaires classiques. Tout début 2020, plusieurs articles (1, 2, 3) seront publiés pour expliquer comment les pirates rentrent chez les opérateurs Télécom pour réaliser ces attaques.
Juin 2019	La Chine aurait réalisé des attaques **DDOS contre Telegram** pour empêcher son utilisation par les protestataires à Hong Kong

Juin 2019	Linux **TCP SACK Panic** : Cette vulnérabilité CVE-2019-11477 dans la fonction SACK (Selective Acknowledgement) permet de provoquer à distance l'arrêt brutal (erreur « kernel panic ») d'un système Linux vulnérable.
Juin 2019	Selon les médias, les USA lancent des **cyber-attaques contre les systèmes de missiles iraniens**. Ces attaques sont présentées comme des représailles contre les tentatives de cyber-attaques iraniennes des infrastructures critiques américaines, et surviennent une semaine après la destruction d'un drone américain par les iraniens.
Juin 2019	**Cloud Hopper** : cette attaque chinoise révélée en 2017 par PwC UK et BAE System puis par l'US-CERT (**TA17-117A**) continue de faire parler d'elle en 2019. Reuter annonce qu'en plus de HP et IBM, d'autres infogérants ont aussi été compromis : Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, Computer Sciences Corporation. En décembre 2019 Le Wall Street Journal publie également un article (repris par FoxBusiness) qui étend encore la liste des victimes.
Juillet 2019	La société **Capital One** annonce une fuite de données impactant 100 millions de citoyens américains et 6 millions au Canada. L'enquête montrera ensuite que l'attaque a été réalisée par une ancienne employée d'Amazon qui a dérobé également les données de 30 autres sociétés.
Juillet 2019	**URGENT/11** : La société Armis annonce avoir découvert 11 vulnérabilités critiques dans le système d'exploitation temps réel (RTOS) **VxWork** de WindRiver. Début octobre, Armis indique que d'autres RTOS sont touchés (en particulier des équipements médicaux) car ils partagent une souche logicielle commune avec VxWork.
Août 2019	**Vulnérabilités des VPN SSL Fortinet, PulseSecure et Palo Alto Network** : 2 chercheurs de la société DevCore présentent à la conférence BlackHat USA 2019, leur étude sur les VPN SSL. Des attaques visant **PulseSecure** débuteront quelques semaines plus tard et deviendront une des attaques les plus actives de l'année 2019. Nous évoquons ce phénomène au paragraphe 3.1.
Août 2019	**Retadup** takedown : Le C3N de la Gendarmerie Nationale française annonce avoir démantelé le botnet Retadup et désinfecté 850 000 ordinateurs dans le monde. A notre connaissance, c'est la première fois qu'une action de ce type est réalisée en France.
Août 2019	**WS-Discovery amplification** (WSD) : Une nouvelle méthode d'attaque DDOS par amplification (découverte en mai) commence à être vue dans des attaques réelles, avec des pics de trafic de l'ordre de 35 Gbps.
Septembre 2019	**SimJacker attack** : La société AdaptiveMobile Security explique une attaque déjà connue des initiés, qui utilise des SMS spécifiques pour activer à distance des fonctions exécutées par la SIM des téléphones mobiles via les fonctions S@T-Browser ou WIB-Browser de certaines SIM.
Septembre 2019	Nouvelle tentative d'attaques contre **CCleaner** : Avast annonce avoir stoppé une attaque qui visait à insérer une backdoor dans le logiciel CCleaner. Ce logiciel avait déjà subi une attaque du même type (supposée chinoise) en 2017.

Septembre 2019	**Emotet** revient en force : Après presque 4 mois sans activité, de nouvelles campagnes de Spam malveillants propagent le malware Emotet.
Octobre 2019	**Adwind RAT** est utilisé dans des attaques visant le secteur du pétrole aux Etats-Unis. Ce RAT (Remote Access Tool) connu depuis 2013 continue à être très souvent identifié dans des attaques visant les particuliers ou les entreprises.
Octobre 2019	**M6 télévision** est touchée par une attaque du ransomware BitPaymer. Ce sera une des innombrables victimes de ces attaques qui ont visé entreprises et organisations en 2019 (cf. notre chapitre 3.2).
Novembre 2019	**DoH : DNS over HTTPS** : Microsoft annonce qu'il supportera DoH dans une version future de Windows 10. DoH permet de garantir la confidentialité et l'intégrité des requêtes DNS, mais pose des problèmes aux FAI et aux produits de sécurités basés sur le trafic DNS. Mozilla Firefox et Google supportent déjà ce protocole, ce qui a valu à Mozilla le prix de « Vilain de l'Internet ».
Décembre 2019	**Fraude au président** : une société d'investissement chinoise se fait voler 1 million de dollars en envoyant son versement à un pirate plutôt qu'à une société israélienne qu'elle voulait soutenir. Dans le domaine de la fraude au président, on peut noter qu'en octobre, des auteurs de telles attaques ont été arrêtés en Espagne.
Décembre 2019	**PlunderVolt** : Cette nouvelle vulnérabilité CVE-2019-11157 impacte les processeurs Intel et permet, en faisant varier le voltage d'un CPU, d'accéder illégalement aux enclaves SGX sur Intel.

3. Analyse des phénomènes les plus marquants de 2019

3.1. BlueKeep : L'attaque attendue n'est pas (encore) arrivée

- **Chronologie de la crise #BlueKeep**

En mai 2019, Microsoft annonce qu'il vient de corriger une faille grave (CVE-2019-0708) qui affecte le service de bureau à distance (RDP) de Windows. Cette faille pourrait donner lieu à des attaques massives comparables à **Wannacry** (en 2017) et Microsoft recommande d'appliquer les correctifs le plus rapidement possible. Cette faille a été surnommée **#BlueKeep** par la communauté cyber.

Nous résumons ci-dessous la chronologie détaillée de cette vulnérabilité, et (heureusement) jusqu'à présent les attaques massives redoutées ne se sont pas produites. Par contre, il est très probable que la vulnérabilité ait été utilisée ponctuellement pour attaquer spécifiquement des machines vulnérables, sans que cela soit réalisé à grande échelle.

Pourquoi n'y a-t-il pas eu encore d'attaque massive ? Un paramètre important pour l'attaquant est de rester discret s'il ne veut pas que son attaque soit détectée, ce qui l'exposerait alors à une possible riposte. Dans le cas de failles très médiatisées, la riposte peut être sévère (par exemple poursuites judiciaires et emprisonnement). Il y a donc toujours une analyse gain/risque à prendre en compte lorsqu'un attaquant décide de lancer une opération.

