Cert IST

Industrie Services Tertiaire

Bilan Cert-IST des failles et attaques de 2020

Publié en Février 2021

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 2020 (cf. chapitre 2), puis nous analysons les éléments les plus significatifs (cf. chapitre 3). Nous fournissons ensuite un récapitulatif des différentes productions du Cert-IST au cours de cette année (cf. chapitre 4).

La conclusion (cf. chapitre 5) 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 2020

Le tableau ci-dessous récapitule des événements marquants de 2020, 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 2020	**Travelex**, spécialiste du change monétaire a été touché le 31/12/2019 par le **ransomware** Sodinokibi. Cette attaque cyber a été le déclencheur d'une crise plus large (dans un contexte Covid difficile) l'ayant amené à restructurer fortement son activité. De nombreuses attaques de ransomware seront annoncées tout au long de l'année. Parmi les très nombreuses victimes on peut citer en France **Bouygues Construction**, **Carlson Wagonlit Travel**, **Steria-Sopra** ou le **CHU de Rouen**, et à l'étranger **Carnival** (croisière), **Brown-Forman** (whiskey Jack Daniel's), **Garmin** (GPS), **Enel** (Electricité), **Software AG** (logiciel), …
Janvier 2020	**Citrix Netscaler et ADC** (CVE-2019-19781) : Une vague d'attaques visant ces équipements Citrix force l'éditeur à développer en urgence des correctifs. Cette crise qui a duré pendant tout le mois de janvier a été surnommée par certains **Shitrix**.

Janvier 2020	**CurveBall : le bug de la NSA** dans la cryptographie elliptique. Microsoft corrige cette vulnérabilité CVE-2020-0601 dans Windows 10 qui affecte la vérification de la signature numérique lorsqu'elle utilise la cryptographie elliptique. Cette vulnérabilité a fait parler d'elle parce qu'elle a été découverte par la NSA (d'où son nom de « bug de la NSA ») et qu'elle casse la signature électronique partout (sur Windows 10) : dans les mails, les sites web, les exécutables, etc…
Janvier 2020	D'autres vulnérabilités Microsoft ont aussi eu un nom en 2020, sans vraiment provoquer d'attaques d'ampleur : **Bluegate** (vulnérabilité RDP Gateway en janvier), **GlueBall** (vulnérabilité dans la signature cryptographique des fichiers MSI, en août) ou **Badneighbor** (vulnérabilité ICMPv6, en octobre). Nous parlons aussi dans la suite du tableau de failles plus graves : **SMBGhost** et **SMBleed** (mars), **SIGRed** (juillet), **ZeroLogon** (septembre) et **Bronze Bit** (novembre).
Janvier 2020	**Intel CacheOut** : une nouvelle attaque des processeurs Intel est annoncée. Depuis Spectre et Meltdown en janvier 2018, les découvertes de ce type se sont multipliées. Pour 2020 on peut citer aussi :**L1DES**, **VRS**, **LVI** (Load Value Injection sur Intel), **Take A Way** (AMD), **CSME IOMMU CVE-2019-0090** (Intel), **StarBleed** (FPGA Xinlinx), **Platypus** (Intel power leakage) et **Crosstalk**.
Février 2020	**Ghostcat** (CVE-2020-1938) une vulnérabilité critique dans le connecteur AJP de **Tomcat** (serveur web Java de la fondation Apache) permet de lire à distance n'importe quel fichier du serveur web (et même d'exécuter du code si le dépôt de fichier est autorisé). Cette vulnérabilité a été très utilisée en 2020 dans des attaques contre les serveurs Tomcat.
Février 2020	Vulnérabilité **Kr00k dans WPA2**. Il s'agit d'une variante de l'attaque KRACK (Key Reinstallation Attack) de 2017 et son nom a d'ailleurs été construit en remplaçant par des zéros 2 lettres de KRACK (l'attaque utilise le fait que la clé WPA2 est écrasée par des zéros lorsqu'une dé-association se produit).
Mars 2020	**SweynTooth** : c'est le nom donné à une série de 12 vulnérabilités (de gravité variable) dans les chipsets **Bluetooth** de certains constructeurs (dont Cypress, NXP et Texas Instrument). D'autres vulnérabilités Bluetooth seront publiées au cours de l'année : **BLURtooth**, **BLESA** et **BleedingTooth**.
Mars 2020	**SMBGhost** : Suite à un cafouillage, la vulnérabilité CVE-2020-0796 dans la compression SMBv3 de Windows est accidentellement révélée 3 jours avant la publication des correctifs Microsoft. Cette vulnérabilité wormable est critique et on redoute des attaques massives comme pour EternalBlue (WannaCry) en 2017. Des programmes d'exploitations sont annoncés (en particulier par la société ZecOps.com) et finalement retardés. Ils sortent en juin et le Cert-IST passe son alerte CERT-IST/AL-2020.005 au niveau orange. En juin Microsoft corrige de nouvelles vulnérabilités SMBv3, dont la vulnérabilité **SMBleed** (CVE-2020-1206) que ZecOps utilise dans son programme d'exploit en combinaison avec SMBGhost. Jusqu'à présent il n'y a pas eu d'attaque massive au moyen de ces vulnérabilités.
Avril 2020	**Zoom** : Cette solution de vidéo conférence suscite un intérêt soudain, du fait du confinement. Des inquiétudes sur sa sécurité amènent certaines organisations à interdire son usage. La société Zoom y répond en redoublant ses efforts sur la sécurité du produit (qui jusqu'alors ne semblait pas une priorité).
Mai 2020	**Strandhogg 2.0** : Cette vulnérabilité **Android** reprend le nom d'une vulnérabilité similaire publiée en décembre 2019 et permet d'espionner les applications lancées sur le smartphone. Elle avait été corrigée en avril par Google, avant d'être détaillée en mai.

Mai 2020	**SaltStack** (un outil permettant de gérer des pools de serveurs dans un Datacenter et comparable à des logiciels comme Puppet, Ansible ou Chef) corrige des vulnérabilités critiques (CVE-2020-11651 et CVE-2020-11652) qui sont dès le week-end suivant utilisées par une vague d'attaques. L'attaque permet de prendre le contrôle de toutes les machines du Datacenter gérées avec SaltStack.
Juin 2020	**L'Australie** annonce être victime d'une attaque de grande ampleur visant tous les secteurs d'activité et provenant d'un attaquant étatique (peut-être la Chine). Elle décrit en détail les modes opératoires dans un rapport baptisé « **Copy-paste compromises** – TTP used to target multiple Australian networks » (cf. § 3.6).
Juin 2020	La société JSof-Tech.com publie **Ripple20** : un ensemble de vulnérabilités qui affectent la pile TCP/IP développée par Treck et qui est utilisée dans de très nombreux produits (objets connectés, équipements industriels ou médicaux, etc.). Cet événement rappelle la publication d'Urgent/11 (été 2019) et Amnesia:33 (voir en décembre ci-dessous).
Juin 2020	**Une vulnérabilité UPnP "CallStranger"** est publiée. Elle est de gravité modérée sauf dans le cas où l'équipement UPnP vulnérable est en jonction entre 2 réseaux : cet équipement pourrait dans ce cas être utilisé comme relais par un attaquant. Nous avons émis le message **INFO-2020.018** pour attirer l'attention sur cette vulnérabilité.
Juillet 2020	**22 900 bases MongoDB** qui étaient accessibles sur Internet sans protection ont été effacées par un pirate (voir cet article ZDNet).
Juillet 2020	Spectaculaire opération de police en France (C3N) et au Pays-Bas contre **les utilisateurs des téléphones EncroChat**. Ces téléphones sécurisés vendus aux criminels utilisaient un serveur situé en France, ce qui a permis une infiltration par le C3N.
Juillet 2020	Microsoft corrige la vulnérabilité **SIGRed** (CVE-2020-1350) qui affecte son serveur DNS et permet à un attaquant distant d'exécuter du code avec les droits SYSTEM sur les machines vulnérables. Il n'y a pas eu de vague massive d'attaques, mais cette vulnérabilité est citée dans le Top 25 des vulnérabilités utilisées dans des attaques chinoises (cf. § 3.6). Nous avons émis l'alerte **CERT-IST/AL-2020.009** pour cette vulnérabilité.
Juillet 2020	Vulnérabilité **SAP RECON** (Remotely Exploitable Code On NetWeaver) : La société Onapsis recommande d'appliquer au plus vite les correctifs SAP pour cette vulnérabilité du composant NetWeaver.
Juillet 2020	La vulnérabilité **BootHole** (CVE-2020-10713) a été largement médiatisée mais son impact reste modéré puisqu'elle affecte Linux principalement. Elle concerne le boot-loader GRUB2 et permet d'exécuter du code au démarrage de la machine (attaque de type bootkit).
Septembre 2020	**ZeroLogon** : Cette attaque exploite la vulnérabilité CVE-2020-1472 sur le service NetLogin de Windows. Elle permet à un attaquant déjà entré dans l'entreprise d'obtenir instantanément un accès administrateur sur les Contrôleurs de Domaines (DC) Windows qui n'ont pas appliqué les correctifs. Cette vulnérabilité est souvent la première qui est testée par un attaquant (parce qu'elle est facile à mettre en œuvre).
Septembre 2020	Des **attaques DDOS accompagnées de mails de chantage** sont observées fin août et début septembre (cf. § 3.5). Ces attaques recommenceront ensuite en fin d'année. Elles n'ont pas eu de conséquences fortes mais montrent que les attaques DDOS sont une nuisance que l'on ne peut ignorer.

