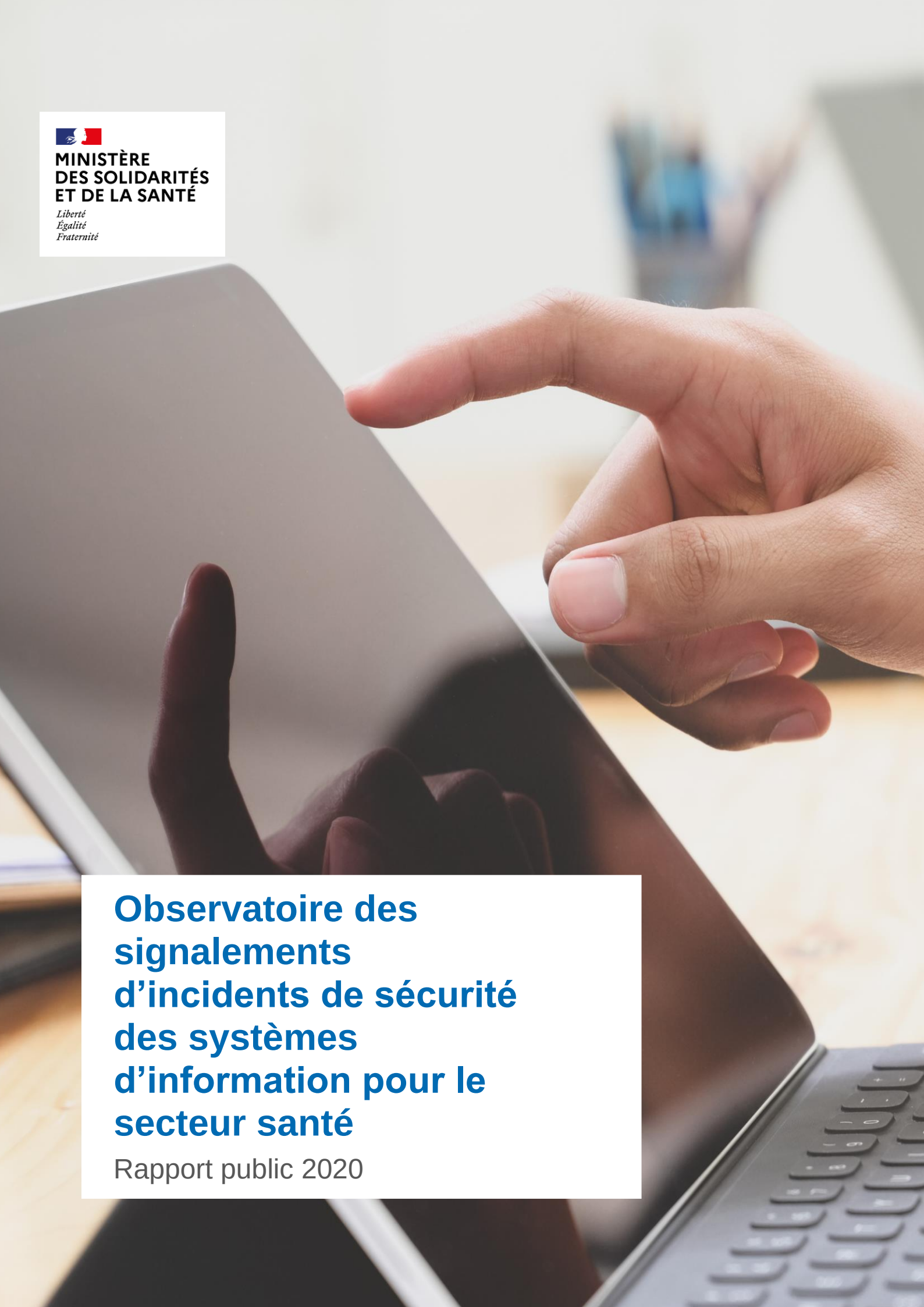
MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité



Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé

Rapport public 2020

SOMMAIRE

TABLE DES FIGURES

1 INTRODUCTION

Le ministère des solidarités et de la santé a mis en place depuis le 1er octobre 2017 un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information des structures de santé.

L'année 2020 a été marquée à la fois par la crise sanitaire COVID-19, qui a mis à dure épreuve notre système de soins, et par une recrudescence de cyberattaques par rançongiciels, visant notamment les établissements de santé. De nombreux établissements ont subi des attaques, avec parfois des conséquences importantes sur la prise en charge des patients. Ainsi, près de quatre cents incidents ont été signalés au ministère des solidarités et de la santé et une centaine de demandes d'accompagnements ont été formulées auprès de la cellule cybersécurité en santé, dédiée à l'appui des structures de santé au sein de l'Agence du numérique en santé (ANS).

La cellule cybersécurité en santé de l'ANS est, depuis 2017, l'interlocuteur privilégié des structures sanitaires et médico-sociales dans le domaine de la sécurité opérationnelle. Elle a intégré début 2021 « *l'InterCERT-FR* » et se positionne comme le CERT de référence pour le secteur de la Santé, avec comme nouvelle dénomination « *CERT Santé* ».

Avec l'appui de l'ANSSI, le CERT Santé a significativement amélioré en 2020 ses services d'appui à la réponse aux incidents et de veille active de la menace de cybersécurité. Au-delà des actions visant à aider les structures à résoudre leurs incidents, le CERT Santé s'attache également à accompagner les structures à titre préventif. Ainsi, 40 GHT ont bénéficié en 2020 du service national de cyber-surveillance et plus de 800 structures ont été alertées d'une vulnérabilité ou d'une compromission potentielle de leur SI.

La déclaration systématique des incidents SSI est un enjeu important pour piloter le niveau de risque, mais aussi pour alerter le secteur en cas de menace nouvelle. Il est donc fondamental que les structures de santé déclarent systématiquement leurs incidents, et le plus tôt possible, afin de bénéficier d'un appui à la mise en œuvre des mesures permettant de réduire les impacts potentiels des actes de cybermalveillance auxquels ils sont confrontés, et d'en freiner la propagation.

Les évènements récents survenus à l'encontre des centres hospitaliers d'Albertville-Moutiers, de Dax ou de Villefranche sur Saône ont montré la nécessité de consolider l'appui aux acteurs, afin d'améliorer leur résilience face à des attaques de plus en plus sophistiquées. Au travers du « *Ségur de la santé* », le ministère a fait le choix d'investir massivement dans la sécurité des systèmes d'information de santé. La montée en puissance du CERT Santé traduit la volonté ministérielle de renforcer les capacités d'accompagnement des structures du secteur, notamment les plus vulnérables.

Dans le cadre de la « *Feuille de route du numérique en santé* », l'ensemble des acteurs du secteur se mobilise pour accompagner le développement du numérique en santé et renforcer la confiance dans ses usages. La sensibilisation et la formation sont des leviers importants pour faire progresser la maturité du secteur en matière de prévention et de bonnes pratiques en cybersécurité. En coordination étroite avec l'ANSSI, le CERT Santé joue un rôle central dans l'animation sectorielle, en vue de favoriser la coopération et l'entraide entre les acteurs, accompagner leur montée en compétence et contribuer à l'amélioration du niveau de résilience collective.

Etienne Champion
Secrétaire général des ministères sociaux
Haut fonctionnaire de défense et de sécurité

2 DISPOSITIF DE TRAITEMENT DES SIGNALEMENTS DES INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION POUR LE SECTEUR SANTE

2.1 Contexte réglementaire

En application de l'article L. 1111-8-2 du code de la santé publique, les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale doivent déclarer leurs incidents de sécurité des systèmes d'information depuis le 1er octobre 2017. Depuis le 18 novembre 2020, cette obligation a été étendue aux établissements médico-sociaux par ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé (ARS).

Dans le cadre de la mise en application du décret n° 2016-1214 du 12 septembre 2016 (JORF n°0214 du 14 septembre 2016) relatif aux conditions de traitement des incidents graves de sécurité des systèmes d'information du secteur santé, l'Agence du numérique en Santé (ANS) est désignée comme le groupement d'intérêt public (GIP) en charge d'apporter un appui au traitement des incidents de sécurité des systèmes d'information.

L'arrêté d'application du 30 octobre 2017 relatif aux modalités de signalement et de traitement des incidents précise le rôle des ARS et de l'ANS dans le traitement des signalements et l'accompagnement des structures.

Le décret d'application de l'article L.1111-8-2 modifiée par l'ordonnance du 18 novembre précisera le rôle et les missions de l'ANS dans le dispositif étendu aux services médico-sociaux, en particulier son périmètre d'intervention en matière d'appui à la réponse à incident et les actions de prévention.

2.2 Présentation des activités

Le dispositif de traitement des signalements des incidents de sécurité des systèmes d'information constitue un élément clé de la stratégie d'amélioration du niveau de sécurité numérique du secteur santé portée par le ministère des solidarités et de la santé, en coordination étroite avec les autorités gouvernementales en charge de la cyber sécurité.

Sa mise en œuvre opérationnelle s'appuie sur la Cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) de l'Agence du numérique en santé. La cellule ACSS a mis en place une démarche méthodique pour améliorer la résilience des structures face aux actes de cybermalveillance.

La Cellule ACSS change de nom en 2021 pour devenir le **CERT Santé**. Elle est désignée comme telle dans la suite du document.

La Cellule ACSS a intégré l'InterCERT-FR en janvier 2021. Cette étape importante pour la reconnaissance des activités de la Cellule ACSS – CERT Santé confirme le positionnement de l'ANS comme acteur principal dans le domaine de la sécurité du numérique en santé et dans la stratégie d'appui opérationnel du ministère de la santé aux structures de santé dans la réponse aux incidents de cybersécurité.

En intégrant l'InterCERT-FR, la Cellule ACSS bénéficie des retours d'expérience et de la coopération avec les autres CERT/CSIRT[1] en vue d'améliorer ses services au profit des secteurs sanitaire et médico-social. Cela contribuera à augmenter la confiance des structures dans ses capacités à leur apporter un appui.

Mise à disposition d'un portail de signalement et proposition d'un appui

Le traitement des incidents reste de la responsabilité des structures de santé. L'accompagnement et l'appui mis en place par le CERT Santé dans le cadre de leur signalement consiste à :

- Traiter le signalement sur le portail des signalements des évènements sanitaires indésirables et notifier au déclarant sa prise en compte ;
- Analyser et qualifier le signalement pour le compte des autorités compétentes;
- Apporter, si besoin, un accompagnement dans le traitement de l'incident de sécurité des systèmes d'information ;
- Diffuser une alerte vers le ministère des solidarités et de la santé et/ou les autorités compétentes de l'Etat selon la nature de l'incident :
  - le fonctionnaire de sécurité des systèmes d'information des ministères sociaux (FSSI), qui assure le pilotage du traitement en cas d'incident de sécurité majeur ;
  - la direction générale de la santé (DGS) via le CORRUSS (Centre opérationnel de réception et de régulation des urgences sanitaires et sociales), dans le cas d'un incident ayant un impact sanitaire ;
  - aux agences sanitaires dans le cas d'un incident majeur impactant la prise en charge des patients ;
  - à l'ANSSI, en cas d'incident concernant une structure relevant de dispositifs spécifiques (OIV ou OSE), ou en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
  - à terme, à la CNIL en cas d'impact sur les données à caractère personnel.

La CERT Santé apporte son appui aux structures dans le cadre de la réponse à un incident :

- Mise à disposition de fiches réflexes (ex : maliciel, hameçonnage ou défiguration de site Web) ou de recommandations de mesures de remédiation correspondant à la nature de l'incident (ex : changement de mots de passe, mise en liste noire d'adresses de messagerie, blocage de protocoles) ;
- Proposition des mesures de confinement complémentaires au cours d'un premier entretien (isolation de l'Active Directory[2], désactivation massive de comptes, etc…) ;
- Assistance à l'identification de la menace et le scénario complet de la compromission (acquisition et analyse de journaux d'évènements et de preuves numériques, analyse de codes malveillants, de fichiers infectés, recherche du « patient 0 » de l'attaque, etc…) ;
- Proposition de mesures de remédiation adaptées (désinfection des systèmes compromis, suppression des fichiers malveillants, correction des vulnérabilités exploitées, etc…) ;

[1]Un **computer emergency response team** (**CERT**) ou **computer security incident response team** (**CSIRT**) est un centre de veille, d'alerte et de réponse aux attaques informatiques, centré sur un secteur d'activité spécifique ou une entreprise.

[2] L'**Active Directory** (**AD**) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

- Orientation vers un prestataire de proximité référencé par le GIP cybermalveillance.gouv.fr dans le cas d'une demande d'intervention sur site.

Le CERT Santé propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité :

- Proposer et émettre un avis sur des plans d'action sécurité :
  - priorisation des mesures proposées (ex : renforcer le cloisonnement réseau du SI support d'activités de soins vitaux) ;
  - propositions pour améliorer la sécurité du SI (ex : utilisation d'une application pour l'administration locale ou pour limiter l'exploitation de vulnérabilités) ;
- Rappeler des bonnes pratiques de cloisonnement réseau (ex : promotion des guides de l'ANSSI sur la configuration d'un domaine Active Directory).

Une fiche de présentation de l'accompagnement à la réponse à incident est disponible sur le portail cyberveille-santé :
https://cyberveille-sante.gouv.fr/sites/default/files/documents/ACSS_Accompagnement_Reponse_Incident.pdf

Animation de la communauté « cyberveille-santé »

Le portail cyberveille-santé dispose également d'un espace sécurisé au sein duquel les correspondants cyberveille-santé du CERT Santé peuvent échanger entre eux sur :

- Des retours d'expérience sur le traitement d'incidents rencontrés et des indicateurs sur les actes de cybermalveillance ;
- Les bulletins de sécurité ou les documents publiés sur le portail ;
- Les actions ministérielles visant à encadrer et à accompagner les acteurs dans la mise en œuvre de la sécurité numérique.

Cet espace sécurisé a vocation à faciliter les échanges autour de la cybersécurité entre les acteurs du secteur santé.