Chronologie détaillée pour la vulnérabilité #BlueKeep dans Microsoft RDP :

15/05/2019	Microsoft publie les correctifs pour la vulnérabilité CVE-2019-0708 dans le cadre des correctifs mensuels (mardi Microsoft) du mois de mai. Le Cert-IST publie l'avis de sécurité **CERT-IST/AV-2019.0601** pour décrire la vulnérabilité et les correctifs disponibles, puis le lendemain l'alerte jaune **CERT-IST/AL-2019.007**, pour avertir qu'il est très probable que la vulnérabilité soit utilisée pour réaliser des attaques massives.
04/06/2019	Le Cert-IST passe son alerte au niveau Orange car de plus en plus de chercheurs annoncent avoir mis au point un programme d'exploit privé pour cette vulnérabilité. Il est désormais possible qu'une attaque massive se produise même si aucun exploit public n'a encore été diffusé. Microsoft a également publié quelques jours plus tôt un article sur son blog MSRC (Microsoft Security Response Center) qui rappelle qu'il est urgent de patcher les systèmes vulnérables.
13/08/2019	Dans le cadre de ses correctifs mensuels (mardi Microsoft), Microsoft complète les correctifs initiaux car de nouvelles vulnérabilités RDP wormables ont été trouvées par Microsoft (CVE-2019-1181 et CVE-2019-1182). Ces vulnérabilités seront baptisées par certains #DejaBlue.
06/09/2019	Un premier programme d'exploitation public (sur Metasploit) est publié sur Internet. Ses fonctionnalités sont encore limitées, puisque l'attaque ne se déroule correctement que pour certains systèmes Windows.
02/11/2019	Les chercheurs Kevin Beaumont (@GossiTheDog) et Marcus Hutchins (@MalwareTechNews) annoncent avoir découvert une attaque assez étendue qui exploite la vulnérabilité BlueKeep. Le but de l'attaquant est d'installer un logiciel de crypto-minage sur les systèmes vulnérables. Du fait des limitations du programme d'exploit utilisé (basé sur celui de Metasploit), la plupart du temps l'attaque se termine par un reboot de la machine attaquée. Microsoft publiera quelques jours plus tard une analyse de cette attaque.

	Quelques jours plus tard, l'auteur de l'exploit BlueKeep pour Metasploit annonce qu'il a amélioré ce dernier pour éviter les "crash" souvent observés avec la version précédente.
	A ce jour aucune attaque massive n'a été observée. Il est cependant probable que la vulnérabilité soit utilisée ponctuellement (sans propagation automatique de type « ver ») pour attaquer des machines vulnérables.

- **Les autres attaques qui ont marqué 2019**

En plus de #BlueKeep, voici les attaques qui sont pour nous, les plus marquantes de 2019 :

- **VPN SSL Pulse secure (CVE-2019-11510) :** ces attaques contre ce VPN SSL ont débuté le 22/08/2019, quelques semaines après une présentation à la conférence Black Hat USA 2019 de détails techniques sur des vulnérabilités récemment corrigées dans les VPN SSL Pulse Secure (avis CERT-IST/AV-2019.0520 du 24/04/2019) mais aussi Palo Alto Networks GlobalProtect (avis CERT-IST/AV-2019.0903 du 17/07/2019) et Fortinet (avis CERT-IST/AV-2019.0668 du 24/05/2019). Nous avons d'abord émis l'alerte jaune CERT-IST/AL-2019.010, puis nous l'avons élevée au niveau orange le 11/10/2019 lorsque le nombre d'attaques signalées s'est multiplié. **Ces attaques ont été très actives pendant tout le dernier trimestre 2019.** Elles auraient permis par exemple l'attaque par ransomware qui a touché la société de change Travelex fin décembre 2019.

- **Microsoft SharePoint (CVE-2019-0604) :** Cette vulnérabilité permet à un attaquant d'exécuter à distance du code malveillant sur un serveur SharePoint vulnérable. Elle a été corrigée par Microsoft le 12/02/2019 et les premiers cas d'attaques (qui pourraient être des cas de cyber espionnage chinois) ont été observés début mai au Canada et en Arabie Saoudite. Nous avons émis à cette date l'alerte jaune **CERT-IST/AL-2019.006**, que nous avons élevée au niveau orange début juin quand il a été confirmé que cette attaque pouvait être réalisée à distance sans compte SharePoint. **Plusieurs attaques utilisant cette vulnérabilité (potentiellement du cyber-espionnage venant de Chine) ont été vues ensuite**, par exemple celles signalées, par le FBI (voir cet article ZDnet de janvier 2020), ou l'attaque subie par ONU à Genève et Vienne (voir cet article TheRegister.co.uk de janvier 2020).

- **Oracle WebLogic (CVE-2019-2725)**: depuis 2 ans, le serveur web WebLogic (Java) est victime d'attaques sur des fonctions de dé-sérialisation Java, et à chaque fois qu'une vulnérabilité est corrigée par Oracle, une autre fonction vulnérable apparait quelque mois plus tard. Nous avions déjà signalé ce phénomène en 2018 (nous avons publiés 2 alertes Oracle WebLogic en 2018) et le phénomène se poursuit en 2019. Nous avons émis l'alerte **CERT-IST/AL-2019.005** le 29/04/2019. **Ces vulnérabilités sont très souvent utilisées pour installer des logiciels de crypto-minage sur les serveurs vulnérables**.

- **L'évolution des attaques de crypto-minage**

Nous mentionnions l'an dernier que 2018 avait été une année de la « crypto-mineur mania », c'est-à-dire que les attaques au moyen de logiciels crypto-mineurs avaient connu une croissance exponentielle. Ce phénomène s'est poursuivi en 2019 avec quelques évolutions :

- Les attaques les plus courantes sont désormais d'installer des logiciels de crypto-minage sur des serveurs vulnérables. Actuellement, dès qu'un programme d'exploitation pour une nouvelle vulnérabilité concernant un serveur est publié, on voit ensuite des vagues d'attaques de crypto-mineurs utilisant cette vulnérabilité. Cela a été le cas par exemple, pour les vulnérabilités **Oracle WebLogic** (CVE-2019-2725 déjà mentionnée ci-dessus), ou **Atlassian Confluence** (CVE-2019-3396, alerte **CERT-IST/AL-2019.003**) ou **Jenkins** (CVE-2018-1000861 de fin 2018, avis **CERT-IST/AV-2018.1362**).
- Il est également assez courant que les pirates installent un logiciel de crypto-minage sur les postes utilisateurs (et grand public) infectés.
- Par contre, le crypto-jacking, qui consistait à installer un code de minage (Javascript) sur des sites web pour que les internautes visitant ce site les exécutent, est un type d'attaque qui a très largement décliné.

