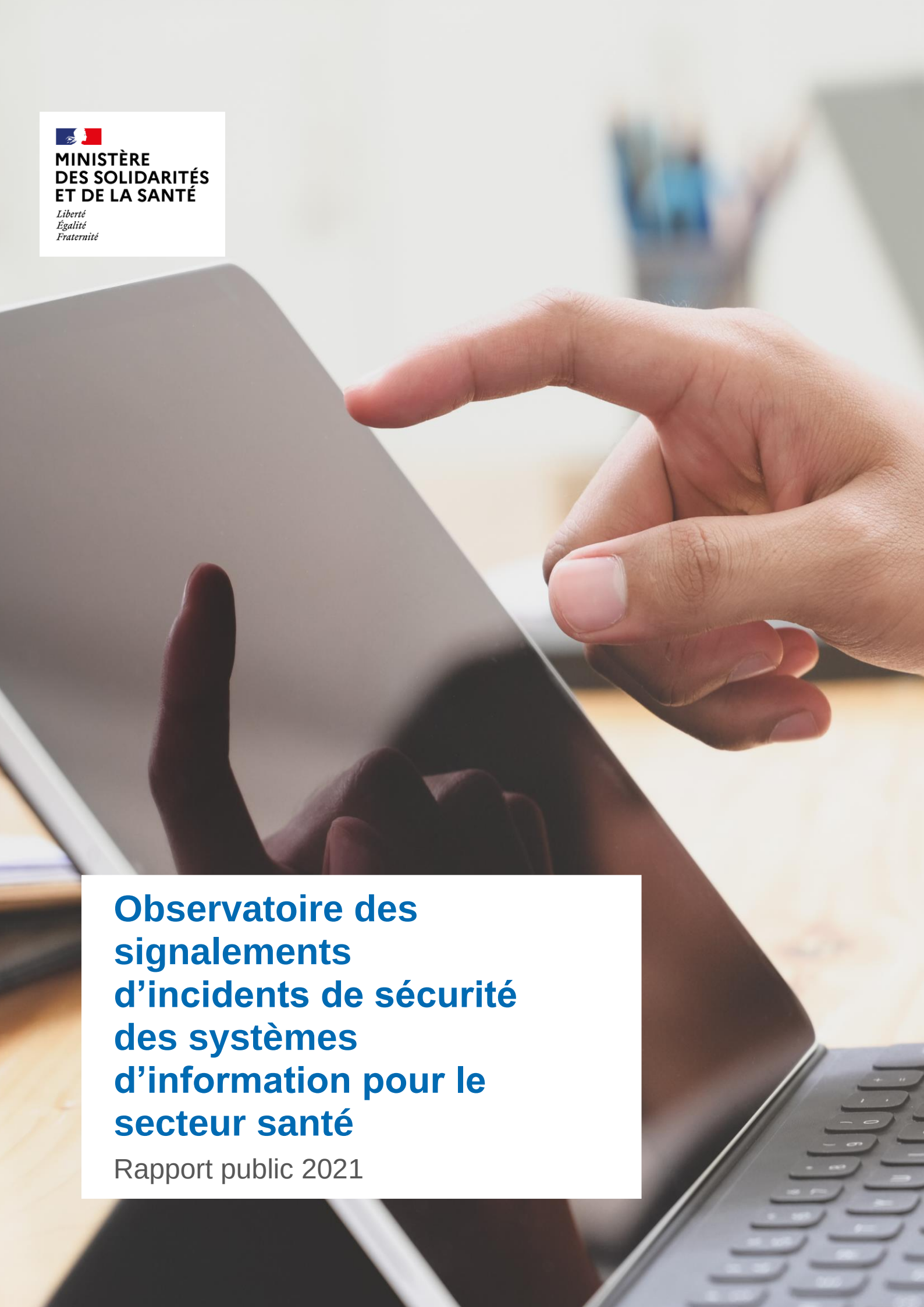
MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

*Liberté*
*Égalité*
*Fraternité*



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

Rapport public 2021

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
*Liberté*
*Égalité*
*Fraternité*

HFDS
HAUT FONCTIONNAIRE
DE DÉFENSE
ET DE SÉCURITÉ

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (2021)

# SOMMAIRE

# TABLE DES FIGURES

# 1 INTRODUCTION

Le renforcement du niveau de sécurité numérique des acteurs du secteur santé est une priorité pour le ministère des Solidarités et de la Santé. Concernant la sécurité opérationnelle, l'Agence du Numérique en Santé joue un rôle central, en particulier depuis l'intégration du CERT Santé au sein de l'InterCERT-FR en janvier 2021.

Aujourd'hui plus que jamais, la mobilisation de tous les acteurs, directions, experts techniques et professionnels de santé est nécessaire afin de parer aux menaces de cybercriminalité qui s'intensifient dans un contexte général instable.

L'année 2021 a été marquée par de nombreux incidents majeurs liés à des attaques par rançongiciel (CH de Dax, Villefranche-sur-Saône ou Arles) mais aussi à l'exfiltration massive de données (AP-HP et encore récemment la CNAM[1]). Il n'y a pas eu cependant à ce jour d'attaque coordonnée visant à désorganiser fortement le système de soins français.

En 2021, le CERT Santé, qui assure également la mission de prévention et d'alerte face aux menaces de cybersécurité auprès des établissements santé et services médico-sociaux, a géré le double de déclarations d'incident (733) par rapport à 2020.

Cette augmentation s'explique en partie par les incidents rencontrés par des prestataires de services (hébergeurs en particulier) ayant une part de marché significative. Plusieurs centaines de structures des secteurs sanitaire et médico-social (40% des incidents signalés) ont ainsi été impactés.

Le nombre moyen mensuel de déclaration a lui aussi augmenté de 33%, même s'il reste relativement faible au regard du nombre de structures concernées par cette obligation de déclaration.

La déclaration des établissements et services médico-sociaux est en forte hausse (multipliée par 4) par rapport à 2020, en particulier pour les établissements accueillant des personnes en situation de handicap, ce qui atteste de leur bonne compréhension de l'extension du dispositif à leur secteur d'activité.

Avec le Ségur du numérique en santé et France Relance, le ministère des Solidarités et de la Santé, avec l'appui opérationnel de l'ANS, et l'ANSSI ont investi massivement dans l'amélioration de la sécurité des systèmes d'information de santé. La collaboration entre l'ANS et l'ANSSI en matière d'alerte et de réponse à incident s'est accentué en 2021. Les deux agences œuvrent en synergie pour aider les acteurs à gagner en maturité et atteindre un niveau de résilience collective indispensable pour surmonter une attaque de grande ampleur.

Depuis le début de l'année 2022, le CERT Santé renforce son accompagnement et améliore les outils mis au service des établissements et acteurs de la santé et du médico-social pour les aider à développer leur capacité à faire face à une menace toujours plus complexe.

Un seul mot d'ordre collectif : **TOUS CYBERVIGILANTS !**

*Annie Prévot et Jacques Lucas,*
*Directrice générale et Président de l'Agence du Numérique en Santé*

[1] https://www.cnil.fr/fr/fuite-massive-de-donnees-de-sante-comment-savoir-si-elle-vous-concerne-et-que-pouvez-vous-faire

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

## 2.1 Contexte réglementaire et organisationnelle

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.

Le CERT Santé, porté par l'ANS, est le premier CERT sectoriel en France. Il a intégré en janvier 2021 l'Intercert FRANCE (anciennement InterCERT-FR) après avoir été accompagnée par l'ANSSI pour gagner en maturité dans la mise en œuvre de ses services. L'InterCERT France est une association loi 1901 qui constitue la première communauté de CSIRT[2] en France. En tant que membre de l'InterCERT France, le CERT Santé bénéficie des retours d'expérience et de la coopération avec les autres CSIRT/CERT dans sa lutte contre les menaces de cybersécurité.

## 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.

[2] Computer Security information Response Team

Sa mise en œuvre opérationnelle s'appuie sur le CERT Santé de l'Agence du numérique en santé qui a intégré l'InterCERT-FR en janvier 2021.

### 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.

Le 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[3], 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…) ;
- Orientation vers un prestataire cyber 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 :

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

- 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) ;
- Proposer des solutions pour renforcer la sécurité (configuration des systèmes, solutions concrètes de sécurisation des sauvegardes, hyperviseurs, de l'administration, du cloisonnement réseau, etc…) basées sur les guides de l'ANSSI.

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 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 trois fois par an 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 sur 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 5.1.

## Intervention de l'ANS en cybersécurité au-delà du champ opérationnel

Les activités du CERT Santé sont parties prenantes d'une intervention plus large de l'ANS dans le domaine de la prévention qui concoure à l'amélioration de la sécurité du numérique en Santé. Elles sont rappelées ci-dessous à titre d'information.