Le CERT Santé organise un webinaire trimestriel sur les menaces de cybersécurité (attaques à partir de l'Internet, rançongiciels, etc…), sur ses services d'appui (réponse à incident, prévention) et les bonnes pratiques pour renforcer la sécurité des systèmes numériques (protection contre les maliciels, cloisonnement, etc…).

Alerte des structures de la menace cyber

Au travers du portail cyberveille-santé dédié à la sécurité du numérique en santé, le CERT Santé, en coordination étroite avec le centre gouvernemental CERT-FR de l'ANSSI :

- Informe et alerte les structures de santé concernant des vulnérabilités ou des dysfonctionnements majeurs de dispositifs médicaux, des technologies de santé ou des technologies standards (système d'exploitation, suite bureautique, base de données, etc.…) ;
- Alerte les structures de santé concernant des actes de cyber-malveillance (messages électroniques malveillants, rançongiciels, vols de données, etc…) ;
- Apporte un appui aux structures dans la gestion de la sécurité et des incidents (fiches réflexes, fiches pratiques, guides de bonnes pratiques).

Améliorer la sécurité de la messagerie

L'utilisation de courriels malveillants (technique de l'hameçonnage) est très développée par les attaquants pour chercher à compromettre un SI. Le CERT Santé propose aux structures de tester les règles de sécurité de leur serveur de messagerie avec un service en ligne. Ce service a pour but d'identifier les améliorations à apporter dans la configuration des règles de sécurité de la messagerie pour réduire le risque de manipulation de contenus malveillants par les utilisateurs. Il permet de vérifier que la politique de contrôle des messages et de leur contenu a pris en compte les principales menaces issues de l'émetteur, de métadonnées du message (en-tête, encodage, découpage en plusieurs parties, etc…), d'une pièce jointe (spam, virus, etc…), d'une URL (hameçonnage), etc. … Le service contient plus de 170 points de contrôle.

Les activités de prévention menées dans le cadre du service national de cyber-surveillance et de la veille proactive sont présentées en 4.5.

3 Synthèse des incidents déclarés en 2020

En 2020, 250 établissements ont déclaré 369 incidents, soit une baisse d'environ 6% par rapport à 2019. *Cette baisse des déclarations pourrait être liée à la gestion de la crise COVID-19*. Le taux de déclaration reste donc toujours faible au regard du nombre de structures concernées par l'obligation de déclaration[3]. Cependant, les structures déclarent de plus en plus leurs incidents d'origine malveillante, surtout lorsqu'il y a un impact avéré ou potentiel sur l'organisation des soins, ce qui atteste de leur bonne compréhension du dispositif mis en place.

La hausse des actes de cybermalveillance dans le secteur santé se confirme en 2020, en totale cohérence avec la tendance globale. Les incidents d'origine malveillante correspondent à 60% des déclarations reçues par le CERT Santé. La part des incidents d'origine malveillante est en constante augmentation depuis trois ans : 41% en 2018, 43% en 2019, pour atteindre 60% en 2020.

Le CERT Santé a été sollicitée de manière plus importante pour accompagner les structures dans la réponse aux incidents de cybersécurité. L'évolution de la menace et l'expertise nécessaire pour faire face à un acte de cybermalveillance ayant potentiellement un fort impact sur le SI nécessitent la mise en place de moyens trop importants pour de nombreuses structures. Elles sont plus enclines à demander un appui au CERT Santé, en particulier en matière d'investigation numérique (analyse d'artefacts et de journaux d'évènements) et d'aide à la remédiation (éradication de la menace et mise en place de plans spécifique de protection). L'ANSSI est aussi intervenu en appui concernant des attaques potentiellement très impactantes sur la continuité des soins, en particulier auprès des opérateurs de services essentiels (OSE).

En 2019, une croissance significative des attaques par maliciels des structures de santé avait été observée. Elles représentent en 2020 pratiquement 25% des incidents déclarés, dont plus de la moitié sont des rançongiciels. Cette menace est toujours bien présente et n'est d'ailleurs pas spécifique au secteur santé mais concerne l'ensemble des secteurs d'activité. Elles constituent toujours la menace la plus importante pour la continuité des soins au sein des structures, surtout lorsque les sauvegardes ont été chiffrées. Dans ce cas, la période nécessaire pour revenir à un fonctionnement normal du système d'information peut prendre plusieurs semaines, impactant durablement l'organisation de la prise en charge des patients.

On constate en 2020 une augmentation de la compromission des accès à distance, que ce soit par l'exploitation de vulnérabilités critiques présentes sur des équipements non mis à jour ou le vol de mots de passe de comptes d'accès. C'est souvent par ce canal que les attaquants accèdent au SI interne pour ensuite déployer un code malveillant (rançongiciel et cryptominer dans la majorité des compromissions). L'évolution de cette menace est liée à l'utilisation accrue des accès à distance avec la pandémie COVID-19 et les difficultés rencontrées par les responsables informatiques à corriger dans des délais contraints ces vulnérabilités critiques sur un SI trop fortement exposé sur Internet.

Les conséquences/impacts de ces actes de cybermalveillance sur le SI sont plus importantes lorsque les règles d'hygiène informatique n'ont pas été mises en œuvre pour la protection des

[3] Secteur santé : 3036 établissements de santé (au 31/12/2018, cf. étude DREES).
Secteur social et médicosocial : près de 35.000 établissements ou services médico-sociaux.

actifs sensibles du SI (configuration des services d'annuaire (Active Directory), cloisonnement des sauvegardes).

La part des incidents d'origine non malveillante est en diminution en 2020 (40% contre 57% en 2019). Il n'y a pas d'évolution notable sur l'origine de ces incidents : il s'agit essentiellement de dysfonctionnement ou de panne liés à la fourniture d'un service par un prestataire (réseau, applicatif, téléphonie) ou de bugs logiciels.

Ces incidents sont principalement dus à des dysfonctionnements de l'infrastructure (infrastructure locale ou bien celle de prestataires), des pertes de liens télécom (panne opérateur) et des bugs. Ces incidents impactent l'organisation des soins, puisqu'ils entrainent souvent une interruption temporaire de l'accès au dossier patient informatisé ou à des plateformes d'échanges de résultats (biologie, radiologie, etc…) Concernant la résolution de ces incidents, les structures et prestataires ont été globalement réactifs et autonomes.

4 OBSERVATOIRE DES SIGNALEMENTS

4.1 Chiffres clés pour la période 2019-2020

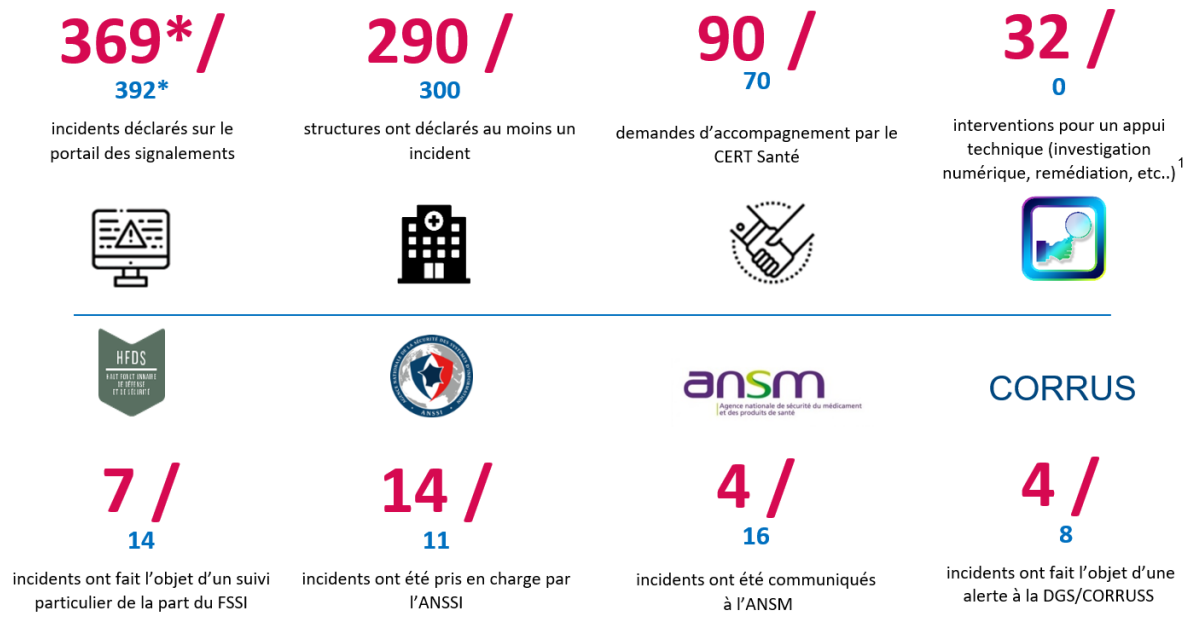


Figure 1 – Chiffres clés des signalements déclarés en 2019 et 2020

En coordination avec le CERT Santé, l'ANSSI et le FSSI sont intervenus directement au profit de 17 structures de santé, dans le suivi de la gestion d'un incident ou l'appui à la réponse.

Pour **l'ANSSI** il s'agit de :

- Dix établissements de santé publics, dont quatre opérateurs de services essentiels (OSE). Ces incidents avaient pour origine des attaques par rançongiciel, par déni de service et un dysfonctionnement des équipements de sécurité (faux positifs) ;
- Deux EHPAD, l'un victime d'un rançongiciel et l'autre pour une compromission potentielle ;
- D'un prestataire d'un établissement médico-social dans le domaine du handicap qui a été victime d'un rançongiciel.

Pour le FSSI du MSS, il s'agit de

- Cinq établissements publics de santé dont deux OSE. Ces incidents avaient pour origine des attaques par rançongiciel, par déni de service, une perte des services téléphoniques et un dysfonctionnement récurrent des infrastructures.

4.2 Informations générales sur les signalements

369 incidents ont été déclarés en 2020. Ce nombre est en légère baisse par rapport à 2019 (392). Pour mémoire, 327 incidents avaient été déclarés en 2018.

Parmi ces incidents, on compte des incidents « hors périmètre » ne concernant pas les secteurs sanitaires et médico-social (pharmacies par exemple) ou ne concernant pas des systèmes numériques. Ces incidents n'ayant pas fait l'objet d'un traitement particulier sont au nombre de 20, ce chiffre a baissé de presque 50% par rapport à 2019 (38).

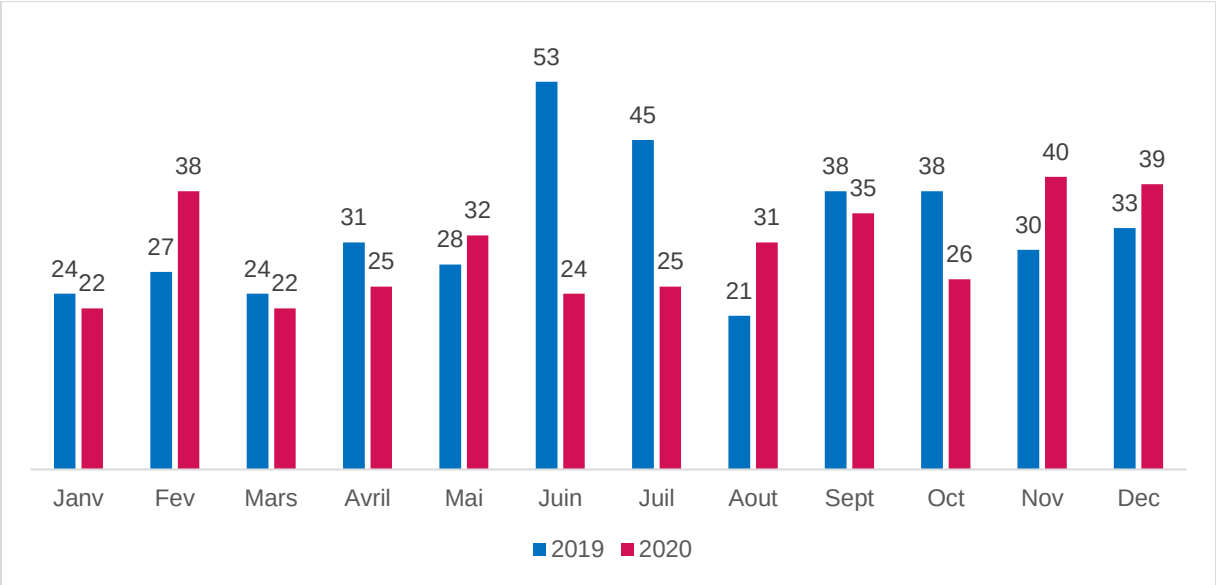


Figure 2 - Nombre de signalements par mois

Par comparaison avec l'année 2019, le nombre mensuel de signalements reste stable en 2020, puisqu'en moyenne 32 signalements ont été déclarés par mois en 2019 contre une moyenne de **30 par mois en 2020**. Ceci s'explique par un pic des déclarations inhabituel observé en juin et juillet 2019 et qui n'a pas été observé de nouveau en 2020.