3.2. Vagues de ransomwares visant spécifiquement les entreprises et les organismes

Les ransomwares existent depuis longtemps et ont été de 2013 à 2016 une des sources majeures d'attaques. Durant ces années, ils visaient de façon indifférenciée les entreprises et les particuliers. En 2018 est apparu une nouvelle forme d'attaque, où cette fois le ransomware vise spécifiquement une entreprise choisie par l'attaquant. Crowdstrike nomme ce phénomène le « Big-Game Hunting » (la « chasse au gros »). **2019 est l'année où le phénomène du big-game hunting est devenu un phénomène majeur dans le paysage de la cybermenace.**

Au-delà des entreprises, ces attaques visent toutes les organisations que les cybercriminels jugent « profitables », c'est-à-dire susceptibles de payer de grosses rançons. Plusieurs attaques ont visé les hôpitaux (par exemple l'hôpital de Rouen en France), et aux Etats-Unis de nombreuses municipalités.

Liste des sociétés touchées par des attaques sévères de ransomware en 2019 telles qu'elles ont été rapportées par les médias. Liste non exhaustive puisque qu'il s'agit uniquement des cas qui ont été annoncés dans la presse.

24/01/2019 : Altran (IT consulting and services) en France.
12/03/2019 : Hexion et Momentive, 2 sociétés industrielles américaines appartenant au même groupe.
15/03/2019 : Mitsubishi Aerospace au Canada.
19/03/2019 : Norsk Hydro, société industrielle norvégienne de production d'aluminium.
21/03/2019 : Arizona Beverages aux Etats Unis.
11/04/2019 : Fleury-Michon (agro-alimentaire) en France (il n'est pas formellement établi qu'il s'agit d'un ransomware).
16/04/2019 : Aebi Schmidt en Suisse (spécialiste du matériel de déneigement et de nettoyage des routes).
17/04/2019 : Verint (Societé de cyber-sécurité) en Israël. L'attaque semble avoir échouée (elle a été contenue dans une DMZ).

02/06/2019 : Eurofin Scientific (laboratoire de bio-analyses) au Luxembourg.
07/06/2019 : ASCO (fabricant avionique) en Belgique.
10/08/2019 : Ramsay Générale (Groupe hospitalier) 120 établissements français touchés.
03/09/2019 : Demant, entreprise danoise de prothèses auditives.
11/09/2019 : Defence Construction Canada (DCC).
24/09/2019 : Rheinmetall Automotive en Allemagne.
12/10/2019 : M6 télévision en France.
23/10/2019 : Go Sport (magasins de sport) en France.
04/11/2019 : Everis (informatique) et Cadena SER (Radio) en Espagne.
10/11/2019 : Pemex (société pétrolière) au Mexique.
12/11/2019 : Edenred (connu pour sa marque "Ticket Restaurant") en France.
27/11/2019 : Prosegur (sécurité et transport de fonds) en Espagne.
31/12/2019 : Travelex (société de change) au Royaume-Uni

Les incidents d'ampleur provoqués en 2019 par les attaques de big-game hunting ont fait évoluer notablement plusieurs domaines de la réponse à incident :

- **La nécessité de savoir reconstruire le SI**. Ces attaques affectent un grand nombre de postes, qui deviennent indisponibles souvent pendant plusieurs semaines. Outre le fonctionnement dégradé (ou totalement stoppé) ces attaques nécessitent une reconstruction du SI pour un retour en fonctionnement normal. C'est un cas de sinistre qui la plupart du temps n'était pas prévu dans le PRA (Plan de Reprise d'Activité) des entreprises touchées.
- **La communication en cas de crise**. L'habitude est souvent de minimiser la communication publique en cas d'incidents. Mais la société Norsk Hydro a choisi en mars 2019 une attitude opposée qui est considérée désormais comme exemplaire (voir par exemple cet article ZDNet) : elle a communiqué en permanence, dès le début de l'incident et de façon très transparente.
- **Le fait de payer ou non une rançon**. Si le discours général est toujours que payer une rançon à l'attaquant est dangereux (contraire à l'éthique et sans garantie sur le résultat technique), le fait de payer quand même (en dernière extrémité quand aucune autre solution n'est possible) est de plus en plus une position affichée ou en tout cas moins tabou. Néanmoins, tous les experts s'accordent pour dire que c'est la plus mauvaise solution et que son résultat est très incertain.
- **La cyber-assurance est de plus en plus considérée comme une mesure indispensable**, qui permet de couvrir une partie des coûts induits par un incident. Dans certains cas, il semblerait même que des sociétés d'assurances participent aux négociations avec les attaquants pour minimiser le montant de la rançon.

3.3. Les attaques cybercriminelles reviennent au premier plan de l'actualité

Sur le front des attaques, les deux acteurs les plus présents sont les cybercriminels (motivés par le gain d'argent) et les Etats (le cyber étant un des outils pour affirmer sa puissance dans l'échiquier mondial). Les cybercriminels cherchent plutôt la discrétion, pour ne pas attirer l'attention sur leurs activités, alors que les Etats peuvent parfois avoir un intérêt à montrer leur force. En 2018, l'actualité avait été plutôt dominée par des attaques étatiques, et les attaques cybercriminelles étaient restées plutôt discrètes.

Cela a changé en 2019 : les cybercriminels ont été très présents dans l'actualité, en particulier au travers de 3 phénomènes :

- Les **attaques de ransomware** dont nous avons parlé au paragraphe précédent (§ 3.2),
- Les **attaques Magecart** visant des achats en ligne des internautes,
- Les **attaques visant les prestataires informatiques** et leurs clients.

Nous analysons ces 2 derniers phénomènes ci-dessous.

• **Les attaques Magecart visant les achats en ligne des internautes**

Les attaques de type Magecart ont fait une poussée spectaculaire en 2019. Ces attaques consistent à installer un « skimmer web » sur des sites web mal protégés afin de voler les données saisies par les internautes (données des cartes bancaires) lors du règlement de leurs achats. Nous avons déjà parlé de Magecart en 2018 dans un article bulletin à l'occasion des attaques **Ticketmaster** et **British Airways**, dans notre fiche attaque CERT-IST/ATK-2018.084, et dans notre bilan annuel sur les attaques de 2018. En 2019, le phénomène s'est encore amplifié avec de plus en plus d'incidents de ce type. A titre d'exemple, en 2019 Magecart a été cité dans 32 bulletins de veille media Cert-IST (en 2018 il avait été cité 13 fois). Il est clair que de plus en plus de groupes cybercriminels utilisent cette technique.