Octobre 2020	Une action conjointe de plusieurs éditeurs (Microsoft, ESET, etc.) tente de **neutraliser le Botnet Trickbot**. L'opération est partiellement réussie (120 des 128 serveurs C&C de Trickbot ont été neutralisés) mais le malware s'est réorganisé ensuite et a renforcé son architecture en utilisant EmerDNS (un système DNS résiliant du projet Emercoin) et des C&C avec une extension **.bazar**. Un des buts de l'opération Microsoft aurait été de perturber Trickbot pendant les élections américaines pour éviter des tentatives d'influences.
Novembre 2020	**SAD DNS** (CVE-2020-25705) est une nouvelle méthode pour réaliser l'attaque de "DNS cache poisoning" découverte en 2008 par Dan Kaminsky et corrigée la même année. SAD DNS contourne cette correction en utilisant une nouvelle méthode (un "side-channel") basée sur les messages "ICMP rate limit" pour deviner le port UDP utilisé par le serveur DNS.
Novembre 2020	**Cobalt Strike** : Une partie des sources de cet outil offensif a été diffusée sur Internet. Cobalt Strike est un outil commercial de test d'attaques, mais il est de plus en plus souvent vu dans des attaques réelles (cf. § 3.7.3). En 2020 il a par exemple été énormément utilisé au cours d'attaques de ransomwares.
Novembre 2020	Une liste de **50 000 machines Fortinet vulnérables** à la faille CVE-2018-13379 circule sur Internet. Cette vulnérabilité a été corrigée par Fortinet en mai 2019 mais les machines vulnérables n'ont probablement pas été mises à jour depuis 1 an et demi.
Novembre 2020	**Kerberos Bronze Bit** est une nouvelle attaque Kerberos, similaire aux attaques "Golden Ticket" et "Silver Ticket". Elle permet, en changeant quelques bits dans un ticket Kerberos authentique, d'augmenter illégalement les privilèges d'un utilisateur connecté.
Décembre 2020	**Amnesia:33** est le nom donné par la société Forescout à un ensemble de 33 vulnérabilités découvertes dans 4 piles TCP/IP open-sources (uIP, FNET, picoTCP and Nut/Net) utilisées dans de nombreux produits (smartphones, console de jeux, capteurs, etc.). Ces découvertes sont issues d'un projet inspiré de Ripple20 (voir ci-dessus en juin) en recherchant des failles dans d'autres piles TCP/IP.
Décembre 2020	**Attaque SolarWinds Orion** : Cette attaque (supposée russe) est un événement majeur de 2020 (cf. § 3.4) par sa nature (attaque via la supply-chain en piégeant le logiciel Orion de la société SolarWinds), son ampleur (compromission de plusieurs agences américaines et d'entreprises de premier plan comme FireEye et Microsoft) et sa sophistication.
Décembre 2020	**Flash Player** c'est fini ! Fin 2020 Adobe arrête ce produit phare des années 2000. Développé initialement par Macromedia (société rachetée par Adobe en 2005) le produit a connu beaucoup de problèmes de sécurité de 2008 à 2012. Depuis 2010 Apple refusait qu'il soit présent sur ses tablettes et téléphones. Flash a ensuite été progressivement supplanté par les fonctions natives de HTML5.

3 Analyse des phénomènes les plus marquants de 2020

Dans ce chapitre nous analysons successivement les événements les plus marquants de l'année :

- La menace cyber induite par la crise de la Covid-19
- Les attaques de Ransomware visant les entreprises
- Les attaques visant les accès VPN et les Appliances exposées
- L'attaque Orion SolarWinds et les attaques par la Supply-chain
- Les attaques DDOS
- Les attaques étatiques de plus en plus sophistiquées
- Les évolutions techniques observées en 2020

En bref, …

Il n'y a pas vraiment de surprise sur la liste des phénomènes les plus marquants de 2020 : Covid-19, Ransomware, et attaque SolarWinds sont bien sûr dans la liste. La suite de ce chapitre analyse plus en détail chaque point, mais si vous n'avez que quelques minutes pour lire ce rapport, voici l'essentiel.

- Covid-19 : Il n'y a pas jusqu'à présent de cas connu où une intrusion a été attribuée formellement aux mesures techniques prises pour permettre le télétravail. Cependant, il est certain que face à l'urgence et pour la mise en place rapide du télétravail, certaines entreprises **se sont exposées à un risque accru d'intrusion.**

- Ransomware : Déjà phénomène majeur de 2019, les attaques de ransomware ont explosées en 2020 et il n'y pas encore de signe d'une décrue. Les cybercriminels multiplient les moyens de pressions sur les entreprises et collaborent entre eux dans un écosystème de plus en plus organisé.

- Attaque des VPN : Ces attaques visent souvent des équipements qui nous semblent trop fragiles (durs dehors mais mous dedans). De plus en plus souvent ces attaques servent de point de départ pour entrer plus profondément dans l'entreprise.

- Attaque SolarWinds : Au-delà de mettre en avant les attaques de la Supply-chain, l'attaque SolarWinds montre que l'environnement Cloud Office 365 est une cible convoitée.

- Attaques DDOS : Elles sont toujours là et constituent une menace pour laquelle l'entreprise doit avoir prévu une réponse.

- Attaques étatiques : Certains états ont démontré en 2020 des capacités avancées en cyber-attaque. Par exemple, la Chine a montré son professionnalisme pour industrialiser les vulnérabilités rendues publiques, et la Russie son expertise pour concevoir des attaques complexes.

- Evolutions techniques : Microsoft Exchange, attaques SAML et OAUTH, et Cobalt Strike sont 3 des domaines techniques que nous avons identifiés comme marquants pour l'année 2020.

3.1 La menace cyber induite par la crise de la Covid-19

La crise COVID-19 est avant tout une crise sanitaire et économique. Mais elle a également généré des inquiétudes soutenues d'un point de vue informatique, et on peut les regrouper en 3 domaines qui se sont succédés (presque) chronologiquement :

- Les attaques mail et web qui utilisent le thème du Covid-19,
- Les attaques qui visent les outils informatiques utilisés du fait du télétravail,
- Les attaques qui visent les hôpitaux, la recherche et les vaccins.

Nous examinons chaque domaine ci-dessous, mais deux questions préalables permettent de mieux cerner la menace cyber induite par la Covid-19 :