●● Répartition des signalements selon l'horaire et le jour de leur dépôt ●●

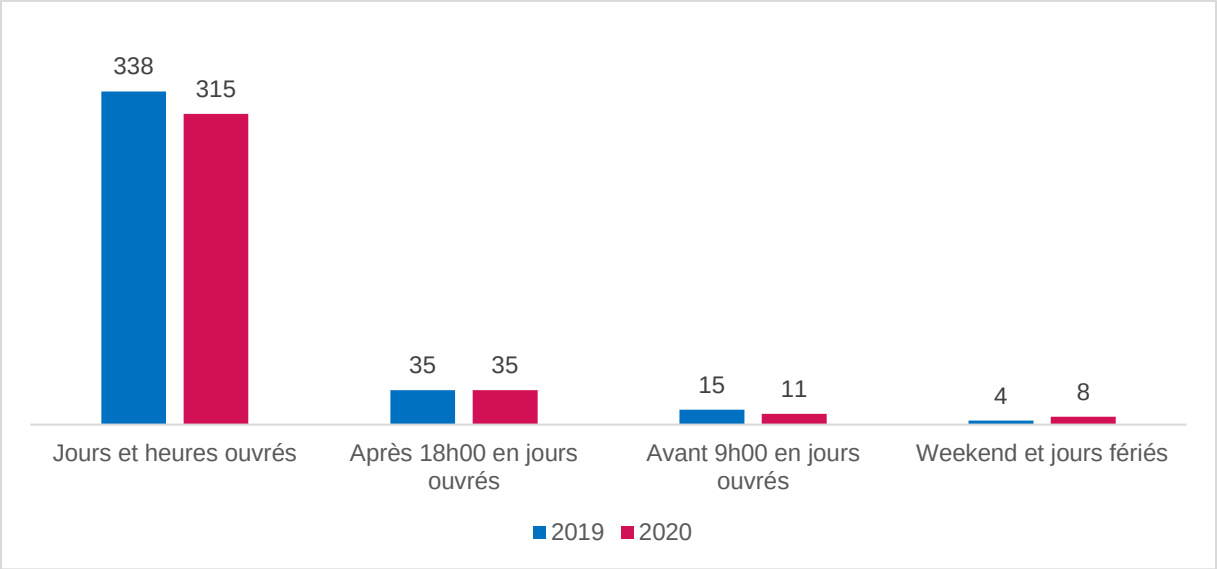


Figure 3 - Répartition des signalements selon l'horaire et le jour de leur dépôt

85% des signalements ont été effectués en heures et jours ouvrés (HO/JO) en 2020, entre 9h et 18h.

Ce sont principalement des structures publiques qui sont à l'origine des déclarations en HNO/JNO. Vingt-cinq demandes d'accompagnement ont été formulées durant ces périodes. Parmi celles-ci, seulement une structure nécessitait réellement un appui pour un incident d'origine malveillante (une attaque massive par rançongiciel), entrainant une interruption du SI support de nombreux services de prise en charge des patients. Cette déclaration réalisée un jour ouvré avant 9h a été prise en charge rapidement par le CERT Santé. Pour l'ensemble de ces demandes d'accompagnement HNO/JNO, aucune mise en danger patient n'a été relevée.

Etat des incidents lors de leur signalement

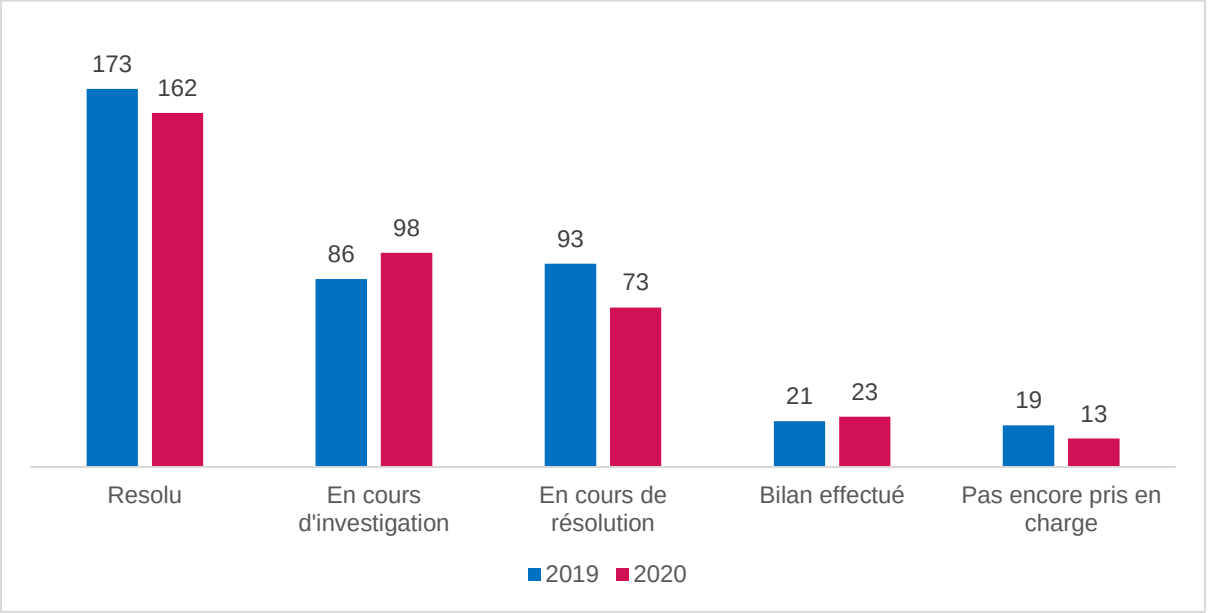


Figure 4 - Etat des incidents lors de leur signalement

En 2020, comme en 2019, près de la moitié des signalements sont résolus par la structure avant leur déclaration. En revanche, la part de ces signalements résolus baisse en 2020, en particulier au profit d'incidents déclarés « **En cours d'investigation** ». Depuis 2019, le CERT Santé est davantage sollicitée par les structures pour des actions d'investigation et la recherche de l'origine de l'incident. Sur trois ans, cette part augmente d'environ 6% chaque année, pour atteindre **27% en 2020**.

21 structures n'ont pas transmis d'informations complémentaires à la suite de leur déclaration, malgré une demande de compléments d'information et/ou une proposition d'appui.

27%

C'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2020**. Il a **augmenté de 6% par rapport à 2019**.

Les accompagnements sont en général demandés lors d'incidents ayant un impact important sur la structure ou bien lorsque la structure veut s'assurer qu'elle a bien entrepris l'ensemble des actions recommandées tant en matière d'investigation que de remédiation, voire d'amélioration de leur résilience face à la menace de cybersécurité. **La principale demande d'appui concerne la gestion des attaques virales et la compromission des systèmes**. A la marge, certaines structures sollicitent aussi parfois le CERT Santé pour intervenir auprès de prestataires lorsque ces derniers sont à l'origine de l'incident (panne réseau, dysfonctionnement applicatif) et ne sont pas suffisamment réactifs dans la mise en place de solutions de remédiation. Le CERT Santé, n'ayant pas de rôle de médiateur, use du maximum de ses prérogatives afin d'appuyer les structures qui en font la demande, ou bien oriente celles-ci vers l'interlocuteur le plus compétent pour agir.

●● Répartition des signalements selon la localisation de la structure●●

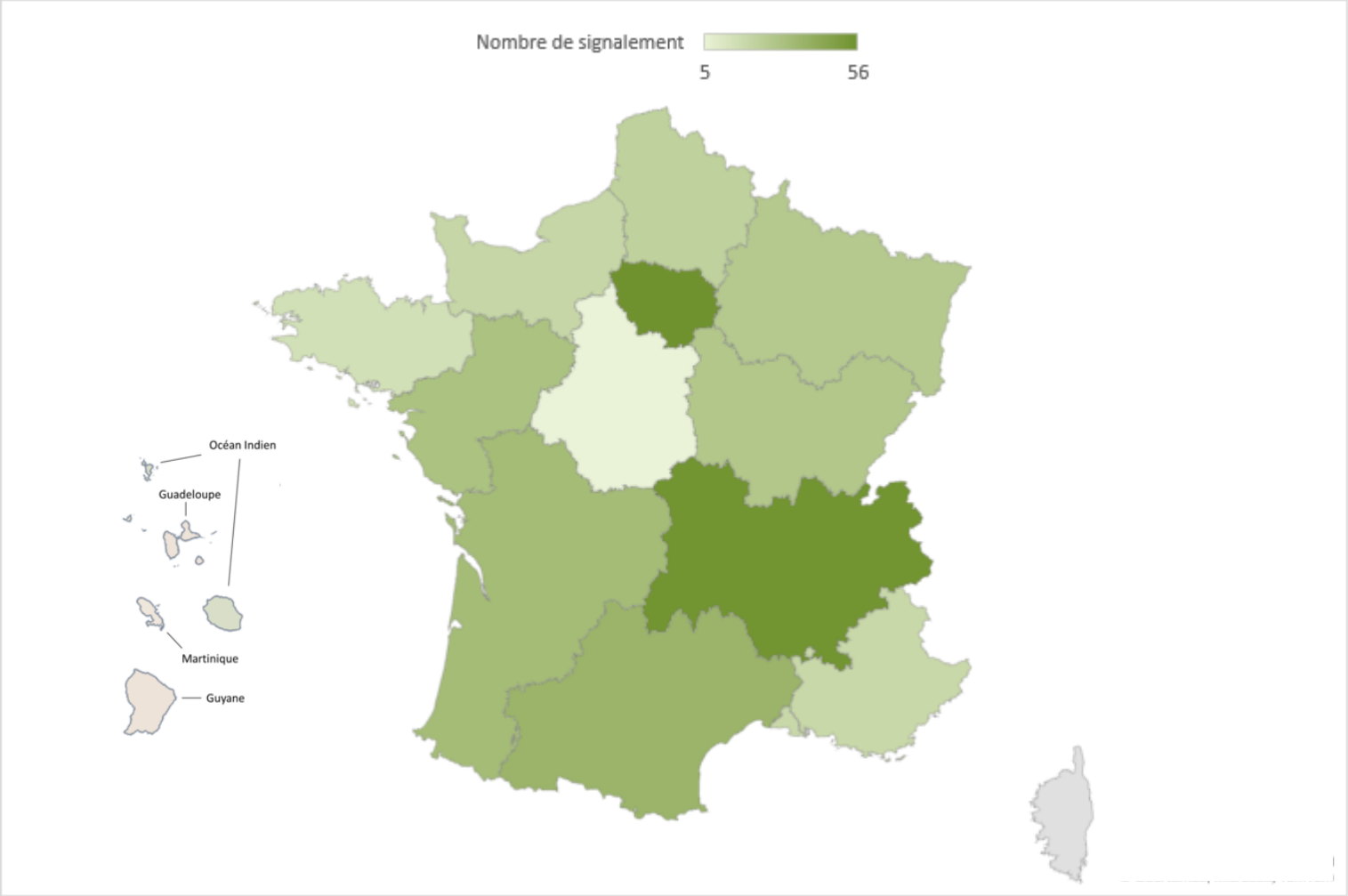


Figure 5 - Répartition des signalements par région

Les régions pour lesquelles le nombre de signalements est le plus important sont l'Ile-de-France et la région Auvergne-Rhône-Alpes avec respectivement 56 et 55 signalements. Ces deux régions représentent à elles seules plus de 30% du total des signalements.

Au moins un incident a été déclaré dans chaque région, à l'exception de la Corse.

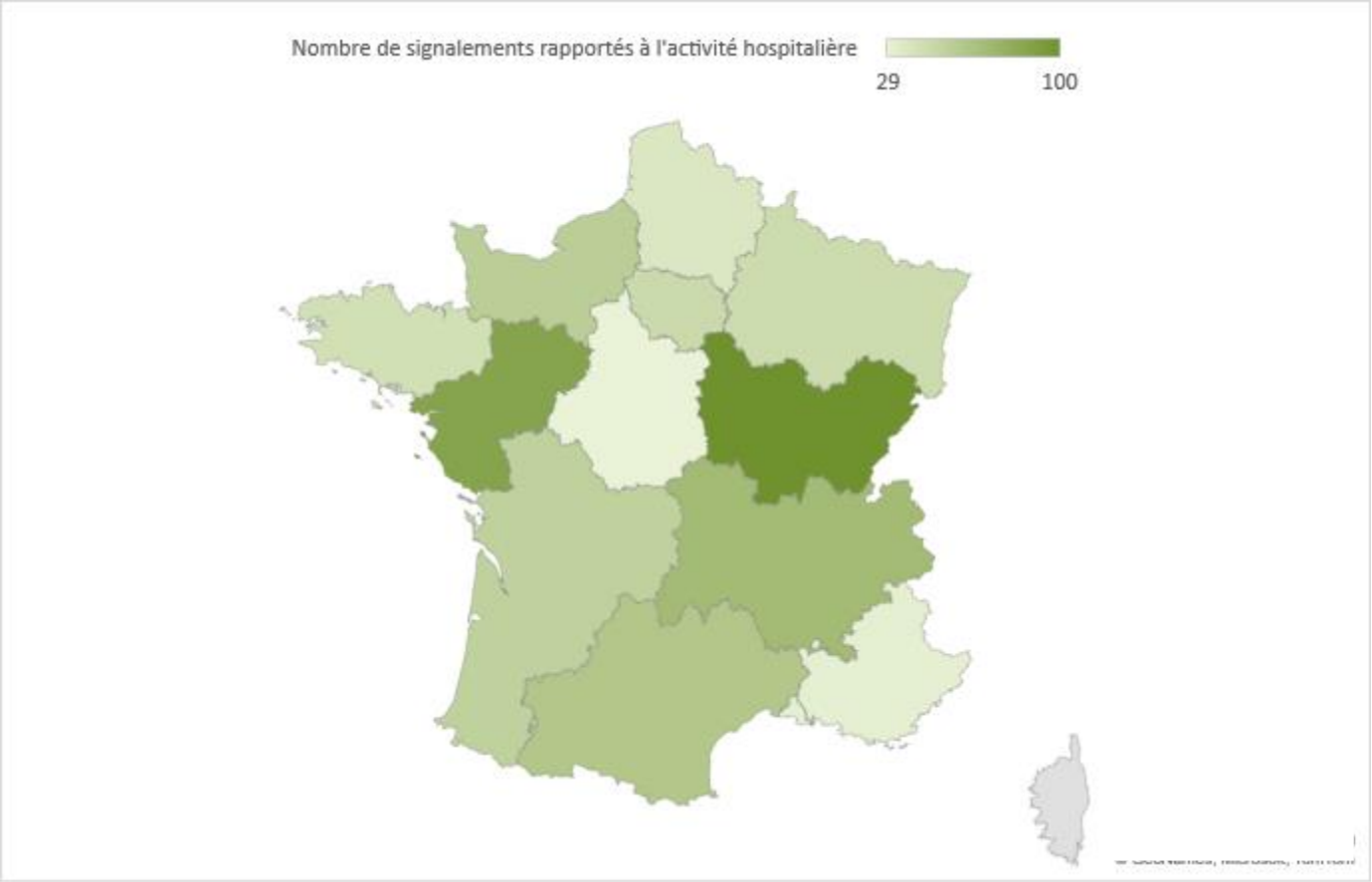


Figure 6 - Nombre de signalements rapporté à l'activité hospitalière des régions

Cette carte présente le ratio entre le nombre de signalements et l'activité hospitalière rapportée au niveau national : plus une région a un nombre de signalements élevé par rapport à son activité, plus celle-ci est foncée. Les DOM-COM n'ont pas été pris en compte dans cette analyse à cause du faible taux d'activité hospitalière par rapport à la métropole. La région avec le ratio le plus élevé (Bourgogne-Franche-Comté) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (4.41% de l'activité nationale soit presque quatre fois moins que l'Île-de-France), la région Bourgogne-Franche-Comté est en tête en matière de remontée des incidents. La région Pays de la Loire arrivent en deuxième position.