Nota : Magecart désigne une technique d'attaque qui est utilisée par plusieurs groupes cybercriminels. RiskIQ identifie au moins 8 groupes distincts.

• **Attaques visant les prestataires informatiques et leurs clients**

Plusieurs attaques révélées en 2019 montrent que des cybercriminels cherchent de plus en plus souvent à s'introduire (informatiquement) dans des sociétés d'informatiques, pour ensuite infecter leurs clients grâce aux accès informatique dont ces sociétés disposent chez ces clients.

Ces sociétés d'informatiques peuvent être :

- Des petites structures assurant la maintenance informatique de diverses sociétés,
- Des prestataires spécialisés, par exemple fournisseurs de solutions pour les médecins, les dentistes, etc.
- Des infogérants intervenant dans des sociétés de grandes tailles.

On parle en général pour les désigner de MSP (Managed Services Providers).

Ce type d'incidents est arrivé par exemple en avril 2019 (voir cet article de Brian Krebs) chez **WIPRO** (une société internationale de consulting et d'infogérance informatique dont le siège social est en Inde). Par la suite la société RiskIQ a publié une étude (intitulée Gift-Card Sharks) montrant que WIPRO n'était qu'une des cibles d'une opération plus large visant d'autres entreprises dans plusieurs secteurs

d'activités, et en particulier les sociétés informatiques **Infosys** et **PCM**. Il s'agissait ici de s'introduire dans des sociétés tierces pour voler des cartes cadeaux (d'où le nom de l'étude) et autres coupons pouvant ensuite être monnayés.

De nombreux autres cas d'infections via les prestataires informatiques avaient pour but d'installer un ransomware chez leurs clients. Voir par exemple ce cas en janvier 2019 (ransomware GandCrab) et celui-ci en juin 2019 (ransomware Revil/Sodinokibi).

Ces attaques via des prestataires rappellent les attaques chinoises **Cloud Hopper, révélées au printemps 2017**, qui ont visé des acteurs majeurs du domaine comme **HP** et **IBM** (au Etats-Unis) et **NTT Data** et **Fujitsu** (au Japon). Dans le cas de Cloud Hopper, il s'agirait par contre d'attaques étatiques avec des visées de cyber-espionnage.

L'actualité de 2019 montre donc un phénomène de diffusion de cette tactique d'attaque dans deux directions :

- De plus en plus de cybercriminels utilisent cette tactique.
- Elle a été vue en premier il y a quelques années dans le domaine des attaques de cyber-espionnage, et elle est désormais aussi utilisée par des groupes cybercriminels avec des visées financières.

3.4. Les attaques étatiques restent très présentes

- **Les attaques visant la communauté Ouighour**

Depuis plusieurs années (2009 au moins), les rapports publiés montrent des cas d'attaques visant des minorités ethniques sous surveillance en Chine, essentiellement les Ouïghours et les tibétains. Ces attaques réputées jusque-là plutôt peu sophistiquées, auraient utilisé le plus souvent des malwares connus et visaient les systèmes Windows. Depuis 2018, les techniques d'attaques seraient en voie de professionnalisation avec notamment de plus en plus d'ingénierie sociale ; les attaques s'orientent désormais davantage vers des téléphones mobiles Apple IOS ou Google Android. Par exemple, en septembre 2019 Citizen Lab, Google Project Zero, et Volexity ont publié des articles à propos d'une attaque de ce type baptisée « Poison Carp » (ou « Evil Eye »).

- **Les téléphones mobiles utilisés pour espionner les opposants**

Les attaques visant les téléphones ne se limitent pas aux opposants chinois. Tous les services de renseignements sont probablement intéressés à disposer d'attaques 0-day pour IPhone ou Android, de façon à pouvoir espionner les téléphones d'individus jugés dangereux. Si cela peut se comprendre dans le cadre de la lutte anti-terroriste par exemple, il y a certainement des dérives, en particularité dans des pays totalitaires.

En 2019, on a parlé en particulier du logiciel Exodus développé par la société italienne **eSurv**, et de Pegasus développé par la société israélienne **NSO Group**.

Un autre phénomène notable pour 2019 est que ces attaques, plutôt que de viser le système d'exploitation lui-même (Android ou iOS), se focalisent maintenant aussi sur les applications installées sur ces téléphones, comme **WhatsApp** (attaque 0-day CVE-2019-3568) ou **iMessage** (attaque Karma utilisée par les Emirats Arabes Unis).

- **Attaque Sea Turtle et DNSpionage par détournement DNS**

En janvier 2019, le CISA américain (organisme au-dessus de l'US-CERT), puis l'ICANN, ont publié des alertes suites aux attaques **DNSpionage** révélées par Cisco TALOS en novembre 2018. Et en avril, Cisco TALOS a annoncé une seconde attaque de même type, plus sophistiquée, baptisée **Sea Turtle**.

Dans les deux cas, il s'agit d'attaques de grande envergure, probablement réalisées par des Etats, qui ont permis de voler les codes d'accès (mail ou VPN) des victimes en les orientant vers des faux sites au moment de leur connexion. Ce détournement des connexions aurait été réalisé en changeant des données DNS.

Les attaques DNSpionage semblent venir d'Iran. Sea Turtle est une attaque considérée comme beaucoup plus sophistiquée, et un article très récent indique que l'attaque pourrait être liée à la Turquie.

- **Etats-Unis, Russie, Iran : la partie visible de l'iceberg**

Dans le bilan de l'année dernière, nous expliquions que les Etats-Unis avaient adopté il y a quelques années pour le domaine cyber, la politique du « Name to Shame » (nommer pour faire honte) et citaient trois pays en particulier : la Russie, la Corée du Nord et la Chine. Cette année, on peut y ajouter l'Iran (voir cette alerte AA20-006A publiée tout début 2020), et c'est bien sûr aussi le résultat des fortes tensions actuelles entre ces 2 pays.