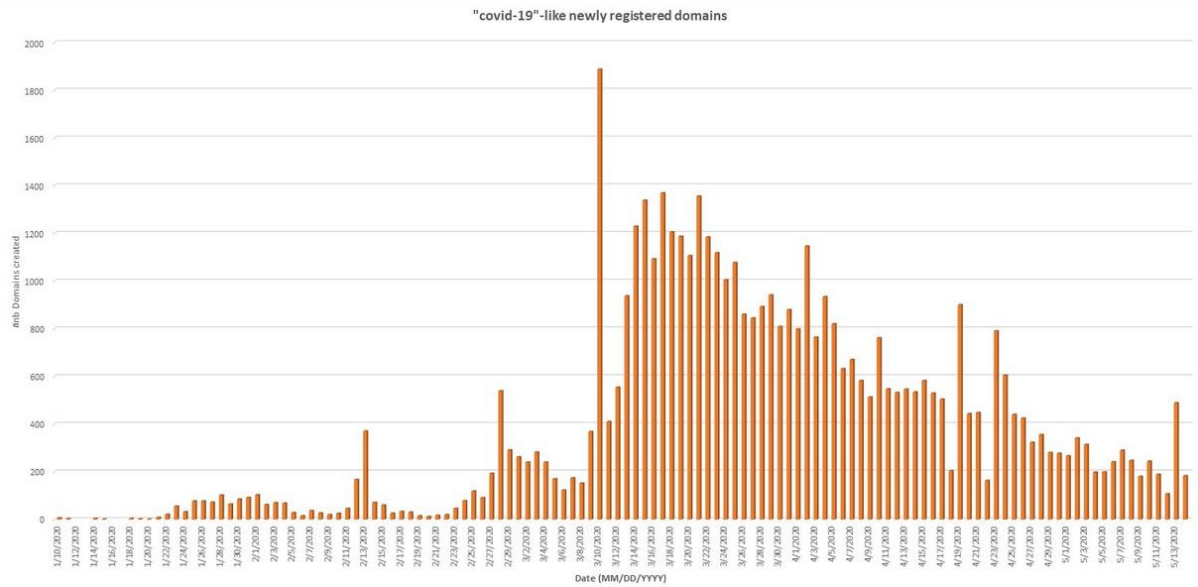
- Qui sont les attaquants ? : On retrouve pour ces attaques, 2 groupes bien connus dans le paysage de la cyber-menace : les cyber-délinquants (le cybercrime) qui cherchent à gagner de l'argent au moyen de la crise de la Covid, et les cyber-espions (les attaques étatiques) qui ont des intérêts stratégiques liés à la Covid.
- Qui sont les cibles ? : Majoritairement, le cyber-espionnage vise les entreprises alors que les cybercriminels visent toutes les personnes susceptibles de payer (grand public, entreprises, hôpitaux et états). Mais, le cyber-espionnage utilise aussi parfois des attaques par rebond, en visant des employés à leur domicile dans le but d'atteindre ensuite leur entreprise. Et ce dernier aspect prend de l'importance dans le cas de la crise Covid-19.

On voit au travers de ces 2 questions que la Covid-19 ne change donc pas fondamentalement le paysage de la menace (mêmes acteurs et même cibles). Par contre deux aspects sont préoccupants dans le cadre de la crise Covid-19 :

- **La quantité d'attaques** : Il y a eu une explosion du nombre de tentatives d'attaque, à cause d'un effet d'aubaine (le thème de la Covid intéresse tout le monde) et aussi d'un effet d'urgence (il faut réagir vite, pour profiter de l'aubaine, mais aussi tirer parti du contexte anxiogène).
- **Les attaques par rebond** visant les télétravailleurs sont facilitées par la mise en place du confinement et le déploiement rapide de solutions techniques pour le télétravail.

• Les attaques mail et web

Le premier effet de la crise Covid a été une explosion des attaques par mail qui utilisaient le sujet de la Covid-19 pour infecter les ordinateurs des victimes à l'aide de pièces jointes piégées, ou les attirer vers des sites web piégés. Ces attaques ont été utilisé par tous les types d'acteurs : les escrocs (vente de produits, faux SMS, etc.), les Botnets habituels (Emotet, Trickbot, etc.) et les attaques de cyber-espionnage (Spear-phishing utilisant le thème de la Covid-19).



La figure ci-dessus montre l'évolution du nombre de noms de domaines créés avec des thèmes relatifs à la Covid-19 de janvier à la mi-mai 2020. Une grande partie de ces domaines étaient malveillants et cette courbe est un indicateur du nombre d'attaques mails et web observées. Les premières attaques ont été des MalSpam Emotet fin janvier 2020. Les attaques se sont multipliées à partir du 25/02/2020 puis ont explosé en nombre à la mi-mars. Elles ont ensuite progressivement diminué. Fin 2020, une légère hausse a été observée, probablement lié à la disponibilité des vaccins.

• Les attaques des outils informatiques

Dans un second temps, les mesures de confinement ont obligé les entreprises à mettre en place (ou à amplifier) le télétravail. Cela a entrainé des problèmes de plusieurs natures :

- La mise en place par des organisations de solutions d'accès mal sécurisées (les seules disponibles immédiatement) : ouverture d'accès RDP non protégés, remise en service d'équipements d'accès obsolètes (non mis à jour), etc.
- La mise en place par les utilisateurs de leurs propres solutions : utilisation d'ordinateurs et de messageries personnelles, utilisation d'outils de vidéo-conférence multiples installés à partir de sources non sûres (voir par exemple cette fausse application Zoom),
- Difficulté pour les entreprises à maintenir les règles de sécurité nominales : report des mises à jour des postes nomades (par crainte de dysfonctionnement ou manque de bande passante réseau), assouplissement des règles d'expiration des mots de passe, adoption d'exceptions multiples, etc.

On manque encore de données pour quantifier l'impact réel de ces difficultés, et il n'y a pas à notre connaissance de cas connu d'incident grave formellement attribué aux mesures techniques mises en place pendant la Covid-19. Il est certain par contre que beaucoup ont fait au mieux, et se sont exposés à un risque accru d'intrusion. Il est important de limiter la durée de cette période de vulnérabilité et d'étudier les mesures pour :

- Améliorer si besoin la sécurité des solutions de télétravail mises en place,

- Détecter le plus tôt possible les fuites de données ou les intrusions réussies qui ont éventuellement pu se produire.

Ce dernier point (la détection) rejoint une préoccupation croissante depuis plusieurs années : à défaut de pouvoir empêcher 100% des attaques, il faut les détecter (a posteriori) le plus rapidement possible (réduire le « Time to Detect ») et limiter leurs impacts.

• Les attaques visant les hôpitaux, la recherche et les vaccins

Ce dernier aspect s'est manifesté à différents moments de la crise :

- Les attaques contre les hôpitaux sont arrivées au début de la crise et se sont plutôt atténuées ensuite. Ces attaques ont été nombreuses. D'une part, certains attaquants espéraient sans doute que les hôpitaux paieraient vite pour se débarrasser des problèmes informatiques (cela n'a pas été le cas à notre connaissance) et se concentrer sur le soin aux malades. D'autre part, quelques-unes des premières attaques ont probablement touchées par hasard des structures de soin, sans volonté de profiter de la crise Covid-19. Par la suite, certains attaquants ont d'ailleurs décidé d'épargner ce type de victimes, mais cette consigne n'a pas été suivie par tous.
- Les attaques contre la recherche et les vaccins. Ces attaques ont été révélées plus tard (à partir de fin avril 2020, pendant l'été et en décembre 2020) et il s'agit cette fois d'attaques de cyber-espionnage ou de désinformation. Le Vietnam, la Chine, la Russie et la Corée du Nord ont été cités pour ces attaques. En décembre 2020 l'Agence Européenne de Médecine a annoncé avoir été victime d'une cyber-attaque (probablement Russe) visant des données de qualifications des vaccins (cf. l'annonce officielle et cet article de Kaspersky).

3.2 Les attaques de Ransomware visant les entreprises

Les attaques de ransomware visant les entreprises (ce que l'on appelle souvent le Big-Game Hunting ou la Chasse au gros gibier) étaient déjà un des phénomènes majeurs pour l'année 2019 (cf. notre bilan pour l'année 2019). Et clairement le phénomène a encore empiré en 2020 avec :

- Une multiplication du nombre de groupes cyber-criminels qui ont adopté cette technique d'extorsion (parce qu'elle est rentable).
- Des techniques de plus en plus pressantes pour convaincre la victime de payer (voir ci-dessous).

L'ANSSI a annoncé un quadruplement dans le nombre d'attaques traitées en France en 2020 par rapport à 2019 (192 interventions contre 54).

Les techniques de pression des attaquants :

En plus de chiffrer les données d'un maximum de machines de la victime, les attaquants ont progressivement ajouté d'autres techniques pour forcer la victime à payer les rançons :

- Voler des données de l'entreprise et menacer de les publier ou de les vendre aux enchères. Cette technique a été vue pour la première fois en novembre 2019 (ransomware Maze contre Allied Universal), mais est devenue presque systématique à partir de 2020. Plusieurs entreprises victimes ont indiqué en 2020 avoir payé une rançon pour que les

données volées ne soient pas publiées, plutôt que pour obtenir de déblocage des ordinateurs.
- Publier sur un site web le nom des victimes, et afficher un compte à rebours avant publication des données volées. Cette publicité à propos des attaques semble même prendre la tournure de véritables campagnes de presse puisque très récemment (en janvier 2021) le groupe d'attaquants DarkSide a invité la presse à les contacter pour être tenue au courant des négociations en cours avec les victimes.
- Réaliser des attaques DDOS pour saturer l'accès Internet de l'entreprise. Cette technique a été utilisée par exemple en septembre 2020 avec le ransomware SunCrypt, mais ne s'est pas généralisée depuis. Il est possible que cette technique de pression ait été inspirée par la série d'attaques DDOS vue en septembre 2020 (cf. § 3.5).
- Intimider physiquement (appel téléphonique de menace) pour pousser les sociétés victimes à payer En décembre 2020, le FBI a indiqué que cette pratique avait été observée depuis février 2020.