En revanche, la région Centre – Val de Loire ainsi que la région PACA déclarent peu d'incidents au regard du nombre d'établissements hospitaliers situé sur leurs territoires de santé.

Il est nécessaire de rappeler à toutes les structures de santé l'obligation de déclaration des incidents de sécurité, en particulier dans les régions où le nombre de signalements rapporté à l'activité hospitalière est faible.

Répartition des signalements selon le type de structure

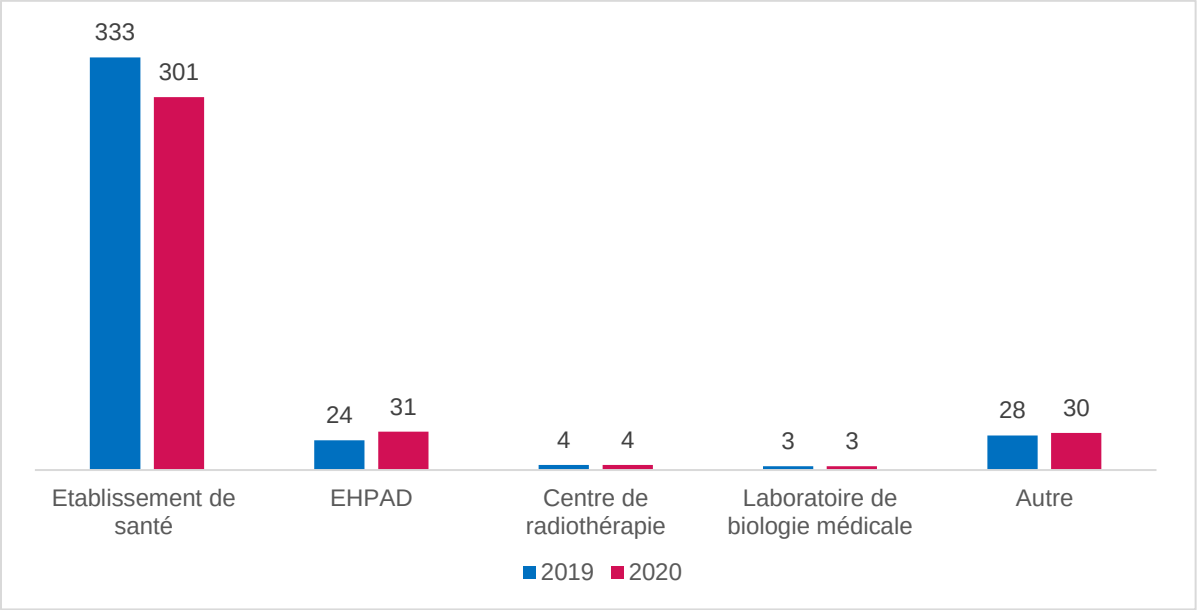


Figure 7- Répartition des signalements selon le type de structure

La majorité (81%) des incidents de sécurité est déclarée par les **établissements de santé** (voir détail figure 7).

En 2020 comme en 2019, les **EHPAD** représentent une part grandissante des déclarations reçues. Depuis le 18 novembre 2020, l'ensemble des établissements du secteur médico-social est dans l'obligation de déclarer leurs incidents graves de sécurité.

La catégorie « Autre » reste stable cette année. Elle correspond principalement à des déclarations réalisées par des cabinets libéraux et des établissements publics du secteur médico-social.

●● Part des signalements comparée à la part des établissements de santé selon leur type ●●

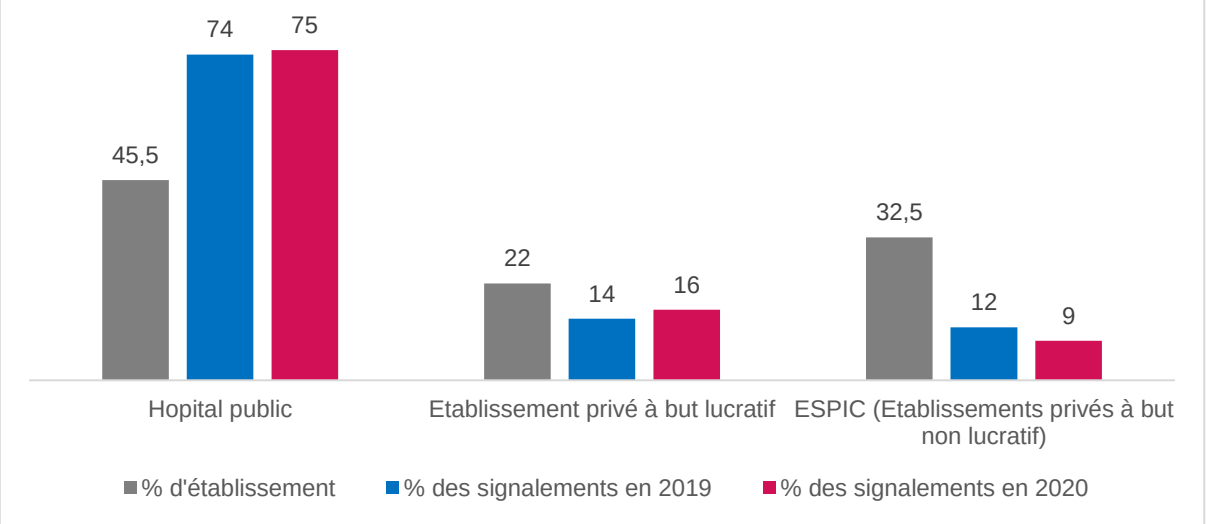


Figure 8 - Part des signalements comparée à la part des établissements selon leur raison sociale

Les **établissements publics** sont, encore en 2020, largement **majoritaires** dans la déclaration des incidents. La tendance à la sous-déclaration des incidents par les acteurs du privé se confirme, en particulier des ESPIC.

39 C'est le nombre de structures qui ont déclaré plus de 2 incidents durant l'année 2020 sur 250 structures au total. Dix d'entre elles ont signalé au moins quatre incidents.

●● Répartition des déclarations selon le type d'impact sur les données ●●

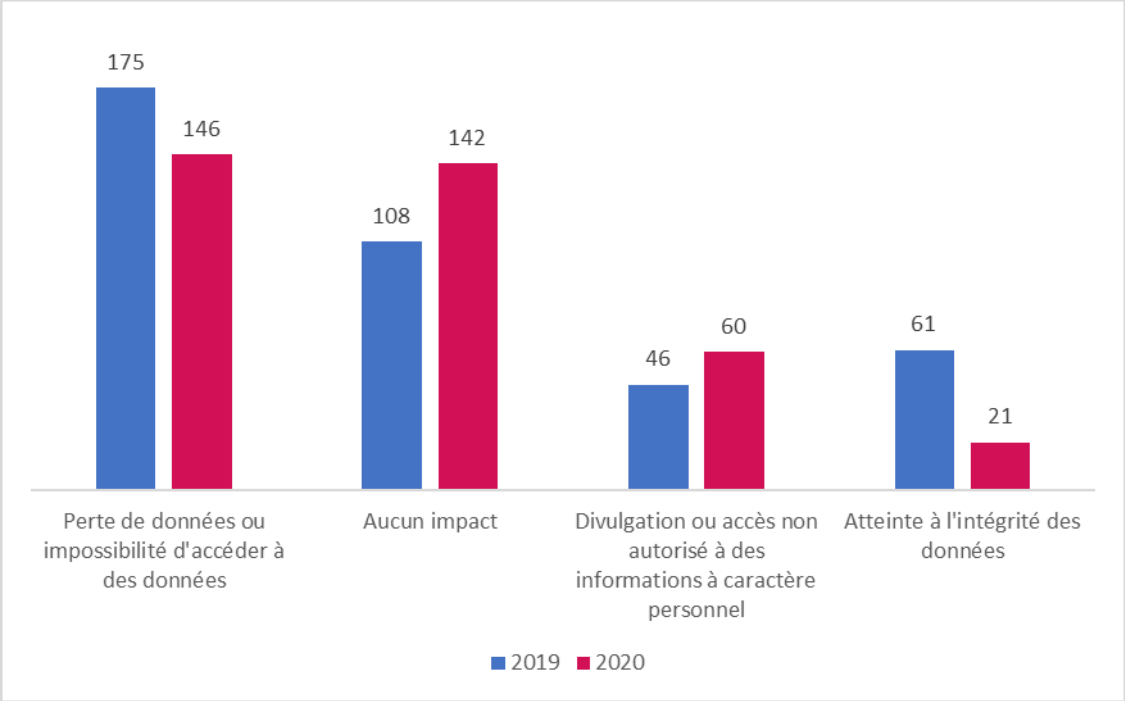


Figure 9- Répartition selon les types d'impact sur les données

Pour la moitié des incidents signalés en 2020, tout ou partie des données présentes sur le SI de la structure étaient impactées. 60% des incidents concernés avaient une origine non malveillante (majoritairement un dysfonctionnement du SI mais aussi une panne électrique ou une perte du lien télécoms). Pour les incidents ayant une origine malveillante (40%), la cause de la perte de disponibilité des données était principalement une attaque par rançongiciel.

Pour 38% des signalements, les structures assurent qu'il n'y a eu aucun impact sur les données. On retrouve alors des incidents ayant pour origine des tentatives de phishing, d'intrusion sur le SI, des attaques par ingénierie sociale, la réception de fausses factures papier ou bien encore des bugs applicatifs ou une perte de la ligne téléphonique.

Concernant les divulgations de données, elles sont dues en majeure partie à des vols d'identifiants de comptes d'accès à distance (VPN, RDP) et de messagerie (Webmail). Accessoirement, cette atteinte à la confidentialité des données peut être due à un vol d'équipement.

35% C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2020. Ce chiffre est relativement stable puisqu'il était de 38% en 2019 et de 35% en 2018.

45%

C’est le pourcentage de structures qui ont été contraintes à mettre en place en 2020 un **fonctionnement en mode dégradé** du système de prise en charge des patients (5% de plus qu’en 2019). Ce mode dégradé dépend de la nature de l’incident et des procédures mises en place dans les structures : application du plan de continuité, utilisation du mode de fonctionnement papier pour gérer les patients, utilisation d’un poste dédié, mise en place de solutions de contournement pour prendre en compte les dysfonctionnements des logiciels de prescription, etc... En moyenne, le mode dégradé a été mis en œuvre par les structures de santé sur la période d’**une journée** mais certains établissements ont été confrontés à cette situation pendant plusieurs jours. 14% des établissements ayant mis en place un mode dégradé ont subi une interruption du système de prise en charge d'un patient.

●● Répartition des déclarations selon le type de données impactées●●

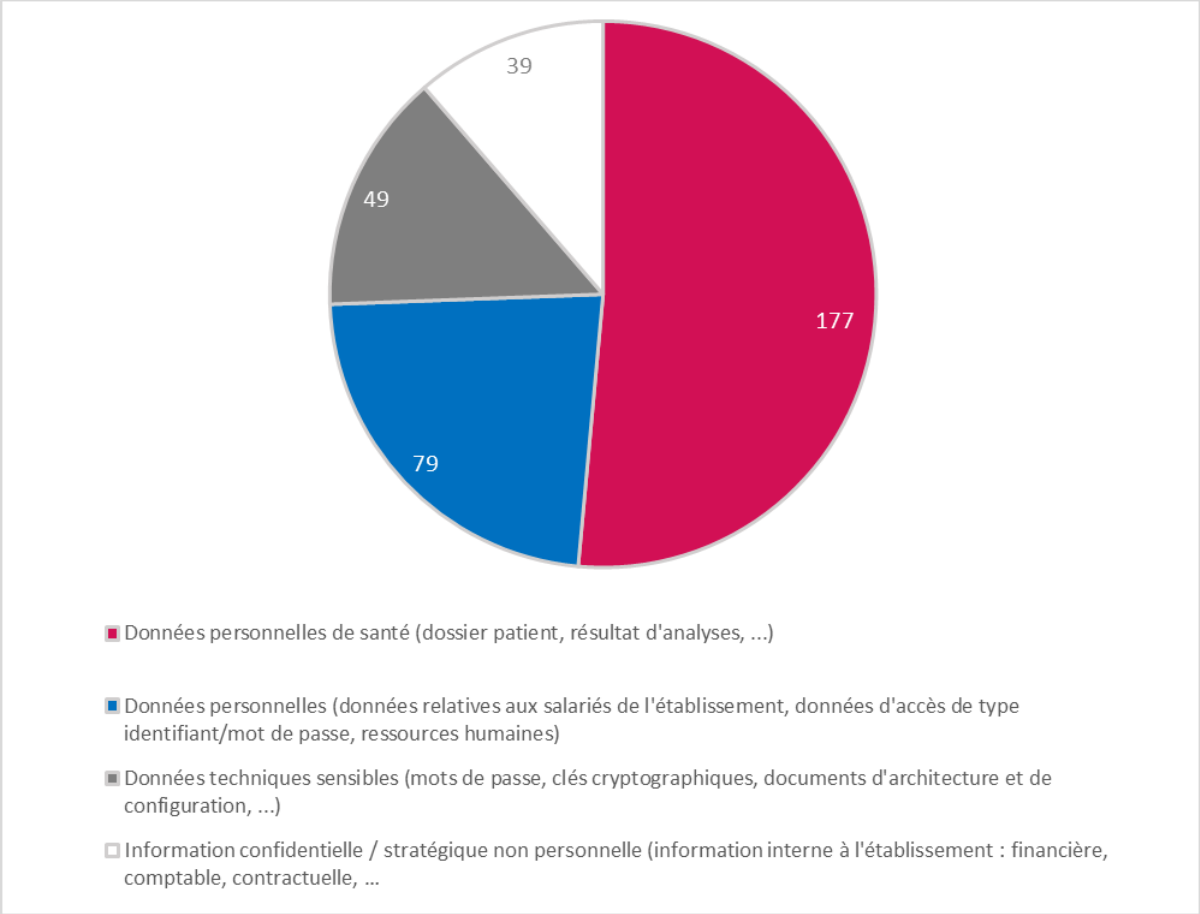


Figure 10 - Répartition selon les types de données impactées

60% C'est le pourcentage de structures indiquant que **l'incident a eu un impact sur des données**, qu'elles soient à caractère personnel, techniques ou relatives au fonctionnement de la structure

46% des incidents impactant des données touchent **plus d'une catégorie de données** parmi les quatre catégories décrites dans le graphique ci-dessus.