### 1. *PGSSI et gestion d'une identité numérique*

L'Agence est responsable de la politique générale de sécurité des systèmes d'information de santé. C'est un corpus de référentiels et de documents opposables mais aussi de guides techniques mis à disposition de l'écosystème pour renforcer la sécurité.

En novembre 2021, un mémento de sécurité informatique ne nécessitant pas de connaissance technique préalable a été mis à disposition des professionnels de santé (PS) en exercice libéral. Il rassemble des règles d'hygiène informatique permettant aux PS de se prémunir contre la majorité des attaques informatiques, ou à défaut d'en limiter les impacts.

Le Ministère des Solidarités et de la Santé (MSS) et l'Agence du Numérique en Santé ont travaillé depuis plus d'un an à construire des référentiels opposables pour garantir une identité numérique pour les personnes physiques et morales du secteur sanitaire et médico-social ainsi que pour les patients.

Un premier référentiel définit des exigences sur l'identification à des services numériques traitant des données de santé à caractère personnel. Concrètement, cela consiste notamment à imposer l'utilisation de mots de passe suffisamment forts, un deuxième facteur d'authentification (code à usage unique, etc.) et à se baser sur des informations d'identification des utilisateurs issues des répertoires de référence (INS, RPPS, FINESS). Ce nouveau référentiel est le premier de la politique générale de sécurité des systèmes d'information en santé (PGSSI-S) à être rendu opposable par arrêté ministériel (arrêté du 28 mars 2022).

### 2. *Doctrine, maturité, référencement*

Responsable de l'élaboration et de la promotion de la PGSSI-S, l'ANS se mobilise pour accompagner les acteurs dans leurs démarches de mise en conformité.

Ainsi dans le cadre du Ségur du numérique en santé, les exigences relatives aux dispositifs s'interfaçant avec Pro Santé Connect ou l'INS, sont vérifiées préalablement à leur référencement. Les applications disponibles dans le store Mon Espace Santé feront également l'objet d'une vérification de conformité.
Enfin, des audits pourront être conduits sur l'ensemble du parc installé aussi bien pour les référencements Ségur que MES.

### 3. *Une collaboration avec les ARS pour renforcer les actions en région*

Le MSS a confié un rôle clé aux ARS dans la déclinaison territoriale de son plan de renforcement de la cybersécurité. Fort de leurs liens de confiance, l'ANS, les ARS et les GRADeS ont mis en place un groupe de travail qui a rapidement défini des actions prioritaires. Ainsi, pour faire face à une menace de cybersécurité grandissante, des travaux ont été initiés concernant la mise en place d'un exercice de gestion de crise adapté au niveau de maturité de la structure. Trois scénarii d'exercice seront élaborés pour être ensuite déployés à l'ensemble des régions.

# 3 Synthèse de l'activité en 2021

En 2021, 582 établissements ont déclaré 733 incidents, soit pratiquement le double par rapport à 2020. Cette hausse est liée non seulement à des incidents majeurs rencontrés par des prestataires et ayant impacté plusieurs centaines de structures des secteurs sanitaire et médico-social (40% des incidents signalés) mais également à un taux mensuel moyen de déclaration ayant augmenté de 33% passant de 30 à 40 signalements par mois (hors incidents prestataires). Le taux de déclaration reste relativement faible au regard du nombre de structures concernées par cette obligation[4].

La déclaration des ESMS est en forte hausse (multiplié par 4) par rapport à 2020, en particulier pour les établissements accueillant des personnes en situation de handicap, ce qui atteste de leur bonne compréhension du dispositif mis en place.

Durant cette année, des établissements et des prestataires (en particulier du secteur médico-social) ont subi des sinistres majeurs à la suite d'une attaque par rançongiciel. Certains établissements de santé ont été contraints de poursuivre leurs activités en mode dégradé pendant plusieurs mois, le temps de reconstruire ou de durcir leur SI afin qu'il soit plus résilient face aux menace cyber. L'ANSSI s'est particulièrement mobilisée dans la conduite des actions de réponse à incident avec la DSI de l'établissement lorsqu'une présence permanente dans la gestion de la crise était nécessaire.

Une centaine de structures a déclaré avoir été les victimes collatérales d'incidents majeurs de prestataires (4) victimes d'attaques par rançongiciel. En effet, ces prestataires ont été contraint d'interrompre leur service de manière prolongée, non seulement pour répondre à l'incident mais aussi bloquer toute propagation éventuelle d'une attaque vers le SI de leurs clients.

Le nombre de structures ayant formulé une demande d'accompagnement a doublé en 2021. Le CERT Santé est intervenu à de nombreuses reprises pour identifier l'origine de la compromission et proposer un plan de remédiation. Lorsque la réponse à incident nécessitait une intervention sur site, en particulier pour la reconstruction dans des délais contraint d'un SI intègre, la structure a fait appel à un prestataire cyber spécialisé dans ce type d'opération. Dans de nombreux incidents, le CERT-Santé et l'ANSSI ont coordonné leurs actions pour apporter l'appui le plus efficace aux structures selon la nature des actions à réaliser (confinement, investigation, appui à la gestion de crise, remédiation).

Comme en 2020, les fuites de données concernant les identifiants d'accès à distance et la compromission de comptes de messagerie ont été nombreuses. Dans certains cas, l'attaquant a été en mesure de pénétrer au sein du SI de la structure pour déployer un code malveillant (rançongiciel et cryptominer dans la majorité des compromissions).

De même, des vulnérabilités critiques concernant la messagerie Exchange et des accès VPN (Fortinet, Pulse, …) ont été publiées et ont fait l'objet d'une activité malveillante importante. Aussi le CERT Santé a mené cette année plusieurs campagnes d'alertes (1959 alertes envoyées en 2021 (+143% par rapport à 2020) à plus de 1100 structures). En mettant rapidement à jour leur systèmes, les structures se sont protégées des campagnes d'exploitation massives de ces vulnérabilités. Par ailleurs, le CERT Santé est également intervenu auprès des structures ayant identifié une compromission éventuelle de leur accès avant la mise à jour de leur système. Dans plus de 40 cas, cela a permis de mettre en place les mesures de remédiation réduisant ainsi la possibilité aux attaquants de pouvoir mener une attaque de plus grande ampleur sur leur SI.

---

[4] 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.

# 4 OBSERVATOIRE DES SIGNALEMENTS

## 4.1 Chiffres clés pour la période 2020-2021

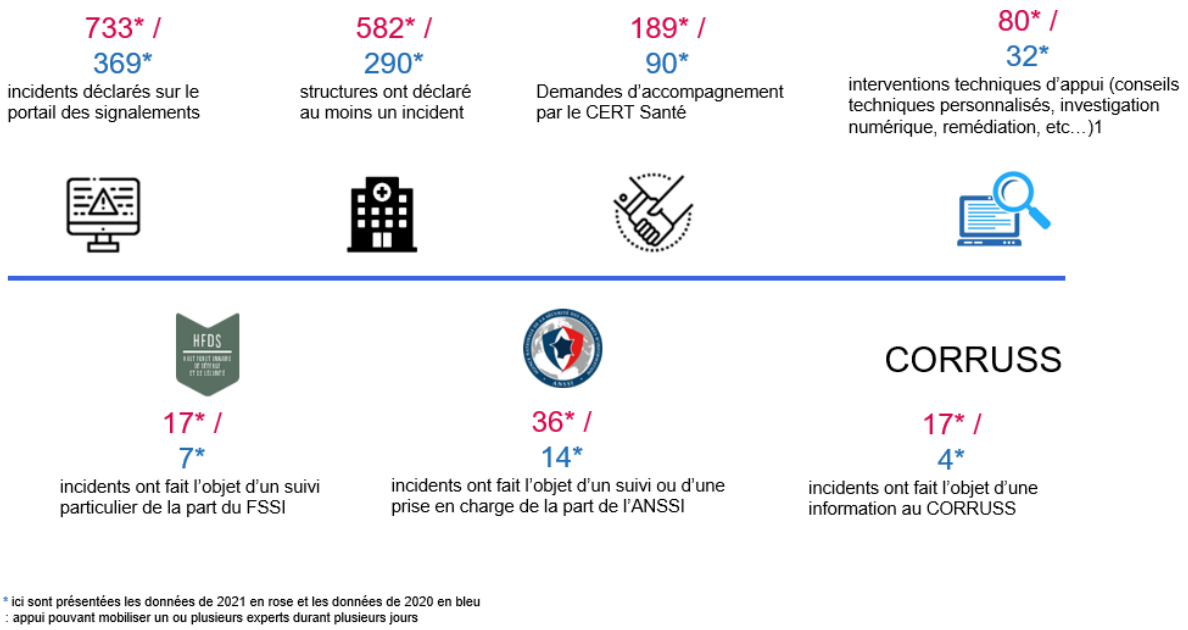



*Figure 1 – Chiffres clés des signalements déclarés en 2020 et 2021*

En coordination avec le CERT Santé, l'ANSSI et le FSSI sont intervenus directement au profit de 37 structures de santé, dans le suivi de la gestion d'un incident ou l'appui à la réponse. Certaines structures ont bénéficié de plusieurs interventions et le FSSI est intervenu à de nombreuses reprises auprès de prestataires sectoriels.