Pour les victimes on a vu aussi plusieurs évolutions :

- En 2019, payer la rançon (et en parler) était devenu quelque chose d'admis (en dernier recours). En 2020, payer une rançon parait de moins en moins une solution si l'on ne peut pas garantir que l'attaquant (ou un autre attaquant) ne reviendra pas avec une nouvelle demande de rançon, parce qu'il a conservé des accès dans la société ou qu'il a conservé des données volées qu'il veut maintenant négocier.
- Le recours aux assurances (pour prendre en charge une partie des coûts de remise en service) et l'intervention de sociétés spécialisées dans la négociation (pour dialoguer avec les attaquants et faire baisser la rançon) deviennent des pratiques communes et recommandées.

• L'écosystème cybercriminel :

Les attaques par ransomware font intervenir tout un ensemble d'acteurs qui collaborent et constituent un écosystème ou chacun est rétribué en fonction des services qu'il rend.

Au sommet de cette chaine se trouve le groupe qui dirige les infections. Il est souvent appelé Groupe RAAS (Ransomware As A Service). Il fournit le ransomware et un accès chez une victime, à un affilié qui est chargé d'explorer le système d'information de la victime et d'y installer le ransomware. Les accès chez les victimes ont été obtenus précédemment sur des forums underground auprès d'un grossiste (un Broker), qui achète ces accès (adresse mail ou login, et mot de passe associé) auprès de spécialistes ATO (Account Take Over). Ces derniers volent ces comptes en organisant des campagnes de phishing ou en testant en masse des couples login et mot de passe obtenus lors de fuites de données (attaque dite de « password stuffing »). Une dernière catégorie d'acteurs est spécialisée dans la fuite de données (vol de bases des comptes) ou l'attaque directe de serveurs (ils vendent ensuite l'accès à la backdoor qu'ils ont installée sur les machines attaquées).

Nota : On connait depuis des décades les attaques en force brute sur les accès SSH, mais ce phénomène s'est largement amplifié depuis quelques années avec les fuites de données et le « password stuffing ». Plus globalement, selon Akamai, les attaques ATO représentent 98% des attaques vues sur l'infrastructure Akamai (chiffres données lors d'une présentation à la conférence BotConf 2020).

Le texte ci-dessous est extrait de la Une de notre bulletin mensuel d'octobre 2020.

Selon un rapport publié en novembre 2020 par Coveware.com (et qui est cohérent à ce qui a été publié par d'autres sources)

- Les rançons sont en médiane de **l'ordre de 100 000 dollars** (pour Q3-2020) mais les montants grimpent rapidement lorsque les sociétés attaquées sont de grande taille (voir le nota ci-dessous). L'attaque de ces grandes sociétés est donc le marché le plus lucratif pour les attaquants.
- Payer une rançon pour éviter la publication des données volées est probablement un mauvais choix car dans certains cas les données ont fini par être publiées.
- Les **accès RDP mal sécurisés** restent le vecteur numéro un d'attaque (devant le phishing et les failles logicielles).
- L'indisponibilité moyenne suite à une attaque de ransomware est de **19 jours**.

Nota : selon les rapports publiés, les rançons de l'ordre de 5 millions de dollars ne sont pas exceptionnelles.

3.3 Les attaques visant les accès VPN et les Appliances exposées

Au cours de l'année 2020, les attaques visant les accès VPN des entreprises (et plus généralement les Appliances qui sont en jonction entre Internet et le réseau d'entreprise) se sont multipliées. Ce phénomène était apparu en septembre 2019 avec l'attaque des équipements PulseSecure et Fortinet et s'est amplifié en 2020.

Voici les équipements visés par ces attaques et les références des avis ou alertes émis par le Cert-IST sur ces sujets (cf. le chapitre 4 pour la distinction entre ces 2 types de publications Cert-IST). **Les entreprises qui utilisent ces équipements doivent absolument avoir appliqué les correctifs pour ces vulnérabilités.**

- **F5 BIG-IP (CVE-2020-5902) :** avis **CERT-IST/AV-2020.0878** du 01/07/2020 et alerte **CERT-IST/AL-2020.008,**
- **Palo Alto Networks (CVE-2020-2021) :** avis **CERT-IST/AV-2020.0868** du 30/06/2020 et alerte **CERT-IST/AL-2020.007,** et **Global Protect VPN (CVE-2019-1579)** : avis **CERT-IST/AV-2019.0903** du 19/07/2019, et alerte **CERT-IST/AL-2019.010**.
- **Citrix ADC et Citrix Gateway (CVE-2019-19781)** : avis **CERT-IST/AV-2019.1624** du 18/12/2019 et alerte **CERT-IST/AL-2020.001,**
- **Pulse Secure VPN (CVE-2019-11510) :** avis **CERT-IST/AV-2019.0520** du 25/04/2019 et alerte **CERT-IST/AL-2019.010**.
- **Fortinet VPN SSL (CVE-2018-13379) :** avis **CERT-IST/AV-2019.0668** et l'alerte **CERT-IST/AL-2019.010**).

• Des Appliances dures dehors et molles dedans ?

La plupart de ces équipements vulnérables sont des Appliances, c'est-à-dire des machines construites pour rendre un service précis (firewall, antispam, WAF, etc…). Une Appliance est souvent construite en utilisant un OS standard (par exemple Linux, FreeBSD, etc.) configuré sur mesure, et des logiciels applicatifs propriétaires. Les attaques vues en 2020 mettent en évidence que certaines de ces Appliances sont « dures dehors, mais molles dedans » :

- La couche externe est dure : il y a peu de services réseaux exposés et ils sont hébergés par un OS robuste.
- Mais les composants internes sont plutôt mous : si une première vulnérabilité mineure est trouvée (par exemple une « traversée de répertoire »), l'attaquant peut ensuite atteindre des composants internes qui ne sont pas assez solides pour résister à des attaques plus profondes.

Du fait d'un manque de cloisonnement et de défense en profondeur (ce qui est préoccupant pour un équipement conçu pour être branché directement sur Internet), une petite vulnérabilité permet donc au final (en enchainant d'autres attaques) une prise de contrôle complète de l'équipement.

• Une cible attractive pour les attaquants

Ces équipements sont souvent exposés en frontal sur Internet et dès qu'une vulnérabilité est trouvée, des attaques se produisent. Certains attaquants se contentent d'installer sur la machine vulnérable un crypto-mineur (un logiciel qui utilise la CPU pour générer de la crypto-monnaie), mais de plus en plus souvent (et c'est un fait marquant de 2020) **ces attaques servent de point de départ pour entrer plus profondément dans l'entreprise**. L'attaquant peut par exemple ensuite installer un ransomware dans l'entreprise (attaque cybercriminelle) ou procéder à du cyber-espionnage (attaque étatique).

On constate aussi qu'**il reste longtemps des équipements vulnérables, même pour les failles médiatisées**, parce que ces équipements ont été oubliés et laissés sans maintenance. Par exemple (comme nous l'indiquions dans notre message **INFO-2020.035**), en novembre 2020 il circulait sur Internet une liste de près de 50 000 machines Fortinet probablement vulnérables à la faille CVE-2018-13379 pour laquelle un correctif existe depuis mai 2019 (les équipements n'ont pas été mis à jour depuis 1 an et demi alors que la faille a été médiatisée).

3.4 L'attaque Orion SolarWinds et les attaques par la Supply-chain

Annoncée le 13/12/2020, l'attaque au moyen du logiciel Orion de la société SolarWinds sera sans doute mieux comprise en 2021 lorsque plus d'éléments seront disponibles. Mais il est déjà certain que cette attaque met au premier plan un risque que nous avons déjà évoqué dans nos bilans annuels (voir nos bilans 2018 et 2019) : les attaques via un fournisseur (à l'insu de ce dernier).

L'attaquant (supposé russe) a commencé par s'introduire dans le système informatique de la société SolarWinds et a modifié la chaine de fabrication du logiciel Orion pour y ajouter une backdoor (baptisée Sunburst). Les versions piégées d'Orion ont ainsi été distribuées par SolarWinds à tous les clients qui ont appliqués les mises à jour officielles du produit. L'attaquant s'est ensuite introduit au moyen de Sunburst chez certains organismes (les plus intéressants pour lui) utilisant ce logiciel Orion, et en

particulier des agences gouvernementales des Etats-Unis et des sociétés américaines à la pointe dans le domaine cyber (par exemple FireEye et Microsoft).