C'est ainsi que parmi les incidents impactant des données, **79%** touchent des **données de santé à caractère personnel**, 35% des informations à caractère personnel hors données patient, 22% des données techniques sensibles et enfin 17% des informations confidentielles ou stratégiques. Les données personnelles sont donc les premières atteintes par les incidents de sécurité déclarés.

Mise en danger potentielle des patients

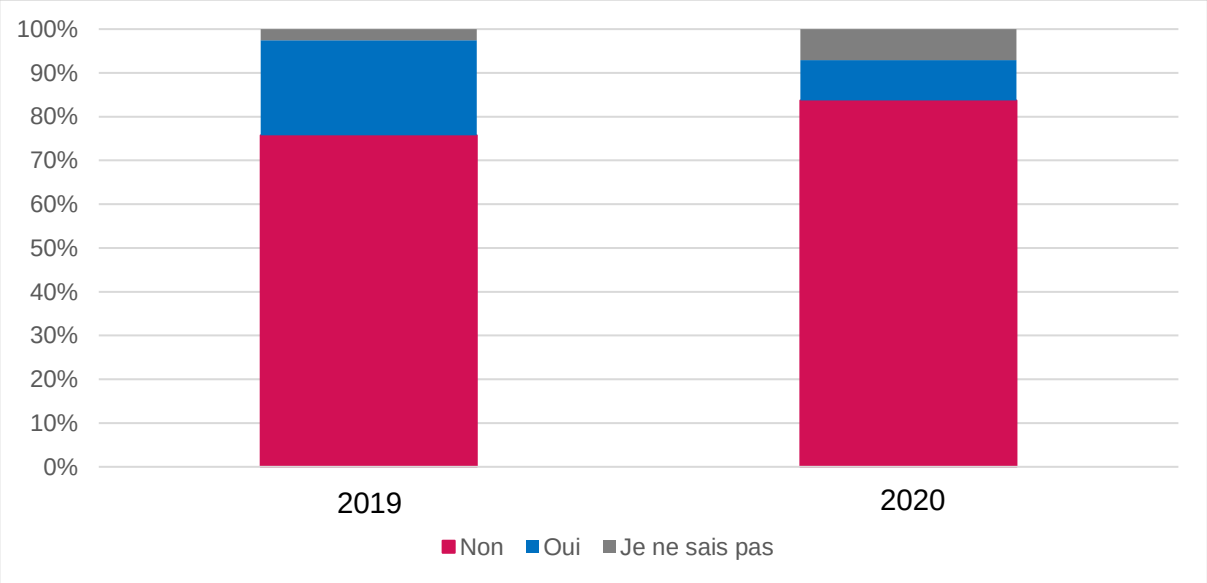


Figure 11 - Mise en danger potentielle des patients

Parmi les **34 mises en danger patient** de cette année 2020 (9% du nombre total d'incidents), **2** incidents ont entrainé une **mise en danger patient avérée**.

Concernant les 91% restant, correspondant à la part de mises en danger **potentielles** de patients, on retrouve principalement des incidents liés à la perte de lien télécoms (en particulier pour des SAMU), ou encore à des indisponibilités totales du SI par exemple.

Les dysfonctionnements des logiciels de prescription/aide à la dispensation liés à des bugs ayant provoqué des erreurs dans les prescriptions et la délivrance des médicaments auraient pu entrainer une mise en danger des patients plus importante sans la vigilance des professionnels de santé et la mise en place de procédures permettant d'identifier les erreurs.

●● Répartition des signalements à origine malveillante ou non malveillante ●●

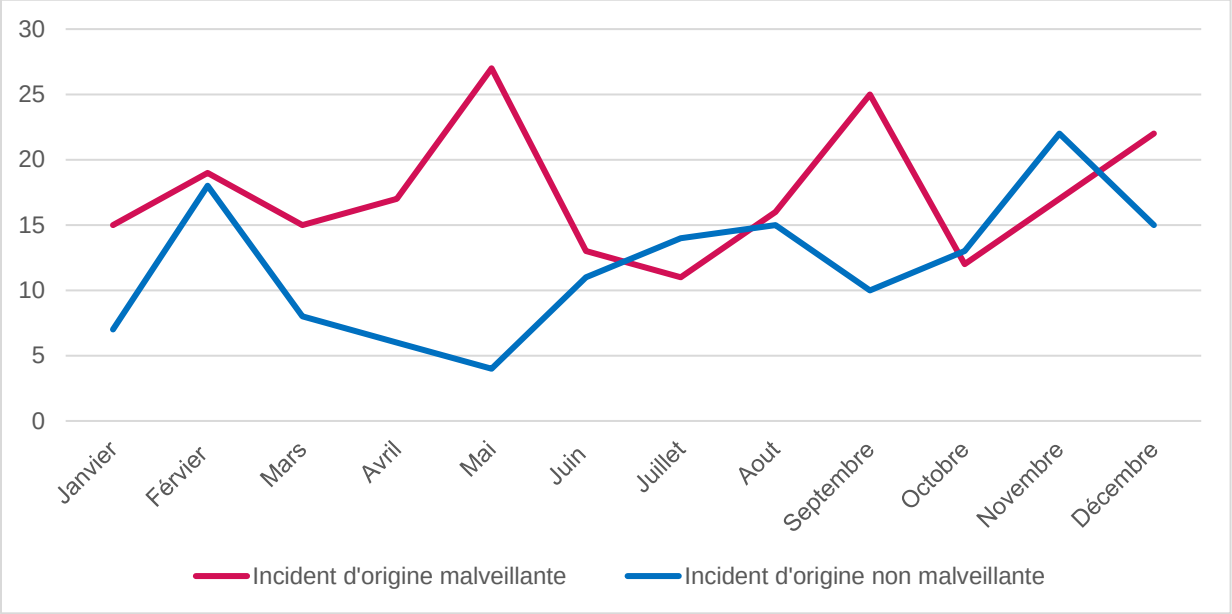


Figure 12 - Répartition selon le type d'incident

Parmi **les incidents déclarés, 60% sont d'origine malveillante et 40% d'origine non malveillante**. Dans l'analyse détaillée de ces deux catégories d'incidents, sont exclus les 20 signalements dits « Hors périmètre » n'ayant pas fait l'objet d'un traitement particulier.

Les actes malveillants

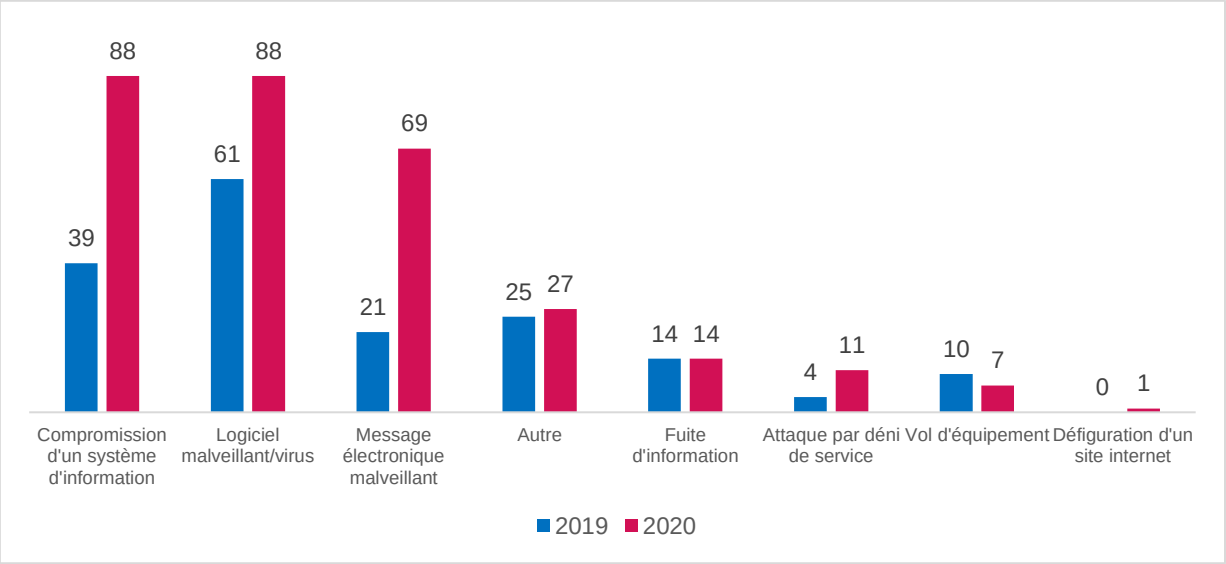


Figure 13 - Nombre d'incidents par type d'origine

La technique du **phishing** constitue encore en 2020 un vecteur d'attaque privilégié pour déployer un code malveillant sur un système ciblé. Le manque de vigilance ou la négligence est souvent à l'origine de la compromission : réponses à des messages électroniques malveillants ou accès à des sites web malveillants. Dans de nombreux cas, les mécanismes de protection des services de messagerie peuvent être améliorés, notamment grâce au service de test de la configuration des règles de sécurité de la messagerie proposé par le CERT Santé (les demandes de compte de test doivent être faites par mail à cyberveille@esante.gouv.fr).

Mais ce sont les **compromissions** de comptes qui sont de plus en plus observées en 2020. Afin de déployer des maliciels, les attaquants exploitent :

- des failles de sécurité (OS, logiciels, progiciels ou matériels non patchés) ;
- l'accès à distance avec des mots de passe peu complexes (RDP, VPN, webmail).

L'analyse des journaux d'évènements des équipements périmétriques permet généralement de retrouver l'utilisation illicite de ces accès.

Les codes malveillants ayant le plus affecté les structures de santé sont les **rançongiciels**. Les structures ont été victimes de variantes de rançongiciels connus comme Ranion, Dharma et Sodinokibi ou encore Magneto et Snake. Certains sont déployés manuellement par l'attaquant, d'autres se déploient automatiquement (comme des vers) sur l'ensemble des machines appartenant à un même domaine Windows. Si des compromissions de comptes (VPN, pare-feu, comptes locaux) sont majoritairement à l'origine de l'infection par un rançongiciel, le phishing est toujours utilisé par les attaquants. Ceci a notamment été observé pendant la vague d'attaques Emotet.

Certains rançongiciels n'ont pas été détectés par les solutions antivirales du marché, il convient donc de ne pas faire reposer sur ce seul outil de sécurité l'ensemble de la protection d'un SI.

Le montant de la rançon n'est pas précisé systématiquement dans le message de l'attaquant. Il est demandé de plus en plus fréquemment à la structure de prendre contact avec une adresse mail.

Pour la majorité de ces rançongiciels, il n'existe pas d'outil de décryptement/déchiffrement au moment de l'incident. Dans ce cas, les structures ne peuvent se reposer que sur des sauvegardes saines. **Il est capital d'avoir anticipé la menace du rançongiciel et de détenir des sauvegardes hors ligne afin de pouvoir organiser au plus vite un retour à la normale dans la structure.**

Lorsqu'elles sont explicitement formulées, les demandes de rançon sont souvent en bitcoin, pouvant aller jusqu'à plusieurs bitcoins (plus de 100k€). Ces sommes sont similaires à celles observées dans d'autres secteurs d'activité et ne semblent pas spécifiques aux structures de santé. De plus, les modalités d'attaque et de demande n'étant pas individualisées ni spécifiques au secteur santé, il est fort probable qu'elles ne visent pas d'établissement en particulier.

Il est rappelé la recommandation gouvernementale de ne jamais payer de rançon :

- Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux ;
- Le paiement de la rançon n'empêchera pas l'entité d'être à nouveau la cible de cybercriminels ;
- L'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (exemple : un fichier de base de données).
- Enfin, son versement s'apparente à subventionner une organisation criminelle.

En 2020, il a été observé la réémergence des **cryptominers**. On trouve en première ligne de ces attaques, dont l'objectif est le minage de cryptomonnaies, le maliciel Wannamine. La caractéristique de Wannamine est le minage de la monnaie Monero après la compromission de comptes VPN ou RDP. Cette attaque a pour effet un fort ralentissement du SI, voire sa paralysie, par l'utilisation de la capacité CPU à 100%.

Les **fuites d'information** regroupent des atteintes à la confidentialité des données, principalement dues à la mise en vente sur le darknet d'identifiants de connexion (comme par exemple après l'exploitation de la faille CVE-2018-13379 sur Fortinet permettant d'obtenir accès à des comptes du VPN).
La catégorie « **Autre** » concerne principalement des tentatives d'escroquerie liées à des factures papier frauduleuses usurpant l'identité graphique d'Office Pro et de tentatives de compromission de systèmes n'ayant pas abouti (scans de ports ou de brute force de comptes d'accès).

Notons qu'une part des incidents (43%) relève de **plusieurs qualifications**. Par exemple, une attaque exécutant le maliciel Emotet après un phishing réussi relève des catégories suivantes : « message électronique malveillant » et « logiciel malveillant/virus ».