L'Iran est connu depuis de nombreuses années pour avoir des capacités importantes en cybersécurité dont des capacités offensives très certainement développées en réponse à l'attaque Stuxnet de 2010 qui le visait; il a été effectivement cité de nombreuses fois dans l'actualité 2019 pour des attaques cyber, par exemple :

- Attaques visant les instituts de recherches utilisant le logiciel de séquençage ADN **dnaLIMS**
- Attaques Outlook par le groupe iranien APT33 (Elfin)
- Attaques d'utilisateurs LinkedIn par le groupe iranien APT34 (OilRig)

On peut noter aussi qu'en 2019 des hackers (utilisant le pseudonyme de « Dookhtegan ») ont publié sur Internet des outils d'attaques qui appartiendraient à des groupes iraniens. Il est difficile de dire s'il s'agit d'une manœuvre de déstabilisation, ou simplement d'un acte isolé d'un hacker. Kaspersky indique qu'il pourrait s'agir d'une action (de déstabilisation) du groupe russe Sofacy (APT28). Ce groupe russe a déjà été cité dans un grand nombre d'attaques, en particulier dans des attaques de déstabilisation (par exemple : attaques contre le parti Démocrate lors des élections américaines de 2016, attaque Macron-leak en 2017).

La Russie a également été citée de nombreuses fois cette année, et de façon plus inhabituelle, en tant que victimes d'attaques :

- Reuter annonce en juin 2019 que les Etats-Unis (et leurs alliés) auraient compromis la société russe Yandex (l'équivalent russe de Google).
- Le New York Times annonce en juin 2019 que les Etats-Unis auraient mené des attaques contre les réseaux électriques en Russie.
- Un groupe de hacker jusque-là inconnu annonce avoir piraté un sous-traitant du FSB et volé plusieurs Téraoctets de données décrivant des projets réalisés pour le FSB.

3.5. Avec ATT&CK et Open-CTI l'analyse et la réponse aux attaques gagne en maturité

ATT&CK est un projet de l'organisme américain **MITRE** qui est devenu la référence pour modéliser le comportement des attaquants. Il permet de développer une défense centrée sur les comportements d'attaques déjà connues, par exemple en identifiant les mécanismes de défense manquant ou en mesurant les capacités de détection d'un SOC. Démarré en 2013, et rendu public en 2015, ATT&CK est devenu très visible en 2018 (la première conférence dédiée à ce sujet a eu lieu en octobre 2018 : ATT&CKcon). **2019 confirme l'intérêt de la communauté pour ATT&CK**. Ce modèle fédère autour de lui beaucoup d'initiatives, comme par exemple Atomic Red Team (jeux de tests simulant des attaques) ou Atomic Blue Detection (librairie d'Analytics EQL permettant de détecter une attaque).

Toujours dans le domaine de la CTI (Cyber Threat Intelligence), en 2019 l'ANSSI et le CERT-EU ont publié en open-source le projet **OpenCTI**. Cet outil permet de classer et structurer les données dont on dispose sur les attaques, les attaquants, et leurs outils. **OpenCTI** complète donc l'offre existante dans le domaine de la CTI qui inclut à la fois des outils open source comme **MISP** et des outils commerciaux comme par exemple : ThreatQuotient, Anomali, ThreatConnect, …

Enfin, le format **SIGMA** (apparu en 2017) s'impose progressivement comme un standard de référence. SIGMA est un langage permettant de décrire une alerte SIEM dans un format neutre indépendant de l'outil utilisé.

Brève publiée dans le bulletin Cert-IST de juin 2019

Sysmon et Sigma

Sysmon et Sigma sont deux "outils" qui prennent une importance croissante dans le domaine de la journalisation et de la détection d'attaques. Nous les présentons dans ce court article.

Sysmon est un outil de Microsoft qui permet de générer des logs complémentaires sur un poste Windows. Ces logs permettent surtout de tracer finement les processus lancés, et ainsi de détecter les processus dangereux. Sysmon trace également d'autres événements comme la création de fichiers, les connections réseaux, ou très récemment les résolutions DNS. Les logs générés par Sysmon sont envoyés dans le journal d'événements standard de Windows (event log). Il existe de nombreux exemples de comportements anormaux qui peuvent être détectés avec Sysmon (voir par exemple la page Sysmon–DFIR). On peut par exemple détecter :

- L'outil Mimikatz,
- Les scripts Powershell malveillants,
- Les souscriptions WMI suspectes (un moyen de persistance).

Sysmon existe depuis au moins 2014 (article le plus ancien trouvé sur le sujet), mais est devenu populaire en 2017. Il fait partie de la suite des outils SysInternals développée par Mark Russinovich.

Sigma est un langage développé par Florian Roth (@Cyb3rops sur Twitter) qui permet de décrire une règle de détection SIEM. Sigma est donc l'équivalent dans le domaine des logs de ce que YARA est pour la recherche de fichiers. Sigma est livré avec un convertisseur (nommé « sigmac ») qui permet de transformer une règle Sigma en un format approprié pour le système de détection utilisé parmi, par exemple : ArcSight, ElasticSearch/Kibana, Graylog, Grep/PowerShell, LogPoint, Qradar, Qualys, Splunk,

SumoLogic.

Plus de 200 règles de détection open-sources sont proposées sur le site de Sigma.

Dans le même domaine que Sigma, on peut citer enfin le site uncoder.io qui propose aussi de convertir des règles de détection d'un format à un autre. Sigma est utilisé par ce site comme langage pivot pour passer d'un format à l'autre. Ce site permet de voir rapidement des exemples de règles Sigma (via le menu déroulant « Select document »).

Pour plus d'information :

- Sysmon : https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Sysmon – DFIR : https://github.com/MHaggis/sysmon-dfir
- Technet : https://blogs.technet.microsoft.com/motiba/2017/12/07/sysinternals-sysmon-suspicious-activity-guide/
- Sigma : https://github.com/Neo23x0/sigma

3.6. Fuites de données : 9 milliards de mots de passe ; et après ?

Depuis plusieurs années, le nombre d'attaques et le volume des données volées est en constante augmentation. L'année 2019 n'a pas démenti cette tendance, avec même un paroxysme pour ce qui concerne les fuites de mots de passes :

- Dès janvier 2019, des listes contenant des millions de noms de comptes et de mots de passes sont diffusées sur Internet. Elles sont regroupées en lots, baptisés **« Collection #1 », « Collection #2 », … , « Collection #5 ».** Il s'agit pour l'essentiel de vieilles listes qui circulaient déjà depuis longtemps dans l'underground.
- De février à avril 2019, un hacker nommé **Gnosticplayers** va ensuite mettre en vente sur le DarkMarket 5 séries de nouvelles listes contenant au total **932 millions de nouveaux comptes** (voir cet article de ZDnet).