Ce n'est pas la première fois que l'on voit une attaque où un logiciel légitime est piégé sur le site officiel de son éditeur. On peut citer par exemple NotPetya en 2017 (piégeage du logiciel MeDoc, attaque supposée russe), ou CCleaner en 2017 (piégeage du logiciel CCleaner, attaque supposée chinoise). **Par contre l'attaque SolarWinds va sans aucun doute servir d'exemple, et cette forme d'attaque va se développer et intéresser de plus en plus de nouveaux groupes d'attaquants.**

Les différents types d'attaques via les fournisseurs :

Il faut noter qu'il existe plusieurs formes d'attaque via les fournisseurs et quelles ont des niveaux de maturité et de risque différents :

- le piégeage de matériel (qui avait été évoqué par exemple en 2018 pour les cartes mères SuperMicro). Ce type d'attaque n'a jamais été démontré pour une attaque de grande échelle. Elle suscite beaucoup de craintes au niveau étatique (cf. les inquiétudes liées au déploiement d'équipements pour la 5G), mais constitue plutôt un risque théorique pour ce qui concerne les préoccupations des entreprises. Nota : le piégeage de matériel est par contre déjà utilisé, et depuis longtemps, pour des attaques très ciblées sur quelques individus (par des services secrets ou la grande criminalité). Mais dans ce cas, il ne s'agit plus vraiment d'une attaque par un fournisseur.
- le piégeage de logiciels (comme pour l'attaque SolarWinds). Ces attaques ont déjà été vues et l'exemple donné par SolarWinds va sans doute être repris par d'autres, d'abord pour des attaques étatiques, mais aussi ensuite pour des attaques cybercriminelles. **Le cas SolarWinds est le signal d'un risque qui est en augmentation et qu'il va falloir traiter.**
- le rebond via un fournisseur ou un partenaire. Ces attaques sont déjà courantes, aussi bien au niveau des attaques étatiques (par exemple l'attaque chinoise **Cloud Hopper** en 2017) que cybercriminelles (par exemple l'attaque des magasins **Target** en 2013).

• Les cibles de ces attaques sont souvent les sociétés les mieux protégées

L'attaque par piégeage du logiciel d'un fournisseur est très puissante parce que la victime ne peut pas la détecter avant d'avoir installé ce logiciel. Elle contourne tous les mécanismes de protection (elle pourra cependant être détectée si elle déclenche des alarmes lors de l'exploration du réseau interne de la victime). Par contre elle est complexe à mettre en œuvre pour l'attaquant. Elle ne sera probablement utilisée que s'il n'existe pas de méthode plus simple pour l'attaquant de compromettre le réseau de la victime.

Si le risque d'attaque est réel (et démontré), il ne constitue donc probablement pas encore une priorité pour la plupart des entreprises. Jusqu'à présent, il y a peu d'études sur les méthodes pour réduire ce risque, mais il est clair que ce sujet va maintenant être exploré activement. La surveillance du réseau interne, de façon à identifier des comportements suspects, est sans doute un des éléments de la réponse technique.

• Une attaque sophistiquée visant le Cloud Office 365

Un autre élément mis en évidence par l'attaque SolarWinds est l'attaque de l'environnement Cloud Office 365 (offre rebaptisée Microsoft 365 en 2020). Les investigations publiées jusqu'à présent montrent qu'une fois entrés dans les entreprises, les attaquants ont cherché à accéder aux informations stockées dans Office 365 et en particulier aux emails. Pour ce faire ils ont volé la clé de signature SAML (ou dans certains cas ajouté une nouvelle clé de signature) de façon à pouvoir générer des tokens d'authentification SAML valides. Une fois ce but atteint, l'attaquant peut accéder à l'espace Office 365 de l'entreprise depuis n'importe où sur le réseau interne, mais aussi depuis l'extérieur de l'entreprise. Ces attaques SAML et OAUTH mises en œuvre ici sont plutôt nouvelles et font parties des évolutions techniques notées pour 2020 (cf. § 3.7.2).

3.5 Les attaques DDOS

Fin août et début septembre 2020, une vague d'attaques DDOS visant des entreprises a été observée un peu partout dans le monde. La presse a signalé par exemple l'attaque de la bourse en Nouvelle Zélande, ou d'opérateurs télécom en France, Belgique et aux Pays-Bas. Mais de nombreux autres cas, avec le même mode opératoire, n'ont pas été rendus publics. Ces attaques ont été accompagnées d'emails de menaces qui demandaient le versement d'une rançon en Bitcoins pour éviter de nouvelles attaques. Les attaquants se présentaient comme faisant partie de groupes réputés comme FancyBear (groupe Russe de cyber espionnage aussi connu sous le nom APT28), Lazarus (groupe nord-coréen) ou Armada Collective (groupe connu dans les années 2016 pour ses attaques DDOS), mais ce n'est probablement pas vrai. Les attaques de démonstration ont repris en fin d'année (et début 2021) et les attaquants ont à nouveau fait du chantage auprès des cibles qui n'avaient pas payé en septembre. Globalement, l'attaquant s'est montré très opportuniste (il changeait de cible rapidement si son interlocuteur ne réagissait pas) et plutôt maladroit dans sa communication.

Nota : Le Cert-IST a émis la note **INFO-2020.027** en septembre 2020 à propos de ces attaques.

Les attaques DDOS ne sont pas une nouveauté et elles se produisent de façon régulière sur Internet. Mais cette campagne DDOS visant les entreprises est quand même notable. Elle montre que :

- Les attaquants cherchent tous les moyens pour faire pression sur les entreprises. On peut se demander si ces attaques DDOS n'ont pas été inspirées par le succès des attaques ransomware.
- Des groupes apparemment relativement peu aguerris peuvent facilement mener des attaques de 150 Gbps.
- Les protections DDOS (le plus souvent en s'appuyant sur un prestataire de service anti-DDOS) semblent de plus en plus nécessaires pour faire face à cette menace.

3.6 Les attaques étatiques de plus en plus sophistiquées

Si 2020 a été l'année des attaques cybercriminelles au moyen de ransomware (cf. § 3.2), il ne faut pas négliger les attaques étatiques. Deux attaques 2020 sont particulièrement intéressantes.

• Les attaques « Copy/Paste », supposées chinoises, contre l'Australie

Le gouvernement australien a annoncé mi-juin 2020 que l'Australie avait été l'objet récemment d'attaques de grandes ampleurs visant tous les secteurs d'activité et provenant d'un attaquant étatique.

Cet attaquant n'a pas été nommé mais beaucoup pensent qu'il s'agit de la Chine. Pour ces attaques, l'ACSC (Australian Cyber Security Center) a publié un document technique intitulé : Copy-paste compromises – TTP used to target multiple Australian networks.

L'Australie ne considère pas ces attaques comme sophistiquées parce que les programmes d'attaques utilisés sont directement dérivés d'exploit qui avaient été publiés sur Internet. C'est pour cela qu'il qualifie ces attaques de « Copy-paste ».

Ces attaques sont cependant intéressantes car elles montrent le professionnalisme de l'attaquant dans son exécution d'une attaque : l'attaque est méthodique, progressive et elle exploite toutes les techniques connues.

Par exemple, pour la phase de Spear-phishing (qui n'est utilisée par l'attaquant que lorsque l'intrusion directe via un serveur vulnérable n'a pas été possible), l'attaquant essaye successivement des techniques de plus en plus avancées :

- Phishing classique avec un mail incitant la victime à visiter une page où elle devra saisir son compte et mot de passe,
- Puis envoi d'un mail avec pièce jointe piégée,
- Puis envoi d'un phishing utilisant la technique OAUTH (cf. § 3.7.2)
- Et si tout a échoué, envoi de mails utilisant des services d'email-tracking pour observer sur quel type de contenus la victime est susceptible de cliquer. Cette technique est sans doute utilisée pour identifier les sujets d'intérêts de la victime et préparer de nouvelles tentatives de Spear-phishing.

Le Top 25 des attaques chinoises :

Un autre document intéressant à propos des attaques étatiques chinoises a été publié en octobre 2020 par la NSA. Il s'agit de la liste des 25 vulnérabilités utilisées par les chinois lors des cyber-attaques.

Cette liste est intéressante parce que bien qu'elle ne contienne aucune vulnérabilité 0days, elle contient uniquement des vulnérabilités très récentes (la majorité de 2020). Cela montre que l'attaquant est à l'affut des nouvelles attaques publiées sur Internet et qu'il sait les industrialiser rapidement.