60% C'est le pourcentage en 2020 des incidents qui ont une origine malveillante. Ce chiffre **a augmenté de 17%** depuis l'année précédente.

●● Evolution du nombre d'incidents d'origine malveillante ●●

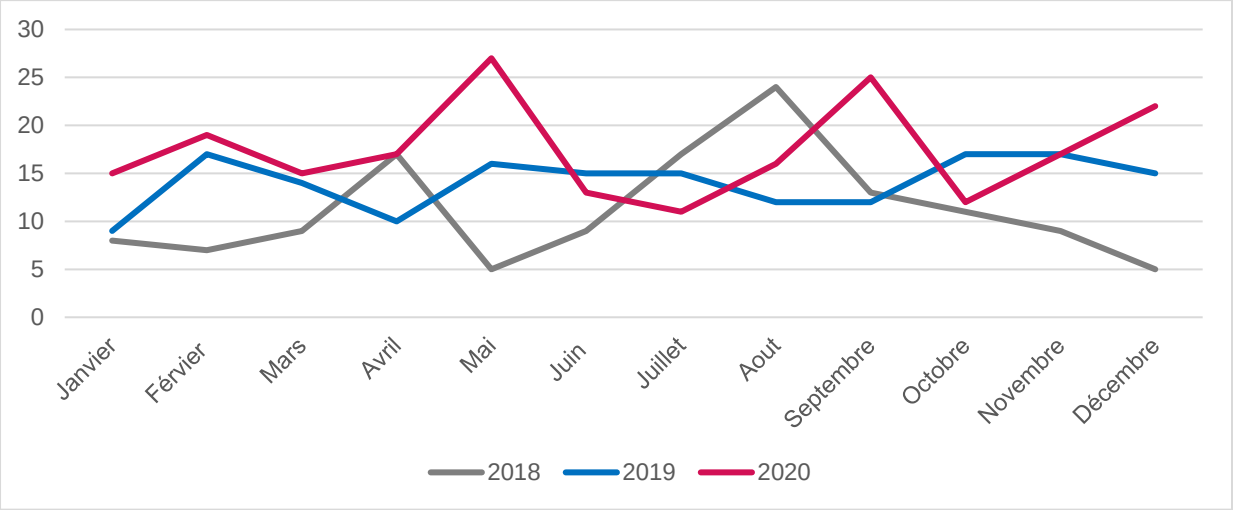


Figure 14 - Evolution du nombre d'incidents dont l'origine est malveillante

En 2019, la courbe du nombre d'incidents ayant une origine malveillante était particulièrement stable, notamment comparée à l'irrégularité observée en 2018. En 2020, les structures n'ont pas non plus eu de répits et des incidents d'origine malveillante ont également été observés chaque mois. On note cependant **un pic de signalements notable en septembre** : il correspond à la vague de **maliciels Emotet**. Fort heureusement, ces attaques ont eu peu d'impact sur le fonctionnement des SI.

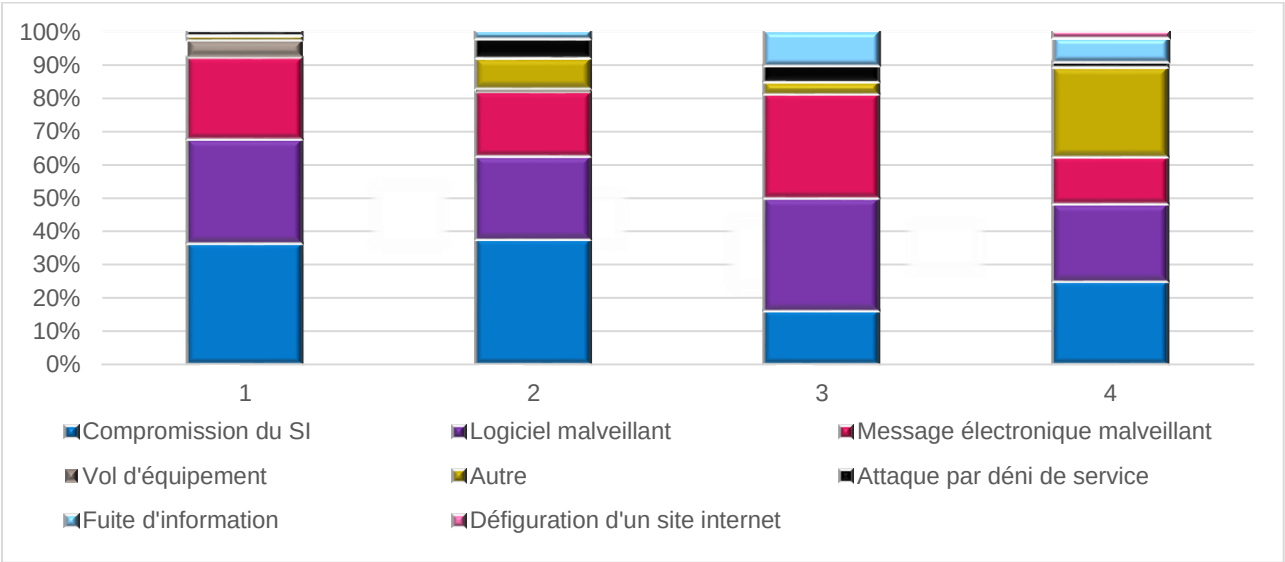


Figure 15 - Origine malveillante des incidents par trimestre

La frise chronologique suivante reprend les temps forts des **campagnes notables** en 2020 et le nom des maliciels identifiés par les structures ou le CERT Santé :

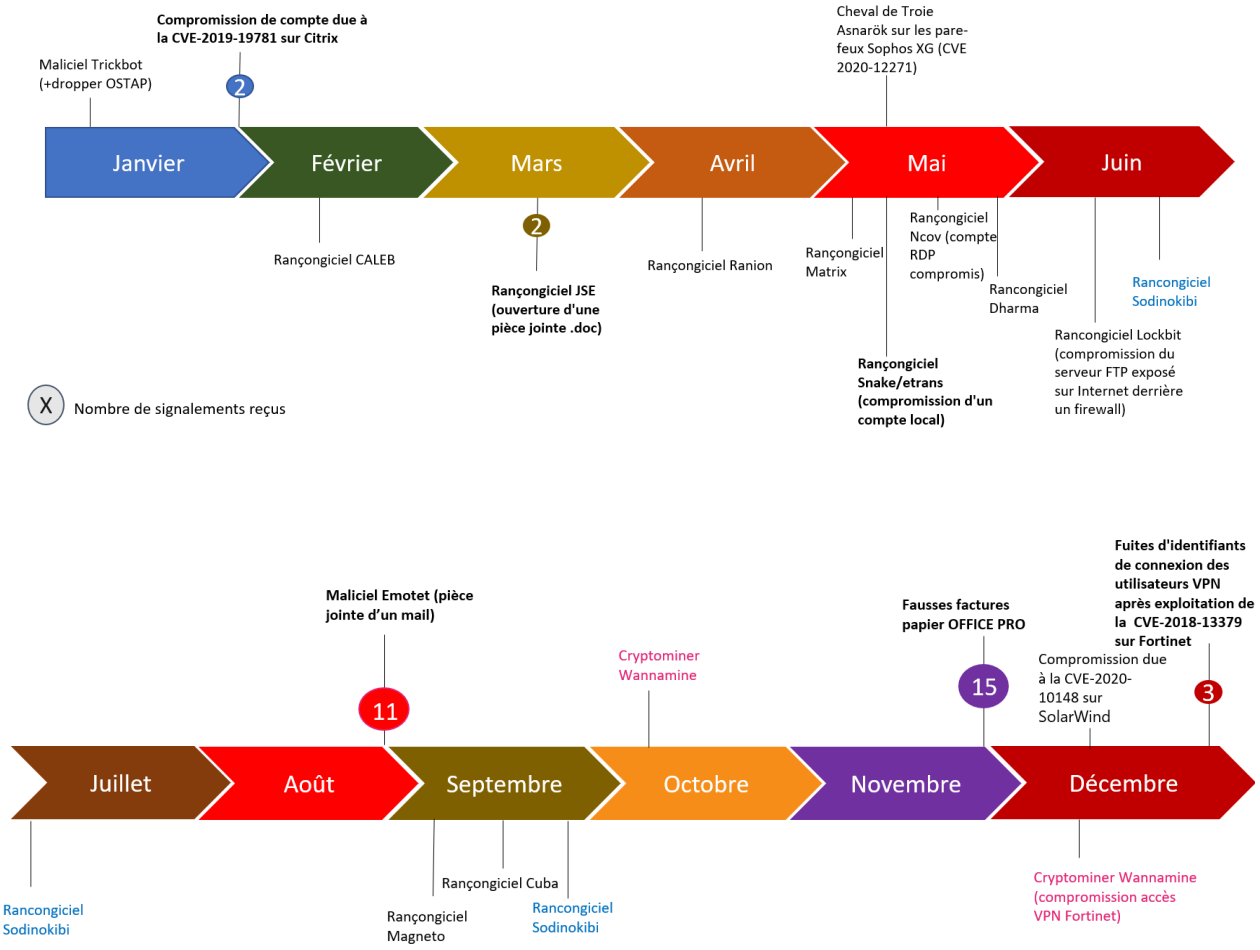


Figure 16 - Chronologie des cyber-menaces identifiées en 2020

En 2020, le CERT Santé s'est fixée comme objectif de **renforcer l'appui technique aux structures de santé**.

Cet appui a permis l'accompagnement de 30 structures, sur une période allant d'un à plusieurs jours, tant en matière d'investigation que de remédiation.

●● Appui technique pour la résolution d'un incident ●●

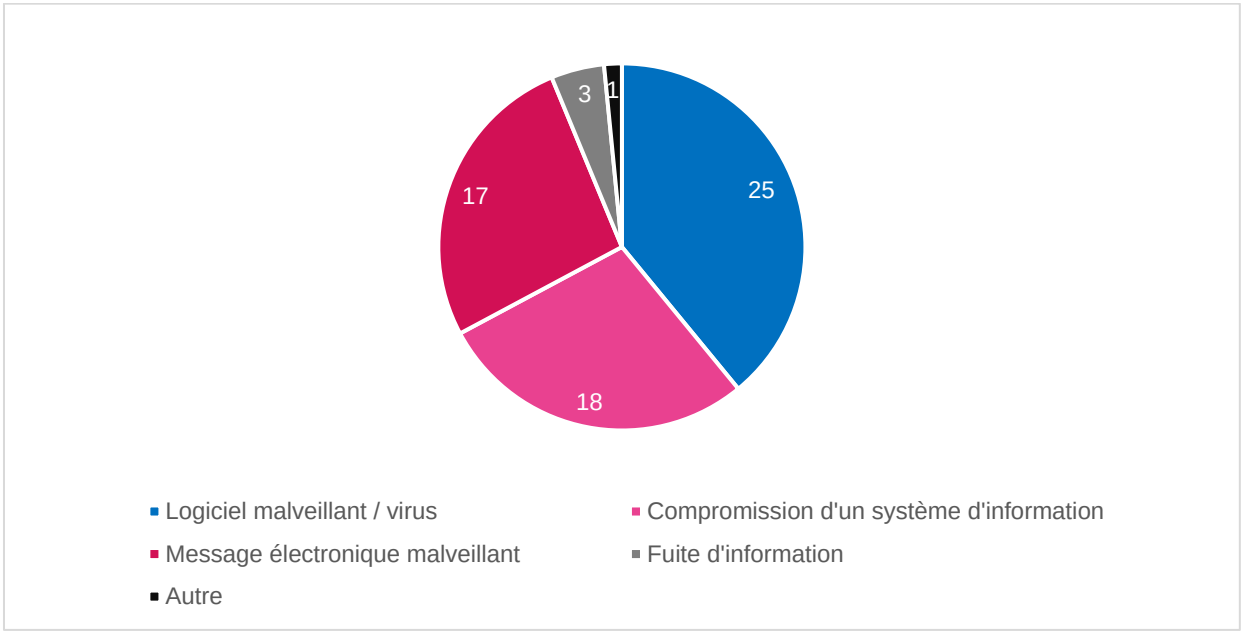


Figure 17 - Origine des incidents pour lesquels une intervention (investigation numérique, remédiation, etc.) a été réalisée par le CERT Santé

●● Accompagnement global des structures de santé ●●

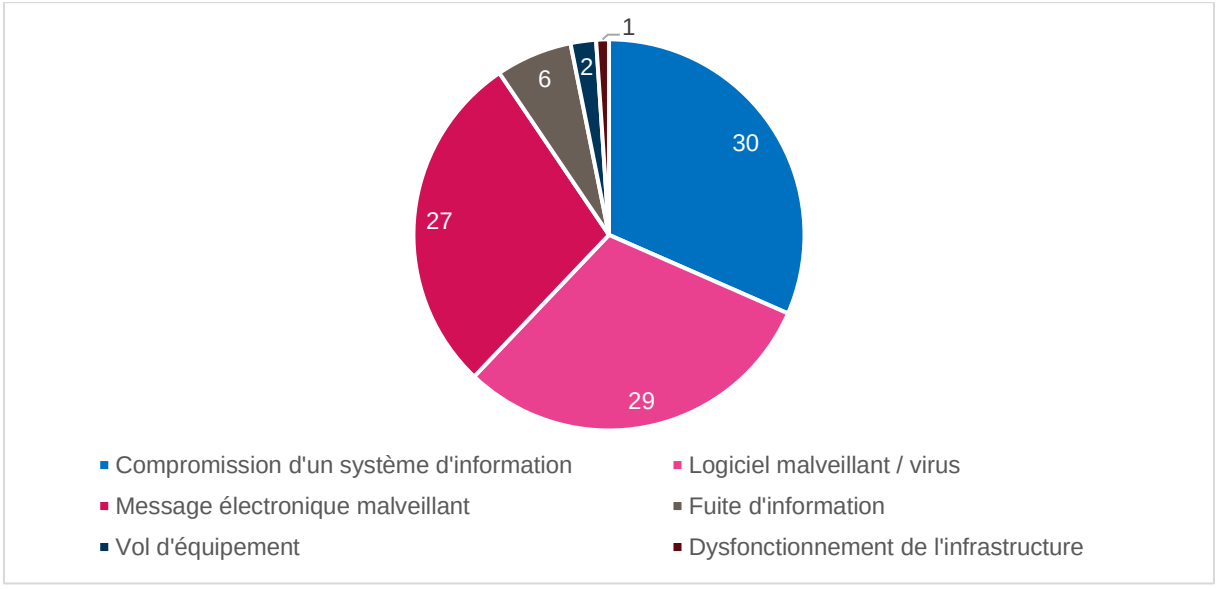


Figure 18 - Origine des incidents pour lesquels des recommandations ont été émises par le CERT Santé

Dans le cadre **de l'accompagnement des structures de santé**, des recommandations ont été émises par le CERT Santé afin, notamment, de permettre aux structures d'améliorer la sécurité de leur SI. Ces recommandations sont **adaptées à la taille de la structure ainsi qu'au niveau de technicité du déclarant et des équipes de la structure**.