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

- Vingt-neuf établissements de santé publics, dont 18 opérateurs de services essentiels (OSE). Ces incidents étaient liés à des attaques par rançongiciel, des compromissions par des chevaux de Troie, des compromissions de comptes (AD, VPN ou messagerie), la vente d'identifiants sur Internet, l'exploitation de vulnérabilités sur des équipements de sécurité ou des dysfonctionnements graves de systèmes critiques ;
- Deux établissements privés et un EHPAD victimes d'un rançongiciel ;
- Un Groupement de Coopération Sanitaire dont une adresse IP figurait dans la liste d'une campagne d'attaque ciblant la France ;
- D'un prestataire de solutions métier pour les établissements médico-sociaux qui a été victime d'un rançongiciel.

Pour le FSSI du MSS, il s'agit de :

- Sept établissements dont un OSE. Ces incidents étaient liés à des attaques par rançongiciels, à la compromission de SI et au dysfonctionnement grave d'un système critique ;

- Neufs prestataires fournisseurs de services spécifiques aux secteurs santé et médico-social ou des fournisseurs de services Telecom ou d'hébergement. Ces incidents avaient pour origine des attaques par rançongiciel, une indisponibilité des services d'hébergement ou téléphoniques.

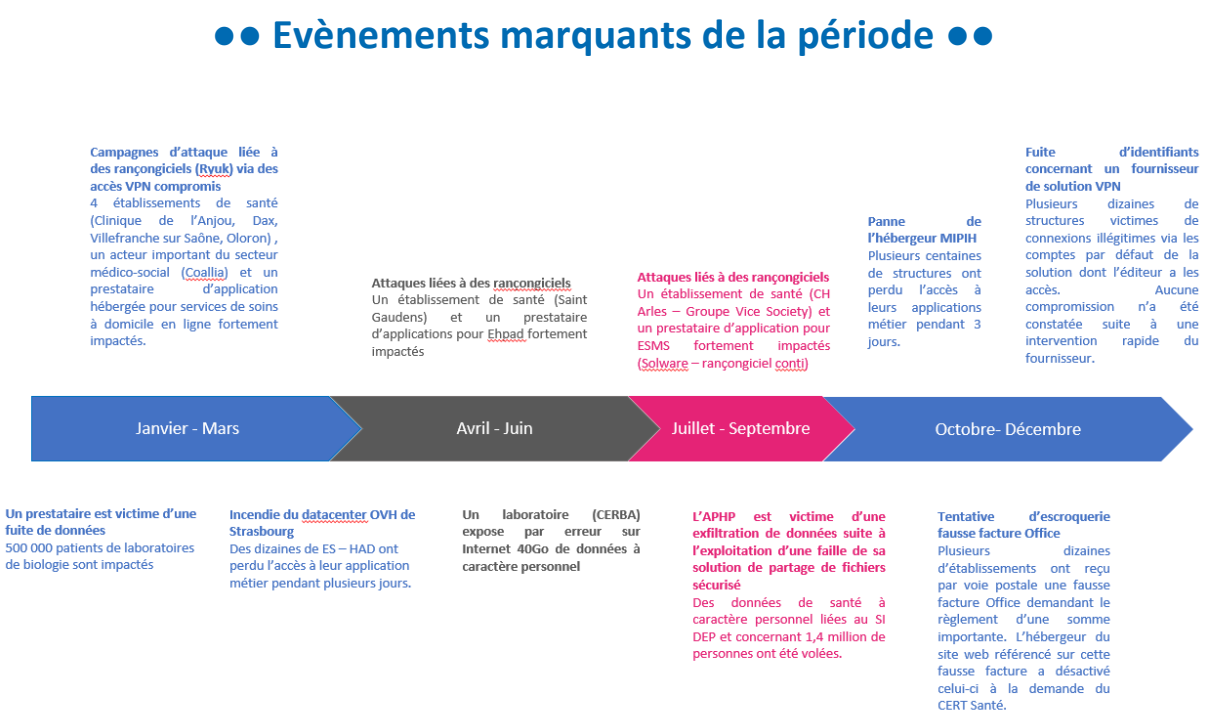



*Figure 2 – Evènements marquants de l'année 2021*

## 4.2 Informations générales sur les signalements

**733 incidents ont été déclarés en 2021**. Ce nombre a presque doublé par rapport à 2020 (369). Pour mémoire, 392 incidents avaient été déclarés en 2019.

Parmi ces incidents, on compte des incidents « hors périmètre ». La majorité des incidents non traités par le CERT Santé sont des incidents ne concernant pas un système d'information support d'une activité sanitaire ou médico-sociale. On comptabilise également dans cette catégorie les exercices de crise cyber qui intègrent une déclaration de l'incident au CERT Santé (4).

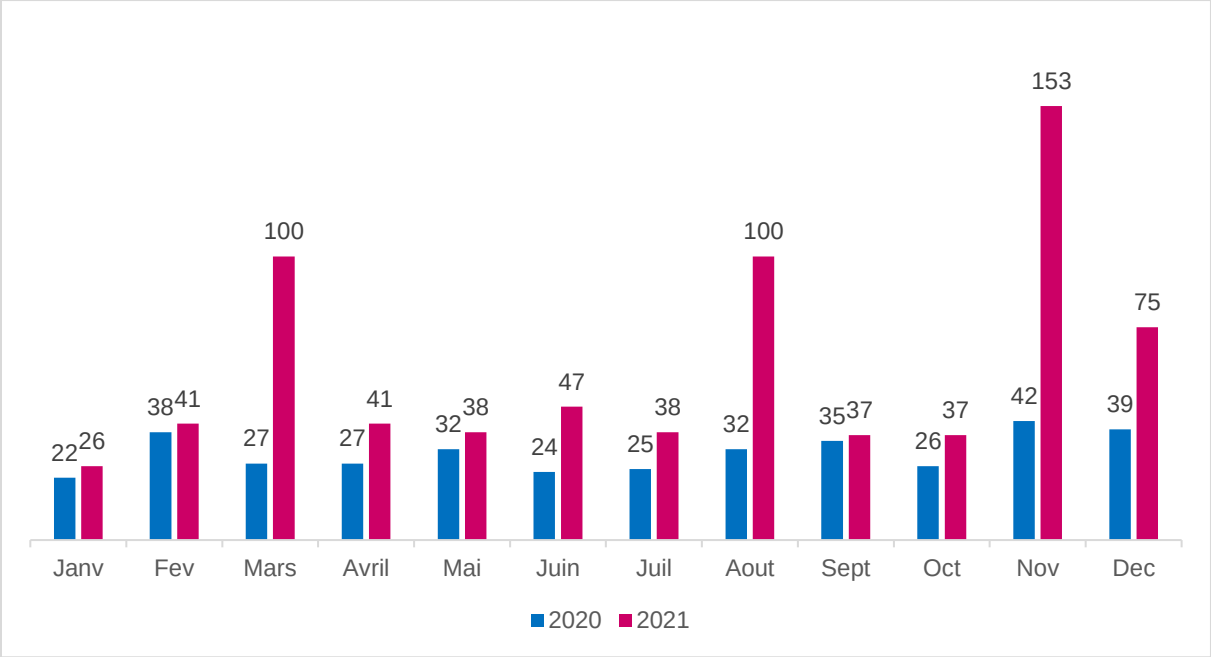



*Figure 3 - Nombre de signalements par mois*

La nette augmentation des déclarations s'explique par un nombre important de déclarations en mars, aout et novembre 2021. Elles sont liées à des incidents ayant touché des hébergeurs d'applications métier des secteurs sanitaire et médico-social et ayant entrainé l'interruption des services et l'impossibilité pour les structures d'accéder à leurs données. On compte en 2021 une moyenne de 61 déclarations par mois (31 en 2020).