• L'attaque SolarWinds, supposée Russe, contre les Etats-Unis

Cette attaque (déjà évoquée au paragraphe 3.4) est remarquable par son niveau de sophistication technique. Selon plusieurs sources c'est l'attaque la plus sophistiquée aujourd'hui sur l'aspect de l'OPSEC (la sécurité opérationnelle), c'est-à-dire que beaucoup d'efforts ont été déployés pour empêcher de détecter l'attaque, de faire des recoupements avec d'autres attaques, et de remonter vers l'attaquant. Par exemple, autant que faire se peut, le même indice (par exemple une adresse IP, un exécutable, etc.) n'a jamais été utilisé deux fois dans l'opération.

On savait déjà que les attaques les plus avancées sont aujourd'hui celles menées par quelques états. Ils sont pionniers dans les nouvelles techniques d'attaques et sont souvent par la suite imités par

d'autres états ou par les cybercriminels. Ces 2 attaques (Chinoises et Russes) montrent à nouveau que la maitrise des opérations de cyber-attaques des états atteint un niveau jusqu'à présent inégalé par les autres attaquants.

3.7 Les évolutions techniques observées en 2020

Nous regroupons dans ce chapitre des faits techniques qui sont apparus ou se sont renforcés au cours de l'année 2020. Ils montrent l'évolution technique des attaques et les points à surveiller. Globalement ces éléments concernent plutôt les serveurs d'infrastructures, que les postes de travail. Le poste de travail (et le phishing visant les utilisateurs) a été longtemps la cible préférée des attaquants. Il semble que désormais les attaques visant les serveurs reviennent dans l'actualité.

3.7.1 Les Attaques visant Exchange, SharePoint et IIS

Nous avons observé en 2020, une augmentation des attaques visant les solutions Microsoft Exchange, SharePoint et IIS (le serveur web de Microsoft).

• Exchange : une cible de choix pour les attaquants

Le serveur Exchange est depuis longtemps une cible convoité par les attaquants. Il permet d'accéder aux mails des utilisateurs (voir par exemple l'outil MailSniper publié en 2016 pour explorer les mails d'un serveur Exchange), mais aussi d'installer une backdoor permettant à l'attaquant de revenir si son accès principal a été découvert (voir par exemple la backdoor LightNeuron utilisée depuis 2014 par le groupe russe Turla).

En 2020, Exchange a été aussi l'objet d'attaques directes ayant pour but de rentrer dans l'entreprise visée. Deux composants d'Exchange sont utilisés lors de ces attaques :

- **Les cmdlet Exchanges** : Les cmdlets sont des fonctions Exchange appelables à distance au moyen de scripts PowerShell. Elles permettent de réaliser des opérations à distance sur un serveur Exchange. Plusieurs vulnérabilités ont été découvertes en 2020 sur certains cmdlets. Ces vulnérabilités permettent à un utilisateur ayant un compte Exchange d'exécuter des actions avec des privilèges élevés (privilèges SYSTEM en général) sur le serveur Exchange.
- **Les API web** : Il existe plusieurs services web permettant d'accéder à des fonctions Exchange au travers une interface web, par exemple ECP (Exchange Control Panel), EWS (Exchange Web Service) ou OWA (Outlook Web Access). Ces API peuvent permettre de réaliser des attaques visant les cmdlets (vulnérabilités vues ci-dessus) ou des attaques visant le serveur web IIS qui héberge ces API (en particulier les attaques VIEWSTATE, évoquées ci-dessous).

Voici les vulnérabilités Exchanges les plus marquantes pour 2020 :

- **CVE-2020-0688** (avis **CERT-IST/AV-2020.0173** et alerte **CERT-IST/AL-2020.004**) : Exchange utilise par défaut une MachineKey connue, ce qui rend possible les attaques VIEWSTATE sur le serveur IIS utilisé par Exchange. Cette vulnérabilité permet à un utilisateur Exchange de prendre le contrôle du serveur IIS via le service ECP.

- **CVE-2020-16875** (avis **CERT-IST/AV-2020.1236**) : une vulnérabilité du cmdlet New-DlpPolicy permet à un utilisateur ayant un compte Exchange, via l'interface web ECP ou un script PowerShell, d'exécuter un code arbitraire sur le serveur Exchange avec les droits SYSTEM.
- **CVE-2020-17083** (avis **CERT-IST/AV-2020.1583**) : une vulnérabilité du cmdlet Export-ExchangeCertificate permet à un utilisateur ayant un compte Exchange, via un script PowerShell, d'exécuter un code arbitraire sur le serveur Exchange avec les droits SYSTEM

Microsoft est bien conscient de cette tendance et a publié en juin 2020 un article de blog sur les attaques visant Exchange : Defending Exchange servers under attack.

• SharePoint : moins d'attaques qu'Exchange mais très convoité

La vulnérabilité CVE-2019-0604 dans SharePoint avait été un fait marquant de 2019 (cf. notre alerte **CERT-IST/AL-2019.006** de mai 2019). Elle avait été utilisée en particulier dans des attaques ChinaChopper (supposées chinoises).

En 2020 les nouvelles vulnérabilités SharePoint ont donc été scrutées attentivement par les attaquants, pour voir si elles pouvaient également être utilisées. Contrairement à CVE-2019-0604, toutes les vulnérabilités publiées en 2020 nécessitent un compte SharePoint pour pouvoir être utilisées. Par contre ces vulnérabilités restent graves puisqu'elles permettent de prendre le contrôle du serveur SharePoint. On notera en particulier : CVE-2020-17017 (**CERT-IST/AV-2020.1572**), CVE-2020-16951 et CVE-2020-16952 (**CERT-IST/AV-2020.1423**), CVE-2020-1147 (**CERT-IST/AV-2020.0938**) et CVE-2020-1181 (**CERT-IST/AV-2020.0764**). La plupart de ces vulnérabilités permettent de lire des fichiers systèmes, ce qui permet ensuite de réaliser des attaques VIEWSTATE contre le serveur IIS de SharePoint.

• IIS : au cœur des solutions Microsoft

Le serveur web IIS est une brique de base utilisée dans de nombreux produits Microsoft comme par exemple SharePoint ou Exchange. Beaucoup des attaques SharePoint ou Exchange cherchent en fait à atteindre le serveur IIS, en particulier pour réaliser des attaques VIEWSTATE contre IIS.

La multiplication de ces attaques nous a amené à publier dans notre bulletin mensuel de juillet 2020 un article sur le VIEWSTATE et sur comment le sécuriser. En bref, le VIEWSTATE est un champ caché inséré dans les pages web de IIS. Ce mécanisme (de la technologie ASP.NET) est vulnérable aux attaques par dé-sérialisations si l'attaquant a pu voler la clé MachineKey stockée dans le fichier web.config. Le vol de ce fichier permet donc ensuite à l'attaquant d'exécuter du code arbitraire sur le serveur web IIS.

Nota : IIS a également été beaucoup attaqué au travers de vulnérabilités de la librairie tierce TelerikUI de la société Telerik.com.

3.7.2 Les attaques des authentifications SAML ou OAUTH

Il s'agit là d'une autre tendance de l'année 2020. Voici quelques événements qui la mettent en évidence :

- Les attaques de phishing utilisant OAUTH (cf. l'encadré ci-dessous) deviennent courantes. Elles ont été vues dans des attaques étatiques (les attaques supposées chinoises qui ont visé l'Australie au 2eme trimestre 2020) et utilisées par un groupe TA2552 spécialisé dans le phishing.
- Nous avons émis en juillet une alerte (**CERT-IST/AL-2020.**007) pour une vulnérabilité SAML (cf. CVE-2020-2021 et notre avis **CERT-IST/AV-2020.0868**) dans les équipements de Palo Alto Networks. Elle permet de se connecter illégalement grâce à des authentifications SAML falsifiées.
- L'US-CERT et la NSA alertent en décembre sur des attaques russes utilisant la technique du **Golden SAML**. Il s'agit des attaques SolarWinds, mais aussi d'attaques antérieures visant VMWare Workspace One Access

Extrait de l'article publié dans le bulletin de septembre 2020

Les phishing OAUTH :

Cette technique gagne en popularité. Elle consiste, plutôt que de demander son login et son mot de passe à la victime, à lui présenter une fenêtre OAUTH lui demandant d'autoriser une Apps à accéder à son compte Office 365. Cette technique a été vue la première fois en 2015 (voir cet article Trend Micro sur Pawn Storm). Il existe des toolkits open-source implémentant ces attaques (PwnAuth de FireEye depuis juin 2019, et O365-attack de MDsec.co.uk depuis juin 2020). Elle a été utilisée en juin 2020 dans les attaques APT ayant visées l'Australie. Et Proofpoint indique fin septembre 2020 que le groupe TA2552 l'utilise dans ses attaques de phishing.