Elles sont donc **variées** et peuvent aller de l'envoi des fiches et guides du portail cyberveille-santé, de la documentation de l'ANSSI, aux conseils plus techniques comme la mise en place de durcissement de systèmes, etc.

La **montée en puissance de l'accompagnement du CERT Santé** est d'autant plus pertinente que le nombre d'incident d'origine malveillante ne cesse de croitre, tout comme les demandes d'accompagnement formulées par les structures.

Les signalements d'origine non malveillante

●● Répartition des incidents d'origine non malveillante ●●

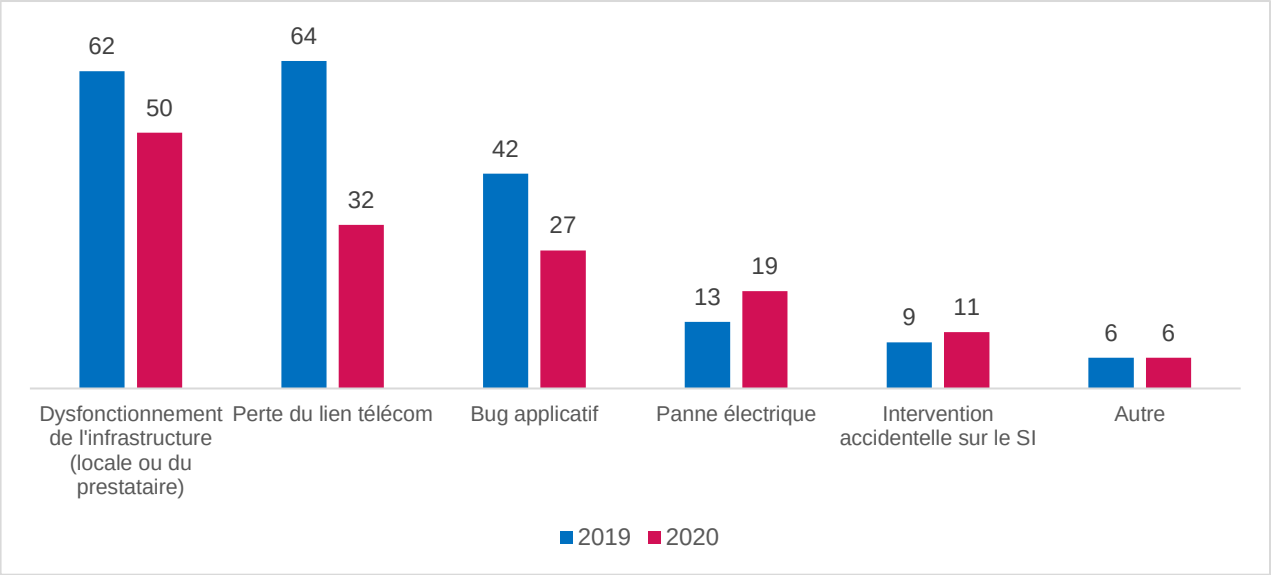


Figure 19 - Origine non malveillante des incidents

Une baisse du nombre d'incidents d'origine non malveillante déclarés est observée entre les années 2019 et 2020.

En 2019, la perte de l'accès à Internet (perte du lien télécom) était l'incident à origine non malveillante le plus fréquent. **En 2020, ce sont les dysfonctionnements du SI (local ou prestataire) qui sont les incidents les plus recensés (35%).** Cela a provoqué principalement des interruptions de service des applications hébergées, des systèmes de stockage, des dysfonctionnements de serveurs (DPI, base de données), des systèmes de gestion d'appels malades ou encore l'arrêt de l'infrastructure réseau (comme la perte de cœurs réseaux par exemple).

Une part grandissante de ces dysfonctionnements est observée non pas dans la structure mais chez son prestataire. Nous pouvons expliquer ceci par la tendance actuelle à l'externalisation de la gestion des applications, faisant reposer la gestion de la sécurité et des incidents sur leurs éditeurs ou prestataires de services informatiques.

La **perte du lien télécom** est la deuxième source d'incident d'origine non malveillante (22%). Cette perte peut fortement impacter le fonctionnement des activités métier des structures de santé, en particulier les structures disposant d'un service d'urgences ou un SAMU. Ce type d'incident est généralement traité en priorité par les opérateurs.

Concernant les **bugs applicatifs**, s'ils étaient la première menace non malveillante à laquelle ont été confrontées les structures de santé en 2018, en 2020, la tendance à la baisse du nombre de ce type d'incidents se confirme.

Ces bugs peuvent être graves notamment lorsqu'ils impactent des logiciels d'aide à la prescription et à la dispensation, engendrant des erreurs dans les prescriptions médicales et la délivrance des médicaments. Les logiciels de dossiers patients informatisés ont eux aussi été particulièrement impactés, ce qui affecte considérablement le bon fonctionnement de la structure.

Dans une majorité des cas, les éditeurs ont apporté des correctifs dans des délais compatibles avec la mise en place temporaire de mesures de vigilance exceptionnelles pour éviter de commettre des erreurs dans la prise en charge des patients.

40% C'est la part d'incident à origine non malveillante en 2020 des incidents, ce chiffre a baissé de 17% depuis 2019.

●● Evolution des incidents d'origine non malveillante ●●

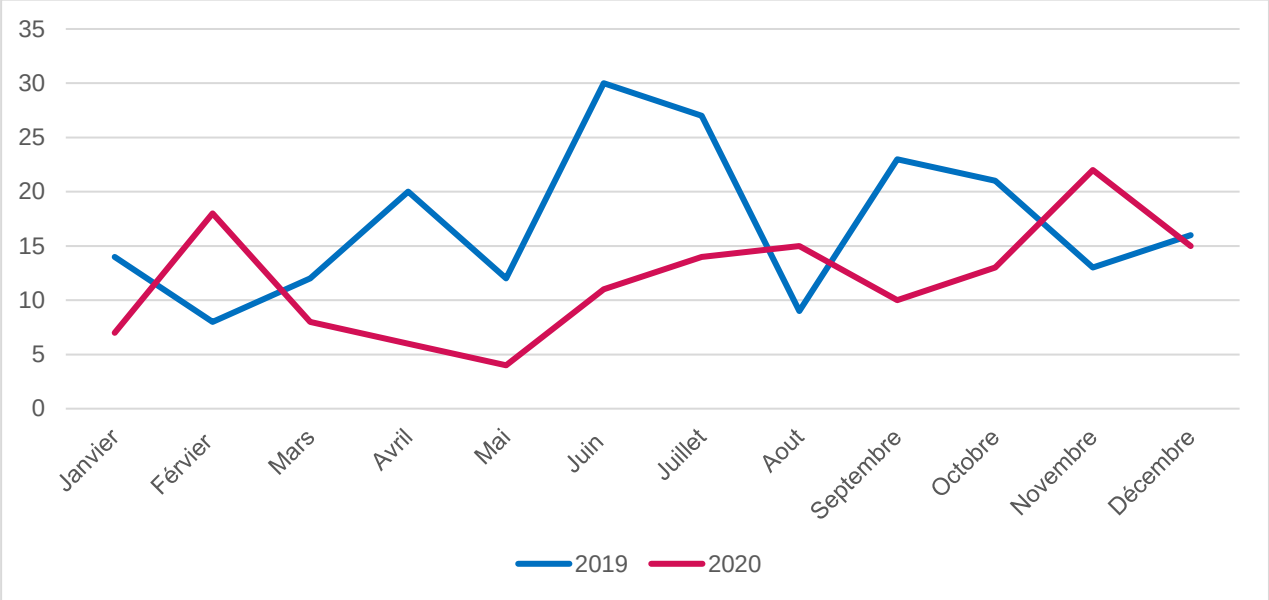


Figure 20 - Evolution du nombre d'incidents dont l'origine est non malveillante

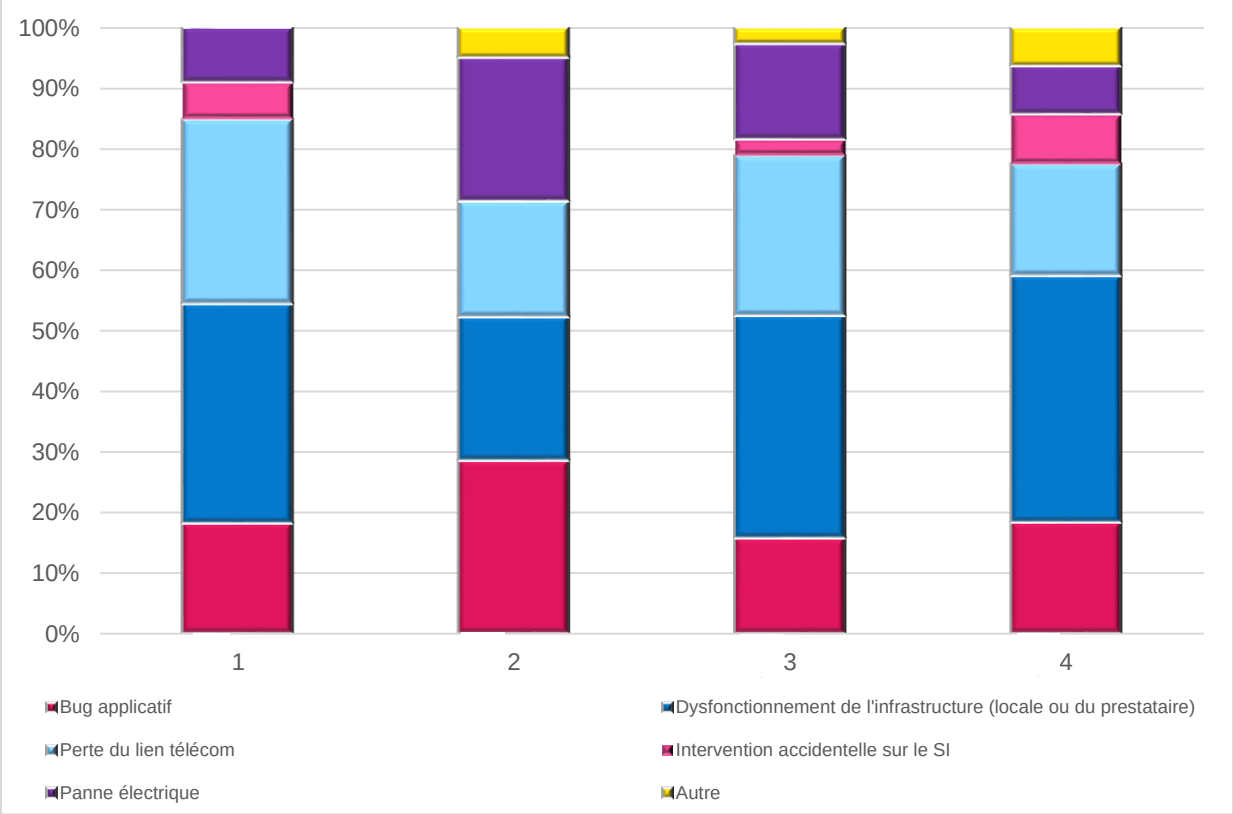


Figure 21 - Origine malveillante des incidents par trimestre

4.3 Incidents notables ayant fait l'objet d'un retour d'expérience anonymisé

Trois incidents font l'objet d'un retour d'expérience en 2020.

Ces retours d'expérience ont permis de faire la lumière sur le mode opératoire de certaines attaques et de présenter les mesures de remédiation à mettre en œuvre en cas d'incident.

Parmi ces incidents, on peut signaler :

- Une cyberattaque par le rançongiciel « Clop » impactant fortement le système d'information et l'activité d'une structure de grande taille. Chiffrant une grande partie des postes de travail et serveurs informatiques, l'attaque a paralysé l'ensemble des services de la structure, en rendant inaccessible l'accès à la plupart des applications métiers ;
- Une cyberattaque par le rançongiciel « Snake » suite à la compromission d'un compte d'accès par VPN ; le rançongiciel a été diffusé au moyen d'une tâche planifiée par GPO et a impacté la quasi-totalité des SI de la structure pendant plus de 24h;
- Une cyberattaque par hameçonnage entraînant une tentative de fraude au virement ; les messages envoyés utilisaient Office 365 et les boites compromises étaient utilisées pour envoyer des messages aux responsables financiers ;.