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

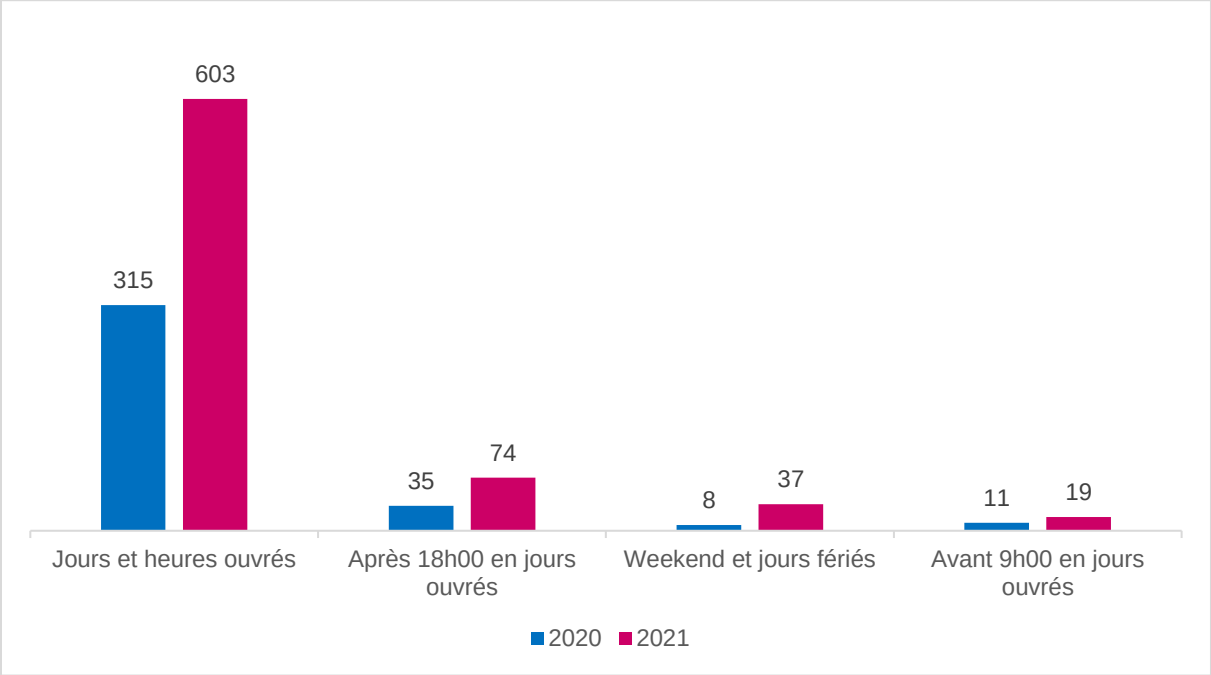



*Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt*

**82%** des signalements ont été effectués en heures et jours ouvrés (HO/JO) en 2021, 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, trois structures (un CH et deux hôpitaux privés à but non lucratif) nécessitaient un appui suite à une attaque par rançongiciel entrainant une interruption du SI support de nombreux services de prise en charge des patients. Ces déclarations ont été réalisées en semaine en soirée ou avant 9h du matin. Elles ont été prises en charge rapidement par le CERT Santé et deux structures nécessitaient un accompagnement sur site au regard de l'ampleur du sinistre. Elles ont également bénéficié d'un appui de l'ANSSI. La troisième a été en mesure de gérer l'incident avec son prestataire informatique. Pour l'ensemble de ces demandes d'accompagnement HNO/JNO, aucune mise en danger patient avérée n'a été relevée.

## ●● Etat des incidents lors de leur signalement ●●

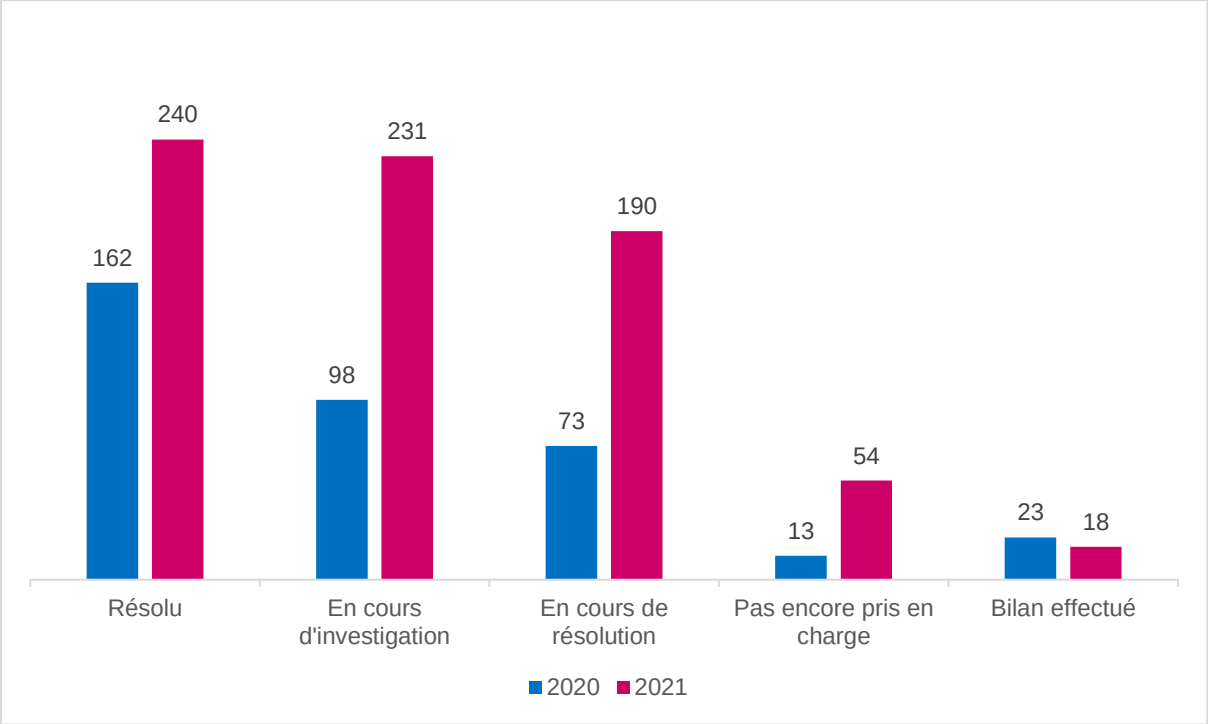



*Figure 5 - Etat des incidents lors de leur signalement*

En 2021, comme en 2020, plus de la moitié des incidents sont résolus ou en cours de résolution par la structure avant leur déclaration. En revanche, la part des signalements résolus baisse en 2021, en particulier au profit d'incidents déclarés « **En cours d'investigation** ». Depuis 2019, le CERT Santé est davantage sollicité par les structures pour des actions d'investigation et la mise en place de mesures de remédiation. Sur trois ans, cette part augmente chaque année, pour atteindre **31% en 2021**.

**33** 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.

**26%**

C'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2021**. Il est **stable par rapport à 2020 (27%)**.

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 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 use alors du maximum de ses prérogatives afin d'appuyer les structures qui en font la demande, généralement avec l'appui du FSSI du MSS, ou bien oriente celles-ci vers l'interlocuteur le plus compétent pour agir.

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

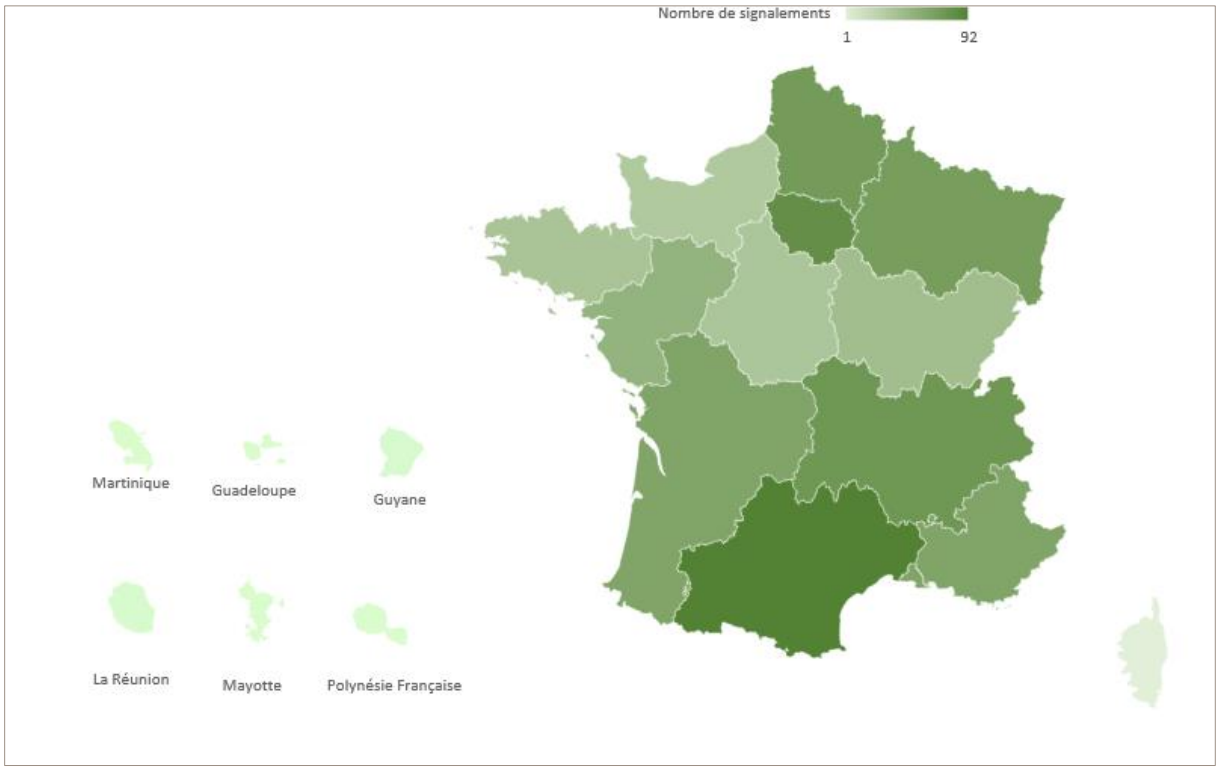



*Figure 6 - Répartition des signalements par région*

Les régions pour lesquelles le nombre de signalements est le plus important sont l'Occitanie et l'Ile-de-France avec respectivement 92 et 81 signalements. Ces deux régions représentent à elles seules plus de 24% du total des signalements.