Evolution du nombre d'avis Cert-IST citant les termes OAUTH et SAML

	Oauth	SAML
2020	8	7
2019	0	12
2018	4	8
2017	1	4
2016	2	1
2015	3	1

Les attaques SAML et OAUTH vues en 2020 visent les environnements Cloud Office 365. Cette tendance devrait se maintenir dans les années à venir puisque contourner les mécanismes d'authentification est un bon moyen d'obtenir un accès aux ressources hébergées dans le Cloud.

3.7.3 L'outil d'attaque Cobalt-Strike

Cobalt Strike est un outil commercial vendu pour réaliser des exercices d'attaques. Il s'agit d'un outil offensif, comme peuvent l'être Metasploit, Immunity Canvas ou Core Impact.

Il existe sur Internet des versions piratées de Cobalt Strike et **en 2020, Cobalt Strike est devenu l'outil le plus utilisé dans des attaques réelles**. Il a été vu de nombreuses fois dans des attaques de ransomware, mais aussi quelque fois dans des attaques étatiques (par exemple l'attaque SolarWinds).

Selon une étude publiée début 2021 par Recorded Future, Cobalt Strike serait l'outil offensif le plus utilisé pour manipuler à distance des machines infectées (devant Metasploit et PupyRAT).

3.7.4 L'attaque ZeroLogon

Apparue en septembre 2020, l'attaque ZeroLogon exploite une vulnérabilité du service Netlogon de Windows et permet à un attaquant ayant déjà obtenu un accès dans une entreprise, de prendre le contrôle complet d'un domaine Microsoft.

ZeroLogon est désormais la méthode la plus simple pour un attaquant d'élever ses privilèges et de prendre le contrôle de l'Active Directory d'une entreprise, si celle-ci n'a pas appliqué les correctifs diffusés par Microsoft en août 2020 (la faille a été corrigée avant d'être rendue publique). Elle a déjà été très souvent utilisée dans des attaques et constitue à ce titre un événement important de l'actualité de l'année 2020. Par contre elle ne constitue pas une avancée technique marquante de l'année et ne devrait pas avoir de conséquence à plus long terme.

Nota : A propos de ZeroLogon, le Cert-IST a émis l'avis **CERT-IST/AV-2020.1101** en août 2020 (pour décrire les correctifs Microsoft), l'alerte **CERT-IST/AL-2020.010** en septembre (pour avertir des premières attaques). Nous avons ensuite tenu au courant de l'évolution de cette menace au travers du blog [Microsoft Zerologon] dans le Hub de Crise (HdC) Cert-IST.

4 Productions du Cert-IST en 2020

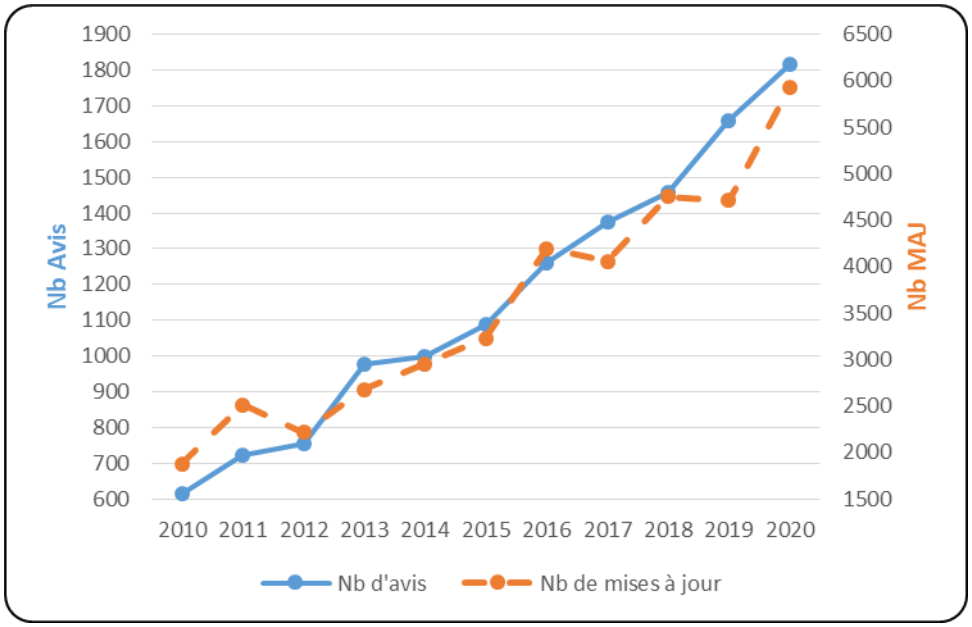
4.1 Veille sur les vulnérabilités et les menaces

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.

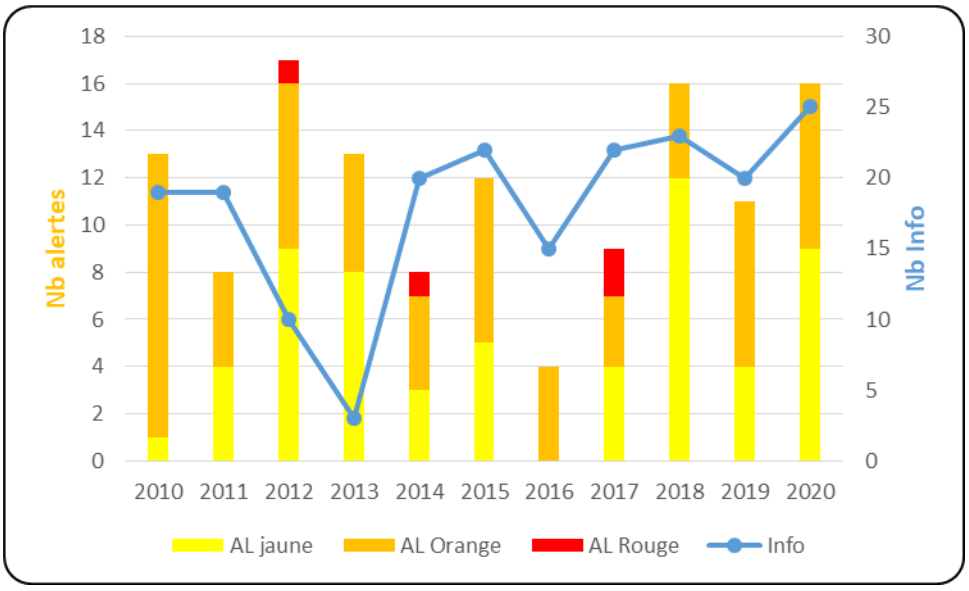
Le Cert-IST émet ainsi plusieurs types de publications :

- **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).

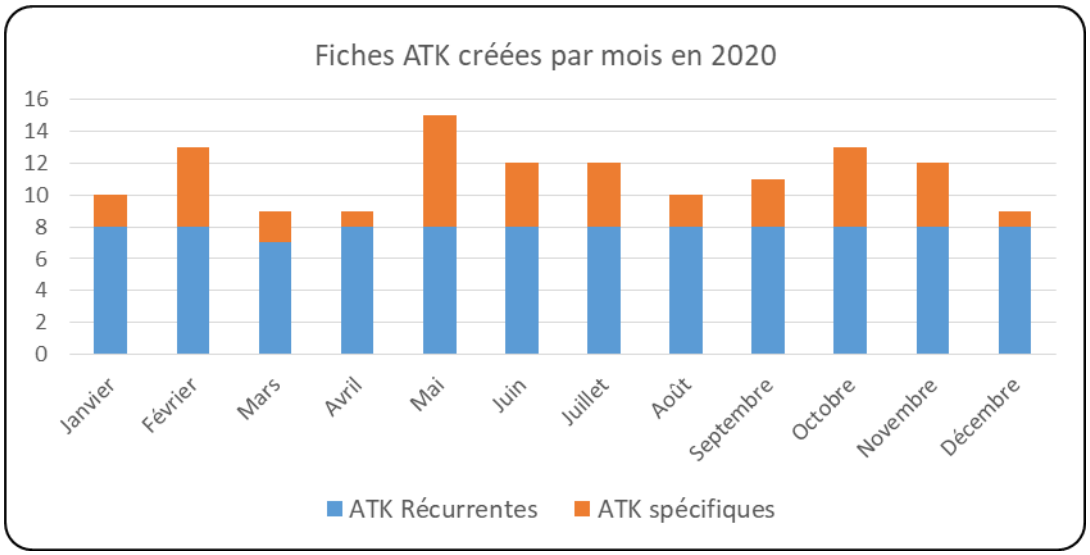
Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.