Le site Have I Been Pwned qui récence tous les comptes volés au cours de ces dernières années, indique disposer actuellement d'une base de plus de **9 milliards de comptes**, ce qui montre bien l'ampleur extrême de ce phénomène.

Nota : Have I Been Pwned n'est pas un site malveillant : chacun peut consulter ce site pour savoir si l'un de ses comptes personnels est dans une de ces listes de comptes volés qui circulent sur Internet. En s'inspirant de ce site, d'autres proposent le même service, par exemple Firefox et Chrome.

- **Que deviennent les données volées ?**

On dispose d'assez peu d'informations fiables sur la nature exacte des données volées et leur usage ultérieur.

Les cas les plus médiatisées concernent :

- des données personnelles de type nom, adresse, date de naissance, … Il s'agit le plus souvent d'extraits des bases de données clients des sociétés attaquées et l'on est informé de ces fuites au travers des déclarations officielles des entreprises touchées (du fait des obligations légales de déclaration).
- des adresses mails, des mots de passe, voire des données de cartes bancaires. Ces données ont clairement de la valeur pour les cybercriminels. Elles sont donc revendues sur les Black Markets

Le reste est beaucoup plus obscur. On imagine bien qu'un pirate qui trouve des données lors d'une intrusion va les copier s'il pense qu'elles ont de la valeur et qu'il sait comment les revendre, et les ignorer lorsqu'elles ne veulent rien dire pour lui. Dans ce domaine, les attaques d'Etats sont plus dangereuses et les attaques concurrentielles (qui visent la propriété industrielle) sont critiques.

De manière inquiétante, les attaques cybercriminelles portant sur des informations relatives à la propriété industrielle, sans commanditaire particulier, semblent en augmentation et constituent un nouveau terrain rentable pour les attaquants. En effet, on a vu fin 2019 un premier cas (cf. ce témoignage de BleepingComputer.com à propos de la société **Allied Universal**) où lors d'attaques de ransomware visant une entreprise, l'attaquant a volé des données, puis menacé de les publier si la rançon n'était pas payée. Autre cas inquiétant, en avril 2019, des hackers ont annoncé avoir piraté la société allemande **CITYCOMP** et menacé de publier des données de leurs clients, parmi lesquels on compte Oracle, Airbus, Toshiba et Volkswagen (voir cet article publié par Vice.com). L'affaire n'a pas eu de suite publique et reste assez mystérieuse.

4. Points de vigilance

Dans ce paragraphe, nous mettons en avant des menaces qui ne sont pas nouvelles mais qui constituent toujours des problèmes très présents. Il s'agit donc d'un appel à la vigilance, sur des domaines qui selon nous nécessitent une attention toute particulière.

- **La protection des accès distants et l'authentification 2-facteurs (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 mots 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 : Certaines solutions 2FA ne sont plus considérées comme sures (en particulier le 2FA par SMS) et nous avons consacré un article de notre bulletin mensuel de février 2019 à ce sujet. Il est cependant évident aussi que face à un attaquant ordinaire, il vaut mieux une solution 2FA faible que pas de 2FA du tout !

- **La sécurité du Cloud**

Ce point est bien connu aussi, mais il vaut mieux le rappeler : déployer une solution dans un Cloud sécurisé ne garantit pas sa sécurité. Il y a eu de nombreux incidents où des espaces Cloud ont été piratés (par exemple des espaces de stockage Amazon S3) parce qu'ils avaient été mal sécurisés par le client du service Cloud. Le fournisseur d'un service Cloud n'apporte la sécurité que sur les niveaux qui sont de son domaine de responsabilité : pour les niveaux supérieurs c'est le client qui conçoit l'architecture globale et qui doit analyser la sécurité de son architecture. Attention donc aux solutions Cloud déployées trop vite, sans analyse technique de la sécurité de l'architecture !

- **Les attaques par les fournisseurs et partenaires**

De plus en plus souvent les attaques ne sont plus frontales, mais passent plutôt par des fournisseurs ou des partenaires. Par exemple :

- Une attaque de spear-phishing par mail est tentée en envoyant un mail provenant d'un fournisseur que la victime connait et en qui elle a confiance,
- Une intrusion réseau est lancée depuis un partenaire attaqué dans le but de servir de point de rebond.

Nous avons développé ces aspects dans notre bilan annuel de l'an dernier et le sujet est toujours très présent dans l'actualité 2019, comme nous l'avons vu par exemple dans le cas des attaques passant par les structures des prestataires informatiques (cf. le §3.3), ou l'attaque subie par **Airbus** en 2018 et 2019.
Face à cette menace la réponse nous semble être composée de plusieurs aspects :

- Les interconnexions réseaux avec les partenaires et les fournisseurs doivent être filtrées et surveillées,
- Il faut admettre le fait qu'un poste utilisateur sera sans doute un jour compromis, par exemple par une attaque mail réussie. Dans ce cas, il faut pouvoir détecter cette attaque et stopper sa

progression le plus rapidement possible avant qu'elle ne permette à l'attaquant d'accéder à des points plus sensibles du système d'information.

- **Le piégeage de logiciels (ou même de matériel)**

Il y a de plus en plus d'exemples d'attaques où un logiciel a été modifié à l'insu de son propriétaire dans le but de servir de porte dérobée une fois que ce logiciel sera installé et utilisé par la victime visée. Jusqu'à présent, ces attaques ont plutôt été des cas d'intrusions sophistiquées comme des attaques réalisées par des Etats (attaques CCleaner et NetSarang de 2017 ou ShadowHammer en 2019).

La plupart des entreprises n'ont probablement pas les moyens de mettre en place des mesures de protection amont efficaces contre ce type d'attaques. Tout comme dans le cas de l'attaque du poste de travail mentionné ci-dessus, il nous semble que l'effort devrait être porté ici aussi sur la capacité de détecter une attaque *a posteriori* et de limiter sa progression au sein de l'entreprise.