Au moins un incident a été déclaré dans chaque région.

## ●● Nombre de signalements rapporté à l'activité hospitalière des régions ●●

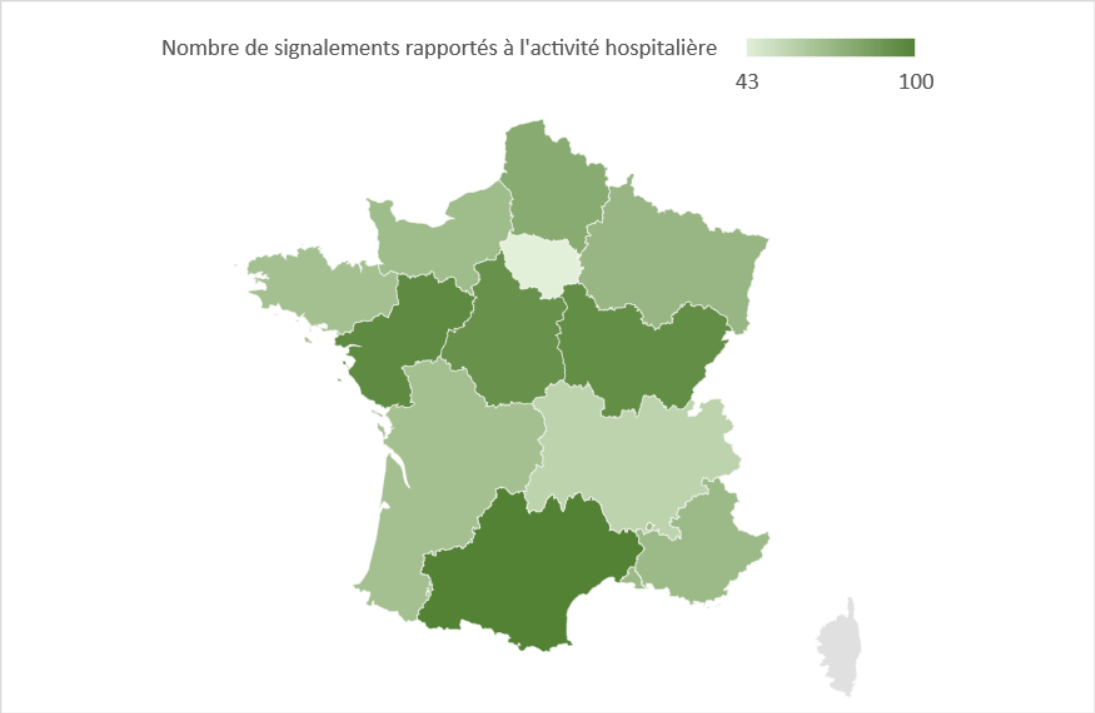



*Figure 7 - Nombre de signalements rapporté à l'activité hospitalière des régions*

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 (Occitanie) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (9% de l'activité nationale), la région Occitanie est en tête en matière de remontée des incidents. Les régions Pays de la Loire, Bourgogne Franche-Comté et Centre Val de Loire arrivent en deuxième position avec un ratio quasi-identique.

En revanche, la région Ile de France déclare peu d'incidents au regard du nombre d'établissements hospitaliers situés sur ce territoire 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 ●●

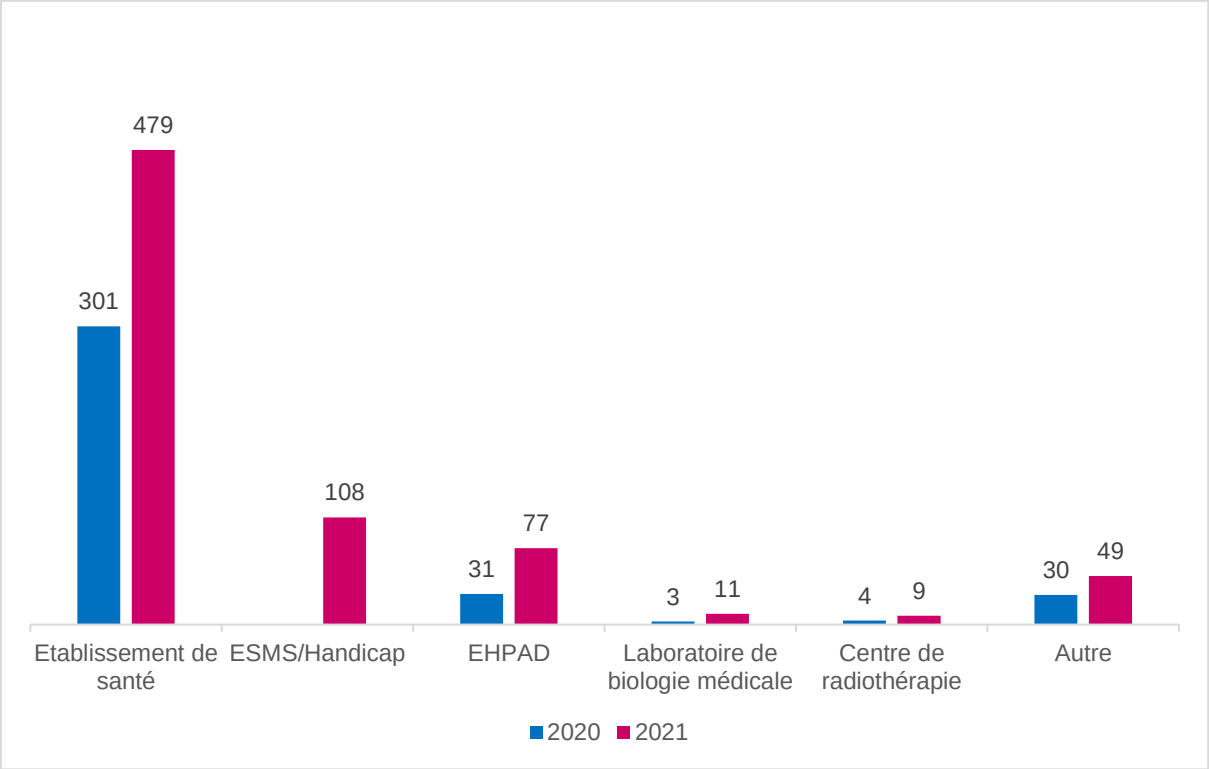



*Figure 8- Répartition des signalements selon le type de structure*

La majorité (65%) des incidents de sécurité est déclarée par les **établissements de santé** (voir détail figure 7). Cependant, elle baisse au profit d'une nette augmentation des déclarations issues des établissements et services médico-sociaux (25% au lieu de 8% en 2020).

La catégorie « Autre » est en augmentation cette année et correspond à des déclarations réalisées par des cabinets libéraux ou des GRADeS.