Nombre d'avis de sécurité publiés par an



Nombre d'alertes publiées par an



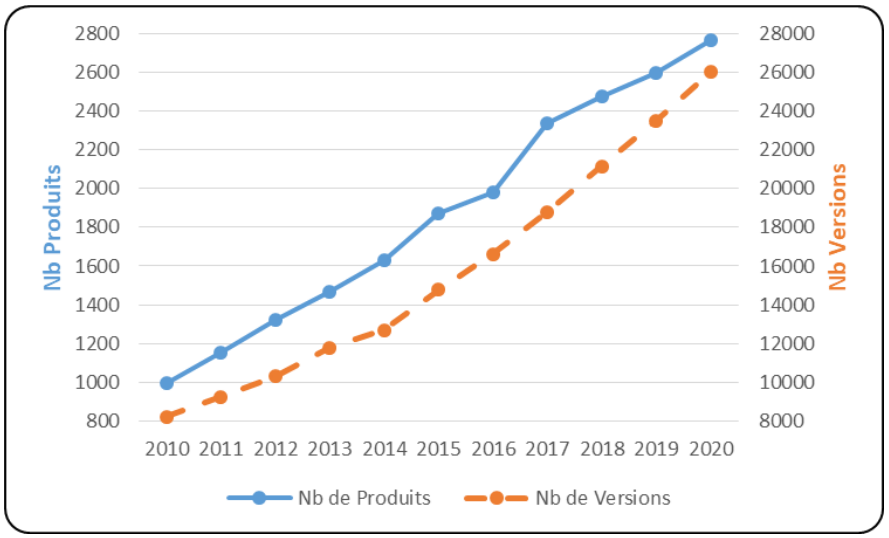
Nombre de fiches attaques publiées par mois

Ainsi, en 2020, le Cert-IST a publié :

- **1 818** avis de sécurité (dont **79** avis SCADA), **5 827** mises à jour mineures et **103** mises à jour majeures.
  Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec en 2020 une augmentation de **9%** par rapport à 2019. 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 **25** 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.
- **135** fiches attaques ont été publiées en 2020, avec dans la base de données MISP **2 884** évènements qui ont été enrichis, et **1 209 983** marqueurs (IOC) ajoutés (au total il y a **4,5 millions** de marqueurs dans la base).

Concernant les produits et les versions suivis par le Cert-IST, fin 2020 le Cert-IST suivait **2 764** produits et **26 021** versions de produits. Le graphique suivant montre l'évolution du nombre des produits et des versions qui sont suivis par le Cert-IST.



4.2 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.

5 Conclusions

• La crise du Covid-19 a exposé les entreprises à un risque accru d'attaque

L'année 2020 est avant tout l'année de la crise du Covid-19. Dans les entreprises, les mesures de confinement ont imposé une adaptation rapide et radicale de l'environnement de travail. Beaucoup ont dû mettre en place ou généraliser le télétravail, au prix parfois d'une exposition accrue aux risques d'incidents de sécurité informatiques (intrusion ou fuite de données). Comme nous le détaillons au paragraphe 3.1, il y a eu une augmentation du nombre des attaques classiques (campagnes de mails piégés, escroqueries via le web) parce que tous les attaquants ont cherché à profiter de la crise. Il est possible aussi (mais on manque encore de recul sur cet aspect) que les outils mis en place pour le télétravail aient permis un accroissement des attaques par rebond (attaques visant le salarié en télétravail pour rentrer dans son entreprise).

A notre connaissance il n'existe pas encore de cas connu d'incident grave formellement attribué aux mesures techniques mises en place pendant le Covid-19. Il est certain par contre que beaucoup ont fait au mieux, et se sont exposés à un risque accru d'intrusion. Il est donc important de limiter la durée de cette période de vulnérabilité.

• 2020 : année record pour les attaques de ransomware

Nous avions conclu l'an dernier notre bilan sur la montée en flèche inquiétante des attaques des ransomwares visant les entreprises, et 2020 a confirmé cette crainte : les attaques ont continué à se multiplier et constituent le phénomène le plus marquant de 2020). Les attaquants ont multiplié les moyens de pressions (cf. § 3.2) et ont montré une fois de plus qu'ils forment une économie souterraine structurée ou chacun est rétribué en fonction des services qu'il rend.

Les attaques par ransomware et le vol de données au sein des entreprises est un marché lucratif. Cela attire de plus en plus de cybercriminels. Pour endiguer cette vague de ransomwares, il faudrait sans doute une réponse judiciaire plus efficace, avec des opérations internationales de démantèlement comparable à ce qui a déjà été vu pour certains Botnets (Trickbot en novembre 2020, Emotet en janvier 2021, etc.). Il semble aussi qu'une fois entrée dans l'entreprise, il soit parfois facile pour le pirate de se déplacer dans l'entreprise, de prendre le contrôle de l'Active Directory et de rester ensuite plusieurs semaines ou mois sans être détecté. Ce constat inquiétant montre qu'il faut renforcer la capacité de détection des comportements anormaux à l'intérieur du réseau (voir ci-dessous).

• L'attaque SolarWinds démontre la capacité offensive avancée de certains états

L'attaque au travers du logiciel Orion de SolarWinds annoncée en décembre 2020 par les Etats-Unis (les victimes connues jusqu'à présent sont des organismes gouvernementaux et des entreprises américaines) est exceptionnelle, par son ampleur et sa sophistication.

La technique d'attaque (infection d'un logiciel chez son fournisseur), met le sujet des attaques au moyen des fournisseurs (supply-chain attack) au centre des préoccupations. Il s'agit cependant d'une attaque complexe qui est surtout intéressante lorsque l'attaquant vise une cible difficile à atteindre avec une attaque directe, ou s'il veut toucher un grand nombre de cibles (cas où le produit piégé est très utilisé).

Bien qu'il constitue une menace réelle, la protection contre ces attaques sera donc sans doute une priorité uniquement pour les organisations les plus avancées en sécurité.

Nota : Nous parlons ici du cas du piégeage d'un logiciels, qui est l'une des 3 formes d'attaques via les fournisseurs (cf. paragraphe 3.4 ; les autres sont le piégeage matériel et l'intrusion via les réseaux du fournisseur).

Ce que montre enfin l'attaque SolarWinds c'est la complexité de l'analyse d'un incident de ce type : c'est une attaque furtive (l'attaquant cherche à limiter les traces) découverte plus de 10 mois après l'intrusion initiale et visant en particulier les ressources Cloud de l'entreprise (Microsoft Office 365, environnement très dynamique et en mutation rapide, et donc complexe). L'analyse d'un tel incident nécessite de disposer de données de supervision (des logs) provenant des différents composants du Système d'Information impacté (passerelles d'accès, postes de travail, environnement Office 365, etc.).

• Les attaques se tournent vers les équipements de bordure (VPN) et vers le Cloud Office 365

En 2020, en plus des attaques traditionnelles visant le poste de travail (attaques par mail ou lors de la navigation Internet) deux tendances sont apparues :

- L'attaque des équipements exposés sur Internet et en particulier des accès VPN (cf. § 3.3),
- L'attaque du cloud Office 365.

• Il faut améliorer les capacités de détection des intrusions

L'actualité de 2020 a montré à nouveau (avec les attaques de Ransomware où les attaques étatiques avancées comme SolarWinds) qu'aucune défense n'est invincible et que l'entreprise doit partir du principe que des attaquants parviendront un jour ou l'autre à rentrer dans le système d'information.

Mais entre l'intrusion initiale et l'atteinte de son objectif, l'attaquant a aussi besoin de temps. Ce temps dépend des défenses qu'il va rencontrer (le niveau de défense en profondeur) et du niveau de furtivité qu'il veut atteindre. Et pendant tout le temps où il sera présent dans l'entreprise, l'attaquant devra faire attention de ne déclencher aucune alarme, qui pourrait attirer l'attention des défenseurs et démarrer une chasse visant à le débusquer.

Ce constat incite à développer d'une part les systèmes d'alarme et d'autre part les procédures de réaction aux alarmes. Cela s'appuie sur des dispositifs de détection spécifiques (par exemple en plaçant des détecteurs dédiés à l'intérieur de l'entreprise : serveurs sentinelles, honeypots, etc.) ou en combinant les événements déjà journalisés (définition d'un comportement anormal) et sur les mécanismes de qualification et de réactions pilotés par les centres de supervision de sécurité (SOC).

Rappel des principes de sécurisation (extrait du bilan Cert-IST 2019) :

- Mettre en place des défenses et cloisonner les architectures en prenant en compte le fait qu'un jour un attaquant parviendra à passer au travers les défenses,
- Maintenir à jour les systèmes en appliquant les correctifs de sécurité,
- Développer les capacités de détection et de réponse aux intrusions.

Association Cert-IST

290 Allée du lac

31 670 Labège

France

info@cert-ist.com

https://www.cert-ist.com

05.34.39.44.88