Ces incidents ont permis de rappeler l'importance de :

- Pouvoir réagir rapidement en cas d'attaque afin d'en limiter l'impact :
  - Faire connaitre et documenter les procédures de signalement des incidents, d'alerte de la chaine SSI, d'escalade et d'activation de crise ;
  - Disposer des informations nécessaires à la gestion de crise en cas d'incident (soit sur des documents imprimés, ou en conservant les informations sur un PC portable hors ligne) (déconnexion de l'Internet, des sauvegardes, des machines, ne pas éteindre les machines en vue des investigations, etc…) ;
  - Organiser régulièrement des exercices de crise permettant d'en vérifier l'efficacité et d'améliorer le dispositif de réponse ;
- Mettre en place des mesures de prévention permettant de limiter l'impact de l'incident :
  - Tester régulièrement les sauvegardes et en limiter drastiquement les accès en écriture (en utilisant par exemple un référentiel d'identité local et non pas des comptes d'accès de l'Active Directory (AD) principal pour l'administration), voire que les plans de sauvegarde permettent autant que possible, d'en disposer de copies isolées du réseau afin d'en éviter le chiffrement ;
  - Installer les correctifs de vulnérabilités critiques dans les meilleurs délais (vérifier les journaux en cas de doute sur une exploitation possible avant la mise en place des correctifs) ;
  - Centraliser en dehors de l'AD des journaux d'évènements (logs) des composants critiques du SI (et vérifier que les informations indispensables sont bien présentes) et les analyser régulièrement: proxyweb, messagerie, authentification (ad, web, vpn, …), filtrage (acl, firewall, …), events windows importants, events linux importants ;

- Cloisonner le système d'information avec des pare-feu et/ou des listes de contrôle d'accès (ACL) (filtrage entre les différentes parties réduit au strict nécessaire) et protéger les interconnexions du réseau avec Internet ;
- Lister l'ensemble des connexions réseaux avec les partenaires et plus largement l'ensemble des accès externes ;
- Vérifier que l'ensemble des contrats liant l'établissement avec les prestataires externes dont dépendent ses missions comportent bien des mentions nécessaires qui permettront, le cas échéant, une intervention dans des délais acceptables ;

► Anticiper les menaces par la veille sur les investigations dans les secteurs publics et privés (notamment des flux contenant des indicateurs de compromission actualisés relatifs à Emotet). Ces flux (comme celui de l'ANSSI) font partie des moyens de détection et de blocage.

Deux fiches sur la réponse à un incident lié à un maliciel et sur les moyens de prévention ont été publiées sur cyberveille :

https://cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiche_Maliciel_IR_RSSI.pdf

https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiche_Maliciel_P_RSSI.pdf

4.4 Publication d'alertes sur le portail cyberveille-santé

En 2020, six alertes ont été publiées sur le portail cyberveille-santé[4] concernant :

► Des campagnes d'attaques :

- Campagne de phishing visant à diffuser le maliciel Emotet, maliciel utilisé pour déposer d'autres codes malveillants susceptibles d'impacter fortement l'activité des victimes ;
- Campagne de phishing par laquelle l'attaquant menace de révéler des informations sur la vie privée de la personne si elle ne verse pas une rançon en Bitcoin. Il s'agit d'une arnaque au chantage à la webcam prétendument piratée ;
- Campagne d'attaques diverses exploitant la pandémie de coronavirus. Via de faux e-mails des autorités de santé, de fausses notes internes en entreprise ou encore de fausses alertes de retard de livraison, les cybercriminels ont tenté dans le monde entier d'exploiter la peur liée à la pandémie pour s'infiltrer sur les réseaux informatiques des entreprises et des particuliers.

[4] https://cyberveille-sante.gouv.fr/alertes

- Des vulnérabilités critiques :
  - Vulnérabilités dans Microsoft Netlogon : identifiée en août 2020, elle permet à un attaquant distant non authentifié connecté à un contrôleur de domaine (via le protocole Netlogon Remote) de provoquer une élévation de privilèges pouvant avoir pour conséquence l'accès à l'ensemble des ressources gérées par les domaines Active Directory.
  - Vulnérabilité dans Windowds DNS Server : elle permet à un attaquant de provoquer un déni de service ou une exécution de code arbitraire à distance.
  - Vulnérabilité dans Citrix Application Delivery Controller (anciennement connu sous le nom de NetScaler Gateway) : elle permet à un attaquant non authentifié d'exécuter du code arbitraire à distance.

5 OBSERVATOIRE DES VULNERABILITES

5.5 Service national cyber-surveillance

Au regard de leurs responsabilités dans les territoires de santé, les audits de cyber-surveillance ont été prioritairement orientés en 2020 vers les groupements hospitaliers de territoire (GHT), afin de leur permettre d'atteindre le prérequis 2.5 du programme HOP'EN.

L'audit de cyber-surveillance est un service de diagnostic et d'évaluation de la sécurité du système d'information vis-à-vis d'Internet (service national de cyber-surveillance). Ce service de cyber-surveillance est :


Gratuit et mis à la disposition des structures de santé (victime d'un acte de cyber-malveillance ou considérée comme OSE) ;


Confidentiel (seul le RSSI de la structure concernée et les auditeurs y ont accès) ;


En grande partie automatisé (des phases de collecte et de tests jusqu'à la génération du rapport).

Le service de cyber-surveillance réalise un audit des domaines des structures de santé exposés sur Internet déclarés par la structure de santé[5] afin de détecter d'éventuelles vulnérabilités.

Pour ce faire, la plateforme de cyber-surveillance mise en place pour le secteur de la santé :

- Cartographie et détermine la surface d'attaque d'un système d'information à partir d'Internet ;
- Détecte les vulnérabilités qui affectent le système d'information d'une organisation ;
- Détecte une éventuelle fuite de données (code-sources, identifiants, données à caractère personnel, etc.) visant le système d'information.

Le rapport de cyber-surveillance fourni présente :

- Le périmètre de l'évaluation avec la liste des domaines et sous-domaines, avec une cartographie des systèmes détectés ;
- Une synthèse managériale permettant de prendre rapidement connaissance du niveau de sécurité constaté et de la typologie des vulnérabilités ;
- Une synthèse technique présentant :
  - les vulnérabilités détectées par niveau de criticité,
  - un plan d'actions de remédiation hiérarchisé ;
- Le détail des vulnérabilités identifiées avec pour chacune :
  - la criticité,
  - le type de vulnérabilité (ou catégorie, telle que usurpation d'identité, défaut de configuration, …),
  - le SI affecté,
  - la description de la vulnérabilité,
  - la recommandation associée en vue de sa correction.

[5] A l'occasion de ce cadrage, le CERT Santé peut détecter des domaines ou sous domaines non déclarés par la structure

Une fois le diagnostic réalisé, un rapport d'audit est fourni à la structure auditée dans des délais courts afin de lui permettre de rapidement mettre en place les éventuelles mesures de remédiation.

Le périmètre de l'audit ainsi que les attendus du rapport sont présentés sur le portail cyberveille-santé[6]. Ces informations permettent d'encadrer les audits de cyber-surveillance lorsqu'ils sont réalisés par des prestataires à la demande des structures.

En 2020, 44 audits ont été réalisés, soit près du double de 2019 (24, année de déploiement) : quarante GHT, deux CHU et deux établissements privés, soit un total de 272 structures de santé. Le nombre de structures auditées a été multiplié par plus de 7 entre 2019 et 2020 et le nombre de domaines par plus de 2 (plus de 6000 domaines et sous-domaines).

5.6 Service de veille proactive

Dans le cadre de la gestion des incidents de sécurité, le CERT Santé est régulièrement confrontée à des structures de santé faisant la découverte de la compromission d'un de leurs serveurs exposés sur Internet. Ainsi, le CERT Santé a mené en 2020 à titre expérimental de nouvelles activités de veille active en sources ouvertes. Constatant une augmentation des actions malveillantes liées aux accès à distance dès le début de la pandémie COVID-19, le CERT Santé a constitué avec l'aide de l'ANSSI une cartographie des structures de santé présentes sur Internet (adresse IP, nom de domaine, principales technologies utilisées).

Le CERT Santé a intégré une communauté de partage d'indicateurs de compromission (IP, nom de domaine, empreintes de fichiers) appelés IOC qui lui permet de renforcer ses actions en matière de prévention de la menace. Cette communauté utilise la plateforme MISP (plateforme ouverte d'analyse de la cybermenace) gérée par le CERT du Luxembourg (CIRCL). Une organisation esante.gouv.fr a été créée pour maintenir à jour une liste d'IOC pour le secteur santé.

Serveurs identifiés dans des listes noires d'activités cyber-malveillantes

Ces machines compromises sont référencées dans des listes noires gérées par différentes communautés intervenant dans la lutte contre la cybercriminalité (firehol, MISP, DnsBL …).

Le CERT Santé récupère quotidiennement cette liste noire, compare les adresses IP avec celles du secteur santé puis alerte par message électronique le RSSI/ référent sécurité de la structure concernée le cas échéant en précisant le type d'activité malveillante (spam, tentative d'accès brute force, ...) et la liste noire référençant sa plage IP ou son nom de domaine.

Vulnérabilités critiques présentes sur des services exposés sur Internet

Grâce à la veille quotidienne sur les vulnérabilités critiques des composants utilisés par les structures de santé et la cartographie Internet des structures, le CERT Santé est en mesure d'alerter par message électronique le RSSI / référent sécurité des structures qui exposent un service (accès à distance principalement) potentiellement vulnérable sur internet dès la publication de la vulnérabilité (CVE).

[6] https://cyberveille-sante.gouv.fr/cybersurveillance

Dans une optique de prévention des incidents de sécurité, plus de 800 messages d'alertes ont été envoyées à 580 structures sanitaires et médico-sociales en 2020.

5.7 Constat et recommandations

Les structures qui ont été audités ou alertées exposent souvent trop de ressources sur Internet et ne portent pas suffisamment d'attention à la sécurisation de leurs services (portail Web, accès à distance, etc…). L'exploitation de certaines vulnérabilités peuvent permettre à un attaquant d'accéder par rebond à tout ou partie de leur système d'information avec parfois des privilèges élevés. Pour les structures ayant été audités deux fois (principalement des CHU), on constate une réduction significative de la présence de ce type de vulnérabilités.

Les recommandations suivantes sont régulièrement communiquées aux structures :

- Réduire les surfaces d'attaque en désactivant les comptes, protocoles et services qui ne sont pas indispensables: certaines structures de santé auditées exposent un grand nombre de services numériques sur Internet y compris des services de télé-administration reposant sur RDP ou d'autres protocoles. Il a ainsi été démontré la possibilité de prendre le contrôle total de serveurs ;

- Appliquer une politique de mot de passe suffisamment robuste afin d'éviter d'être la cible d'action malveillante depuis Internet (voir guide https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_s%C3%A9curit%C3%A9_mot_passe.pdf);

- Améliorer le suivi des correctifs : des structures de santé exposent sur internet des systèmes avec des composants obsolètes. Il est indispensable d'assurer une veille des composants exposés sur internet et de les mettre à jour suivant un processus éprouvé lorsque des correctifs sont disponibles. La priorité doit être donnée aux correctifs de sécurité correspondants à des vulnérabilités critiques afin de se prémunir au plus vite d'attaques cherchant à les exploiter ;

- Analyser régulièrement les journaux de ses équipements périmétriques : installer un correctif pour une vulnérabilité critique sur un composant exposé sur Internet n'est pas la garantie d'être protégé contre une exploitation antérieure, il faut également analyser ses journaux pour vérifier si elle a été exploitée et en cas de doute renouveler l'ensemble de ses comptes ;

- Renforcer les configurations et la sécurisation des accès : beaucoup de failles détectées lors des audits concernent une mauvaise configuration des protocoles utilisés (par exemple le protocole SSL/TLS utilisé dans le cadre d'échanges chiffrés https) ou une divulgation d'informations sensibles. L'ensemble de ces vulnérabilités peut être corrigé assez simplement par la mise en œuvre de bonnes pratiques ;

- Vérifier la suppression des failles web classiques (présentées dans le Top 10 OWASP7) : se conformer aux bonnes pratiques de développement (par exemple le contrôle des saisies utilisateur). Il peut également être mis en œuvre un web application firewall (WAF) qui bloquera l'essentiel des tentatives d'exploitation des failles référencées par l'OWASP s'il est correctement configuré ;

- Inclure un engagement du prestataire (DPI, Gestion des activités de biologie médicales, gestion des activités de radiologie, etc…) sur le maintien en condition de sécurité de son infrastructure : de nombreuses vulnérabilités critiques ont été ainsi découvertes sur des systèmes gérés par des tiers externes. Lors de la contractualisation d'une prestation avec un tiers, il est essentiel d'inclure des engagements sur le maintien en condition de sécurité ainsi que la possibilité de réaliser des audits.

[7] Le Top 10 OWASP est un document de sensibilisation standard pour les développeurs et la sécurité des applications Web. Il représente un large consensus sur les risques de sécurité les plus critiques pour les applications Web.

6 GLOSSAIRE

ACSS	Accompagnement Cybersécurité des Structures de Santé
ANS	Agence du numérique en santé
ANSM	Agence Nationale de la Sécurité du Médicament et des produits de santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
ARS	Agence Régionale de Santé
CERT	Computer Emergency Response Team
Code malveillant	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau. Remarques : Les virus ou les vers sont deux types de codes malveillants connus.
CORRUSS	Centre opérationnel de réception et de régulation des urgences sanitaires et sociales
Cryptovirus	Rançongiciel - Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.
Cybermalveillance	La cybermalveillance recouvre toute activité criminelle réalisée par le biais d'Internet et des technologies du numérique. Elle englobe toute forme de malveillance effectuée à l'aide de l'informatique, d'équipements électroniques et des réseaux de télécommunication.
Cybersécurité	État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.
DGS	Direction Générale de la Santé
DNS	Délégation au numérique en santé
Forensique	L'analyse forensique en informatique signifie l'analyse d'un système informatique après avoir été victime d'une cyberattaque.
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et Sécurité
LDAP	Lightweight Directory Access Protocol
Phishing	Hameçonnage - Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.
RGPD	Règlement Général sur la Protection des Données

NOTES PERSONNELLES

NOTES PERSONNELLES

Pour aller plus loin, rendez-vous sur :

- le site du Ministère des Solidarités et de la Santé : solidarites-sante.gouv.fr
- le site de l'Agence du numérique en santé : esante.gouv.fr
- le portail cyberveille : cyberveille-sante.gouv.fr/

Pour prendre contact :

- au sein du Ministère des solidarités et de la santé : ssi@sg.social.gouv.fr
- au sein de l'Agence du numérique en Santé : cyberveille@esante.gouv.fr

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

AGENCE DU NUMÉRIQUE EN SANTÉ