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

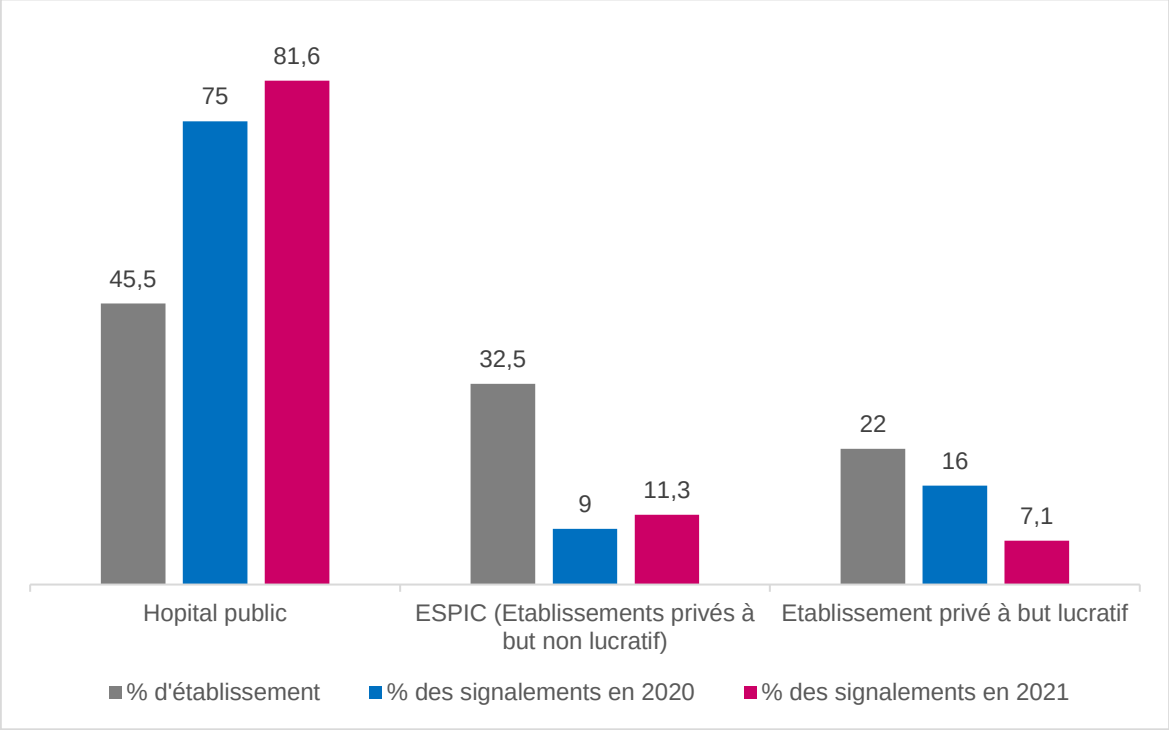



*Figure 9 - Part des signalements comparée à la part des établissements selon leur raison sociale*

La part des **établissements publics** dans la déclaration des incidents a encore augmenté en 2021. Celle des établissements privés à but lucratif a été divisée par un peu plus de 2. **97 établissements référencés OSE** ont déclaré au moins un incident en 2021.

**72** C'est le nombre de structures ayant déclaré plus de 2 incidents durant l'année 2021 sur 582 structures au total. 14 d'entre elles ont signalé au moins quatre incidents.

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

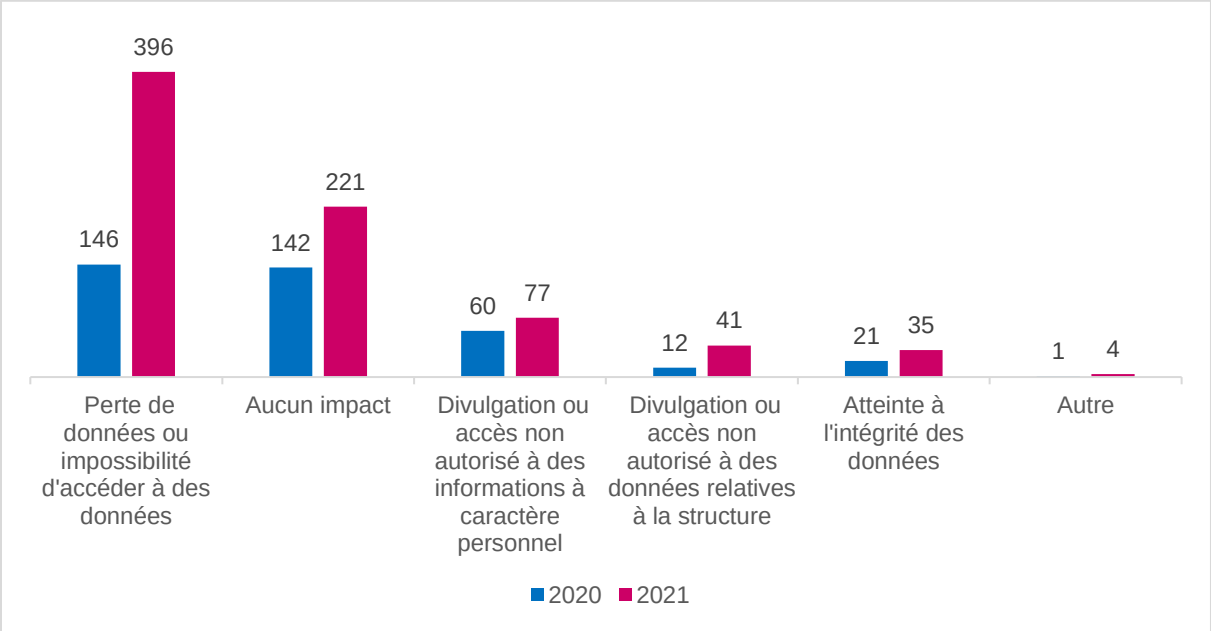



*Figure 10- Répartition selon les types d'impact sur les données*

**Pour la moitié des incidents signalés en 2021, tout ou partie des données des applications de la structure n'étaient plus accessibles**. Ces incidents avaient une origine malveillante (rançongiciels) ou non malveillante (panne de l'hébergeur).

Pour 30% 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.

**45%** C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2021. Ce chiffre est en augmentation puisqu'il était de 35% en 2020 et de 38% en 2021.

52%

C’est le pourcentage de structures qui ont été contraintes de mettre en place en 2021 un **fonctionnement en mode dégradé** du système de prise en charge des patients (7% de plus qu’en 2020). 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. **3**% 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●●

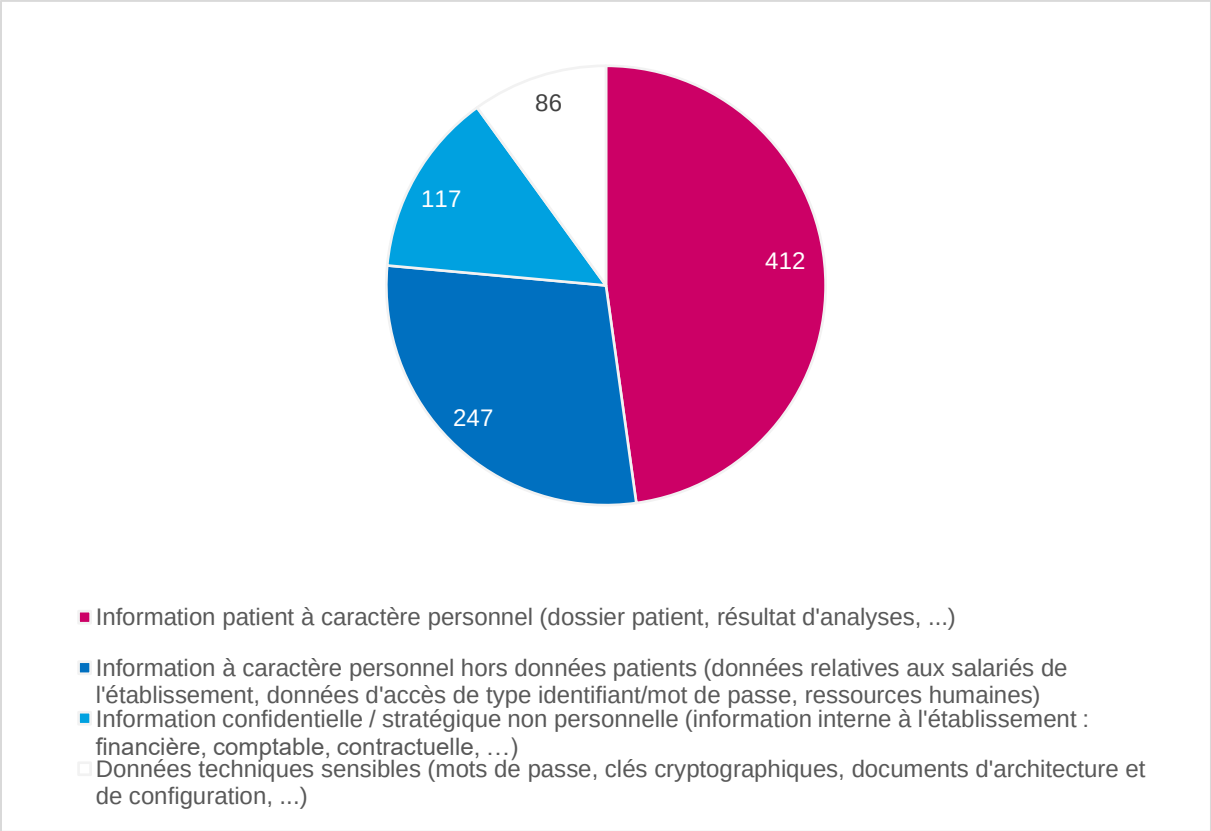



*Figure 11 - Répartition selon les types de données impactées*

**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, **56%** touchent des **données de santé à caractère personnel**, 34% des informations à caractère personnel hors données patient, 16% des informations confidentielles ou stratégiques (principalement des identifiants de compte utilisateurs) et enfin 12% des données techniques sensibles. Les données personnelles sont donc les premières atteintes par les incidents de sécurité déclarés.