5. Productions du Cert-IST en 2019

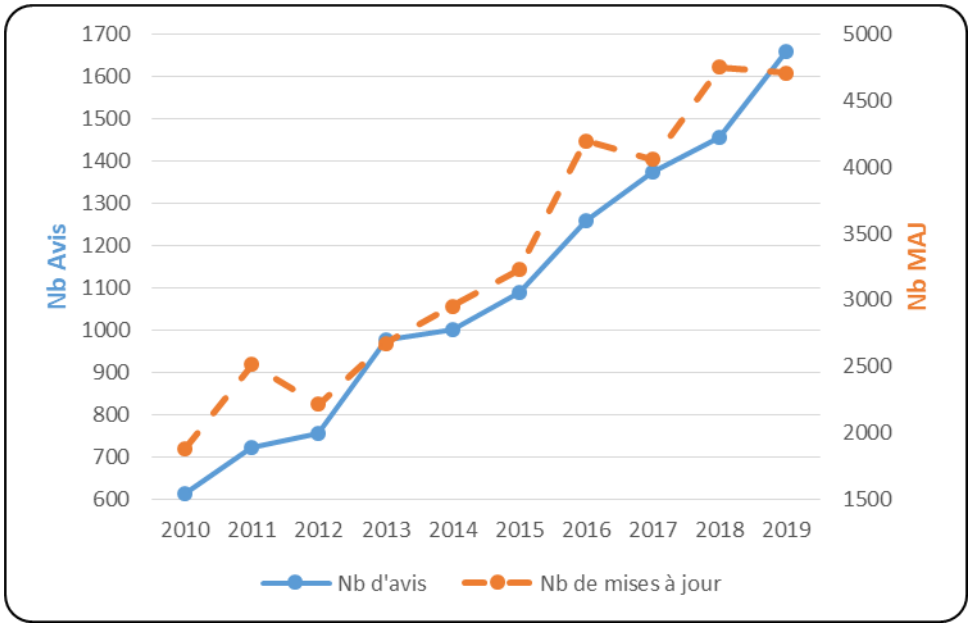
5.1. Veille sur les vulnérabilités et les menaces

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.

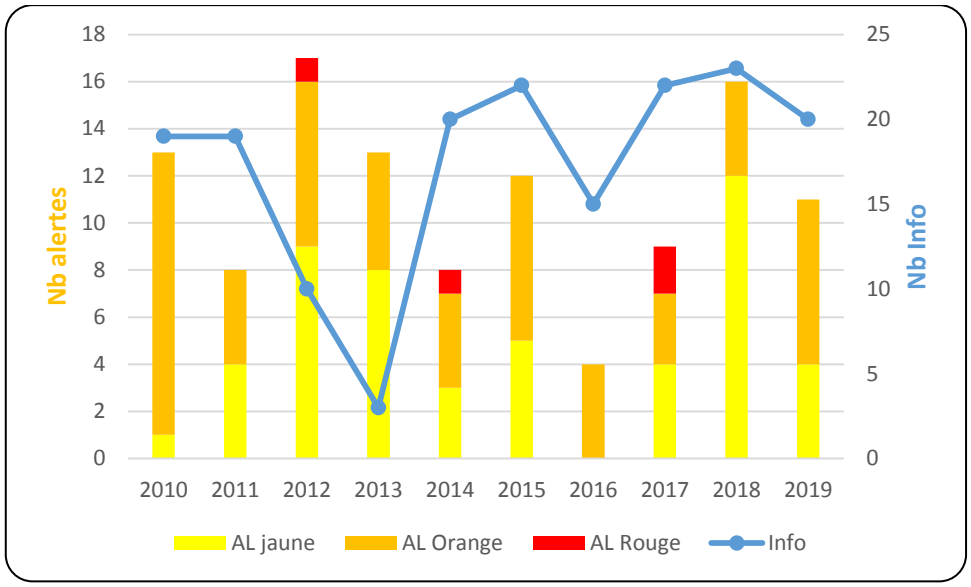
Le Cert-IST émet ainsi plusieurs types de publications :

- **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 par exemple au cas où des programmes d'attaques – des "exploits" – sont publiés.
- **Les Alertes (AL)**, qui sont émises lorsqu'il y a un risque spécifique d'attaque et les **messages INFO** lorsqu'une menace existe (et qu'elle est médiatisée) 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).
- **Les 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).

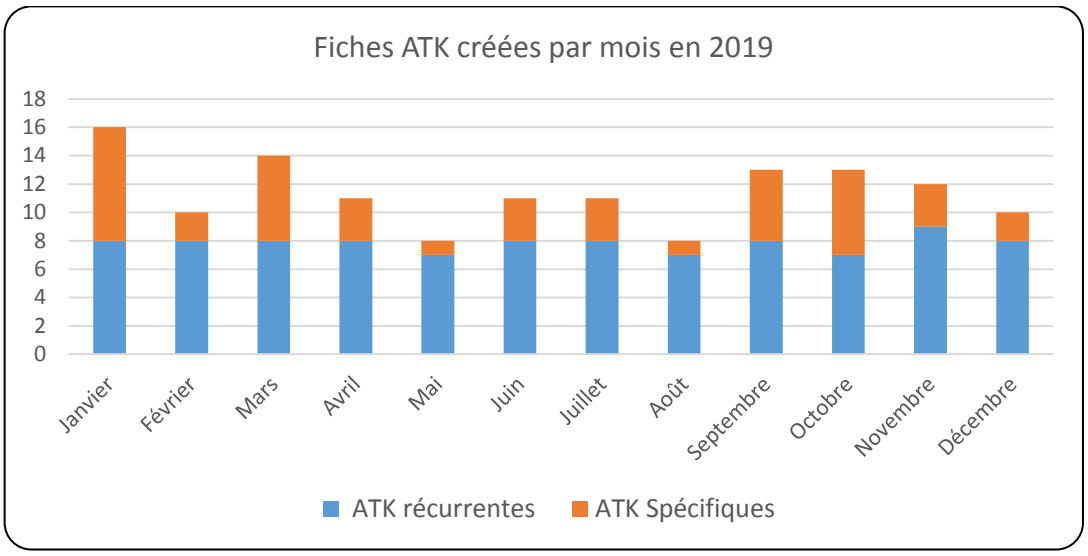
Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.