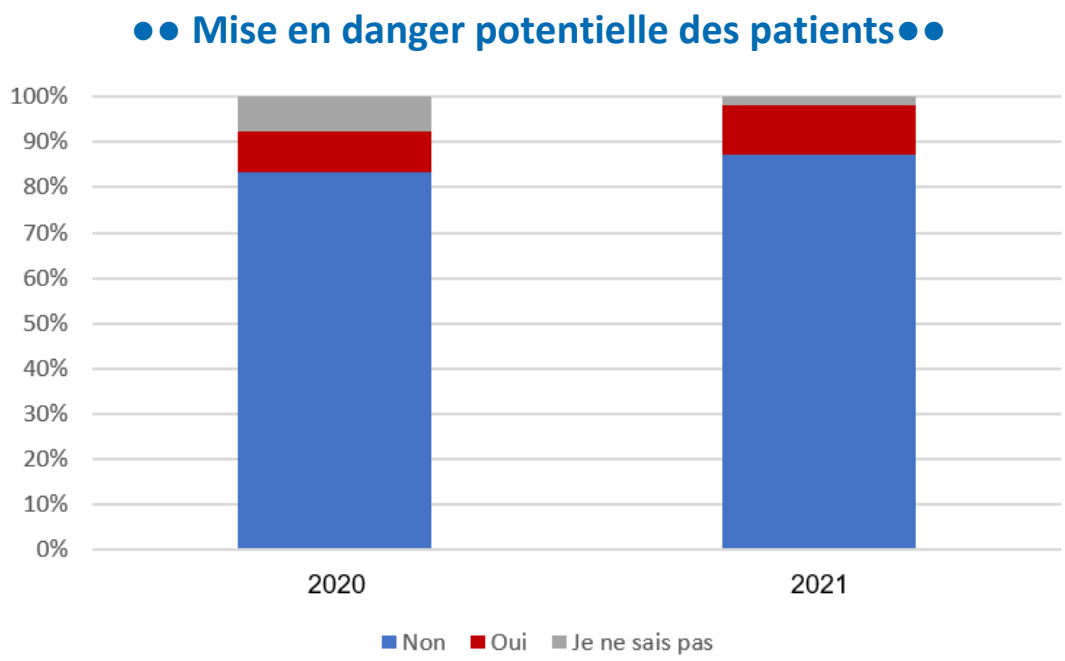



*Figure 12 - Mise en danger potentielle des patients*

Parmi les **80 mises en danger patient** de cette année 2021 (11% du nombre total d'incidents), **5** incidents ont entrainé une **mise en danger patient avérée**.

Concernant les 94% restant (75), correspondant à la part de mises en danger **potentielles** de patients, on retrouve principalement des incidents liés à l'interruption de services hébergés durant plusieurs jours ou du service téléphonique support du SAMU.

Par ailleurs, 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 ●●

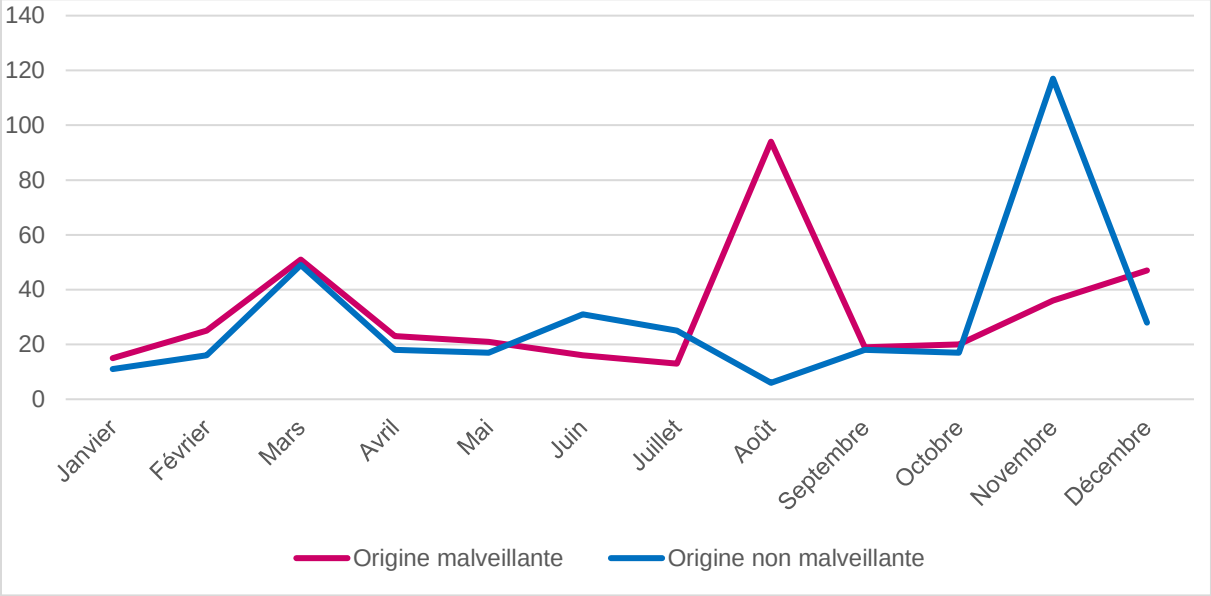



*Figure 13 - Répartition selon le type d'incident*

Parmi **les incidents déclarés, 52% sont d'origine malveillante et 48% d'origine non malveillante**. Dans l'analyse détaillée de ces deux catégories d'incidents, sont exclus les 46 signalements dits « Hors périmètre » n'ayant pas fait l'objet d'un traitement particulier. Les deux pics correspondent à des incidents ayant impactés des hébergeurs de solutions applicatives pour les acteurs sanitaires et médico-sociaux.

## Les actes malveillants

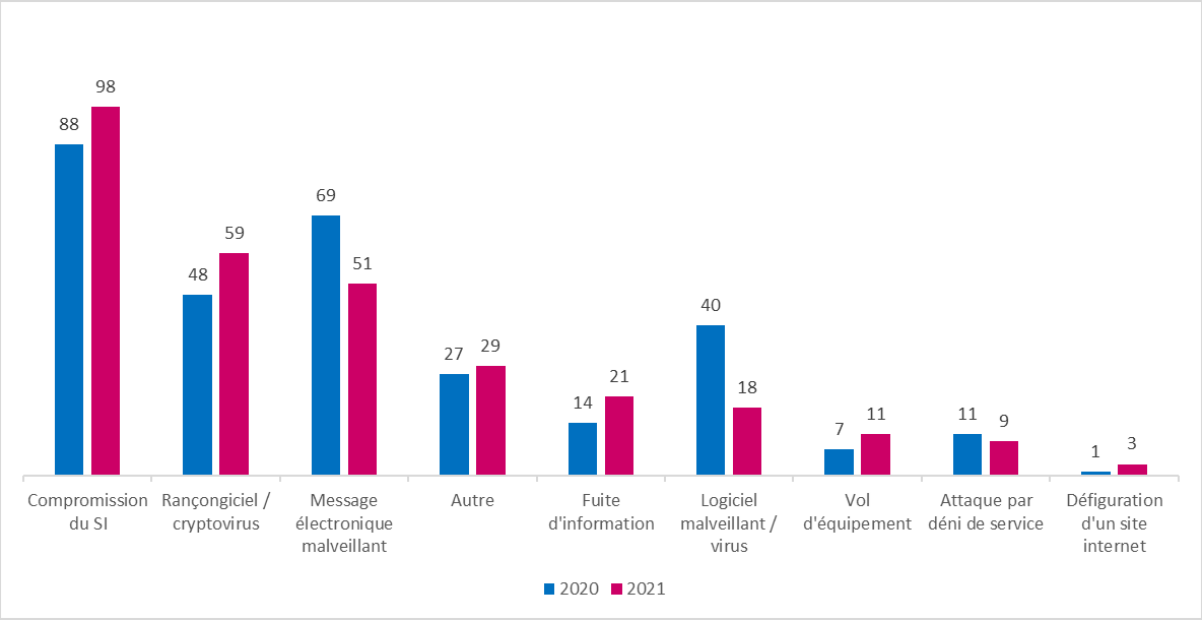



*Figure 14 - Nombre d'incidents par type d'origine*

L'année 2021 a été marquée par une forte activité malveillante relative au vol d'identifiants (login – mot de passe) de comptes de messagerie et de comptes d'accès à distance. Les attaquants récupèrent les identifiants selon trois modes opératoires : la technique de l'hameçonnage (phishing), l'exploitation de vulnérabilités sur des équipements qui n'ont pas été mis à jour et les tentatives de récupération en testant un grand nombre de mots de passe (technique de brute force). Les acteurs malveillants qui cherchent à compromettre les SI ne sont pas nécessairement ceux qui ont récupéré les mots de passe. En effet, des groupes d'attaquants sont spécialisés dans l'exploitation des vulnérabilités des solutions exposées sur Internet pour récupérer des identifiants et les revendre sur le « darknet ».