Nombre d'avis de sécurité publiés par an



Nombre d'alertes publiées par an



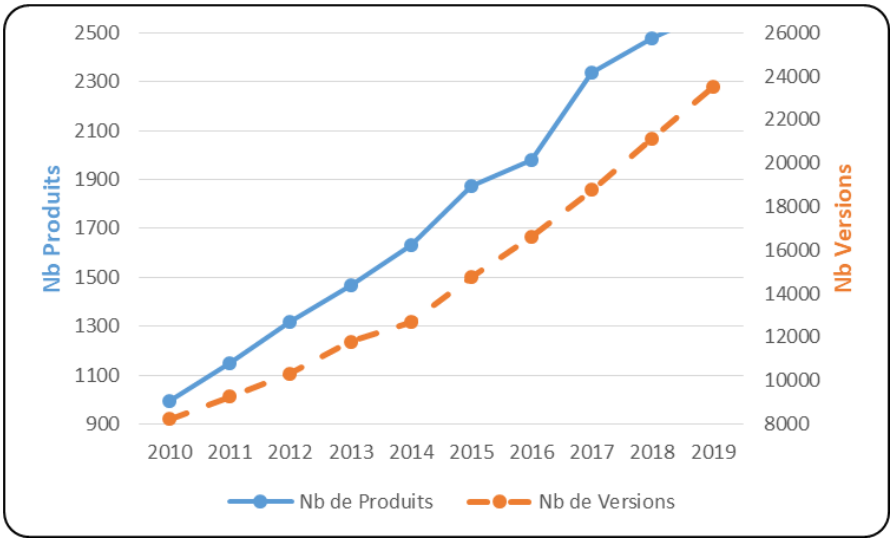
Nombre de fiches attaques publiées par mois
Nota : le service ATK (et IOC) est disponible depuis juillet 2016

Ainsi, en 2019, le Cert-IST a publié :

- **1 659** avis de sécurité (dont **80** avis SCADA), **4 597** mises à jour mineures et **112** mises à jour majeures.
  Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec en 2019 une augmentation de **14%** par rapport à 2018. 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.

- **11** alertes et **20** messages Info. Les dernières alertes rouges ont été émises en 2017 (Wannacry et NotPetya). D'année en année, l'activité dans cette catégorie est très fluctuante et on ne note pas de tendance sur l'évolution globale.
- **136** fiches attaques ont été publiées en 2019, avec dans la base de données MISP **2 854** évènements qui ont été enrichis, et **498 577** marqueurs (IOC) utilisables.

Concernant les produits et les versions suivis par le Cert-IST, fin 2019 le Cert-IST suivait **2 594** produits et **23 504** 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

- **2019 : une monté en flèche inquiétante des attaques de ransomwares**

L'année 2019 montre une menace de plus en plus forte pour les entreprises et prend même une tournure critique si l'on considère l'évolution des attaques de ransomwares (cf. § 3.2)

Certaines des attaques de ransomware de 2019 ont été annoncées dans la presse, en France (M6, Fleury Michon, CHU de Rouen, etc…) ou dans le monde (Norsk Hydro, Mitsubishi Aerospace, ville de Baltimore, etc.). Elles ont toutes en commun d'être des attaques visant spécifiquement des grandes organisations (susceptibles de payer des rançons substantielles), et d'avoir causé des arrêts informatiques majeurs (parfois de plusieurs semaines).

Au-delà des ransomwares, tout ce qui rapporte de l'argent est susceptible d'intéresser les cybercriminels, et en 2019 les attaques les plus visibles ont concernés également (cf. § 3.3) :

- Les crypto-mineurs : un très grand nombre des attaques vues en 2019 avaient comme objectif d'installer un logiciel de crypto-minage sur les serveurs d'entreprises vulnérables.
- Les « skimmers web » : de nombreux sites web marchands ont été infectés par des attaques **Magecart** (nom donné à cette technique d'attaque) où un code JavaScript est installé par le pirate pour voler les données (de carte bancaire) saisies dans le formulaire de paiement du site.

- **Les entreprises dans le viseur des cybercriminels et des cyber-espions**

Depuis plusieurs années, on observe une progression de la menace avec des attaques qui touchent un éventail de plus en plus large d'entreprises :

- Les attaques cybercriminelles ont historiquement débutées (aux alentours de 2005) contre les banques et leurs clients, ou contre les sites de pari en ligne. Aujourd'hui les cybercriminels attaquent avec un ransomware n'importe quelle entreprise susceptible de payer une rançon importante.
- Les cas de cyber-espionnage et les attaques sponsorisées par les Etats sont devenus un phénomène d'ampleur en 2013. Alors qu'elles concernaient avant tout les entreprises internationales, ces attaques prennent aujourd'hui souvent pour cible les sous-traitants de ces entreprises, pour effectuer ensuite des attaques par rebond.

Si les entreprises sont clairement devenues des cibles de grand intérêt pour les cybercriminels, on observe également une diffusion de plus en plus rapide des techniques d'attaques des attaquants les plus aguerris vers les autres :

- Les cybercriminels s'inspirent de ce qu'ils voient ailleurs : les attaques par infiltration (rentrer discrètement dans l'informatique d'une entreprise et y progresser plusieurs semaines pour atteindre les cibles de valeurs) ont été vues d'abord dans les attaques étatiques et de cyber-espionnage, mais sont maintenant aussi couramment pratiquées par les cybercriminels.
- Les cybercriminels savent très vite convertir un « exploit » (programme permettant d'exploiter une vulnérabilité, développé par des experts et rendu public plus tard via des outils ouverts comme Metasploit) en une campagne d'attaques.

- **La sécurité en profondeur : une base indispensable de défense**

Les entreprises qui ne sont pas attentives à leur sécurité informatique sont aujourd'hui très vulnérables aux cyber-attaques.

Cela implique tout d'abord de mettre en place des défenses et de cloisonner les architectures. Aucun système n'étant infaillible, il faut aussi se poser des questions (dès la conception d'un système) telles que :

- Que se passera-t-il lors d'une attaque réussie ?
- Comment peut-on limiter la propagation de cet incident ?
- Quel sera l'impact en cas de fuite de données ?

Un autre élément important est de maintenir à jour les systèmes en appliquant les correctifs de sécurité diffusés par les constructeurs. Après les erreurs humaines (incluant le phishing), les correctifs non appliqués sont la plus importante cause d'intrusion. On a souvent observé que de vieilles vulnérabilités permettaient toujours des intrusions plusieurs années après que des correctifs soient disponibles. Bien sûr il existe souvent une fraction de systèmes « non-patchables » au sein des organisations (obsolètes, non répertoriés, etc.), cependant le déploiement des correctifs de sécurité reste une pratique fondamentale pour la sécurité. Pour les vulnérabilités les plus graves, le Cert-IST émet des alertes (une dizaine par an) en plus des avis de sécurité (cf. § 5.1). Ces alertes sont des indicateurs pour les entreprises que le déploiement des correctifs doit être particulièrement rapide.

- **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 un socle de défense solide 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 » (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 cybersécurité 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). Mais pour les attaques par infiltration **c'est en fait le défenseur qui a l'avantage**, car 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 dans l'entreprise 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