A partir de l'obtention d'un compte utilisateur, l'acteur malveillant va chercher à obtenir des accès privilégiés sur le SI soit en réalisant une activité d'hameçonnage en interne de la structure soit en exploitant des faiblesses du SI qui lui permettront d'élever ses privilèges. Lorsque l'acteur cherche à extorquer des fonds à sa victime, il déploie un rançongiciel pour bloquer son SI.

Les attaques par rançongiciel ont été particulièrement importantes lors du premier trimestre entrainant des sinistres majeurs pour certaines structures. Il a été constaté « une sorte d'accalmie » entre avril et novembre mais elles sont de nouveau en augmentation depuis décembre 2021.

Une augmentation des attaques par rançongiciel visant les fournisseurs de service (hébergeurs de solutions métier) a été constaté. Les attaquants cherchent à compromettre le SI du prestataire afin de pouvoir se propager sur le SI de l'ensemble de ses clients et démultiplier les effets d'une attaque. Aucune propagation de la compromission du SI d'un prestataire n'a été relevé en 2021.

Plusieurs mécanismes de déchiffrement (et leur clé associée) permettant de recouvrir des données à la suite d'une attaque par rançongiciel (Avaddon, REvil/Sodonikibi, Black Byte, etc…) ont été publiés en 2021. Ils ont fait l'objet de bulletins d'information sur le portail cyberveille-santé.

**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.

Pour renforcer la sécurité de son SI face à la menace rançongiciel et les conséquences d'une compromission majeure, le CERT Santé a publié en avril 2021 un plan d'action préventif se focalisant sur 5 points stratégiques du système d'information (SI) : système de sauvegarde, système de gestion des environnements, administration des systèmes, l'accès à distance par VPN et le proxy.

Les fuites d'information concernent des identifiants de connexion (principalement à des VPN) et des données de santé à caractère personnel.

La catégorie « Autre » concerne principalement des tentatives d'escroquerie liées à une nouvelle campagne d'envoi de factures papier frauduleuses usurpant l'identité graphique d'Office Pro. Il y a également des déclarations relatives à l'usurpation d'identité dans le cadre de l'accès à des SI nationaux.

Notons qu'une part des incidents (22%) relève de plusieurs qualifications. Par exemple, une attaque par rançongiciel, suite à la compromission d'un compte VPN lié à des identifiants en vente sur Internet relève des catégories suivantes : « fuite de données », « compromission de SI » et « rançongiciel ».

La catégorie « Logiciel malveillant / virus » correspond aux codes malveillants pouvant être utilisés pour déployer des rançongiciels (emotet, trickbot), pour générer de la cryptomonnaie ou pour perturber le fonctionnement des machines.

**52%** C'est le pourcentage en 2021 des incidents qui ont une origine malveillante. Ce chiffre **a diminué de 8%** depuis l'année précédente.

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

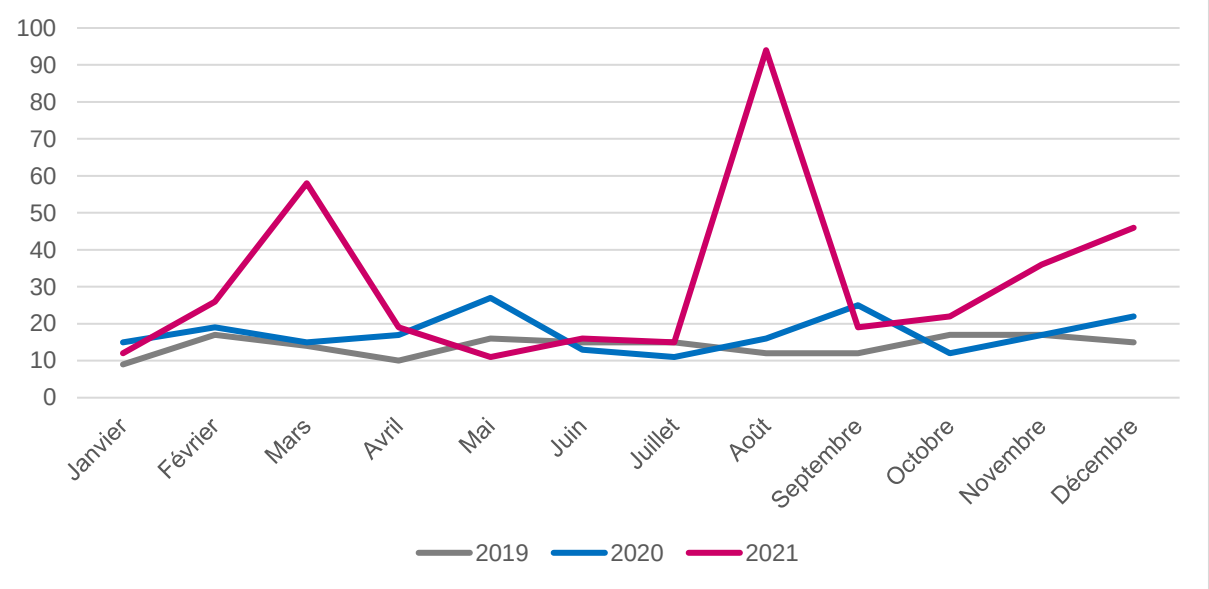



*Figure 15 - Evolution du nombre d'incidents dont l'origine est malveillante*

Les deux pics de signalements correspondent à des attaques par rançongiciel de prestataires qui ont conduit à l'interruption de services pour les structures.

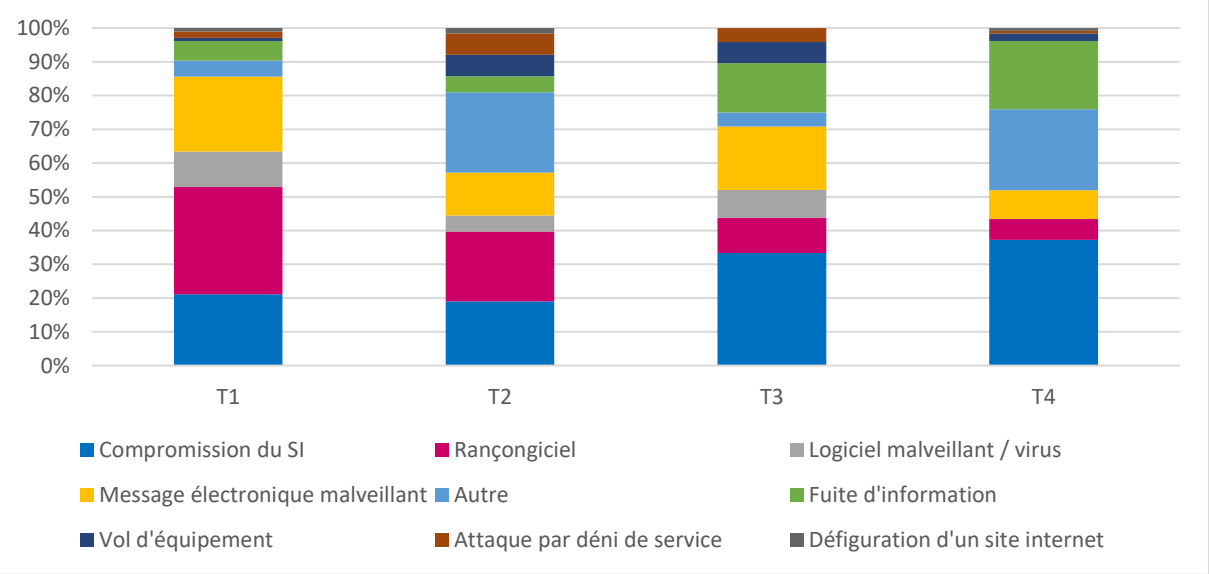



*Figure 16 - Origine malveillante des incidents par trimestre*

La frise chronologique suivante présente les rançongiciels et les principales vulnérabilités ayant fait l'objet d'une exploitation (mais sans lien avec les attaques par rançongiciel) et qui ont été identifiés au cours de l'année :

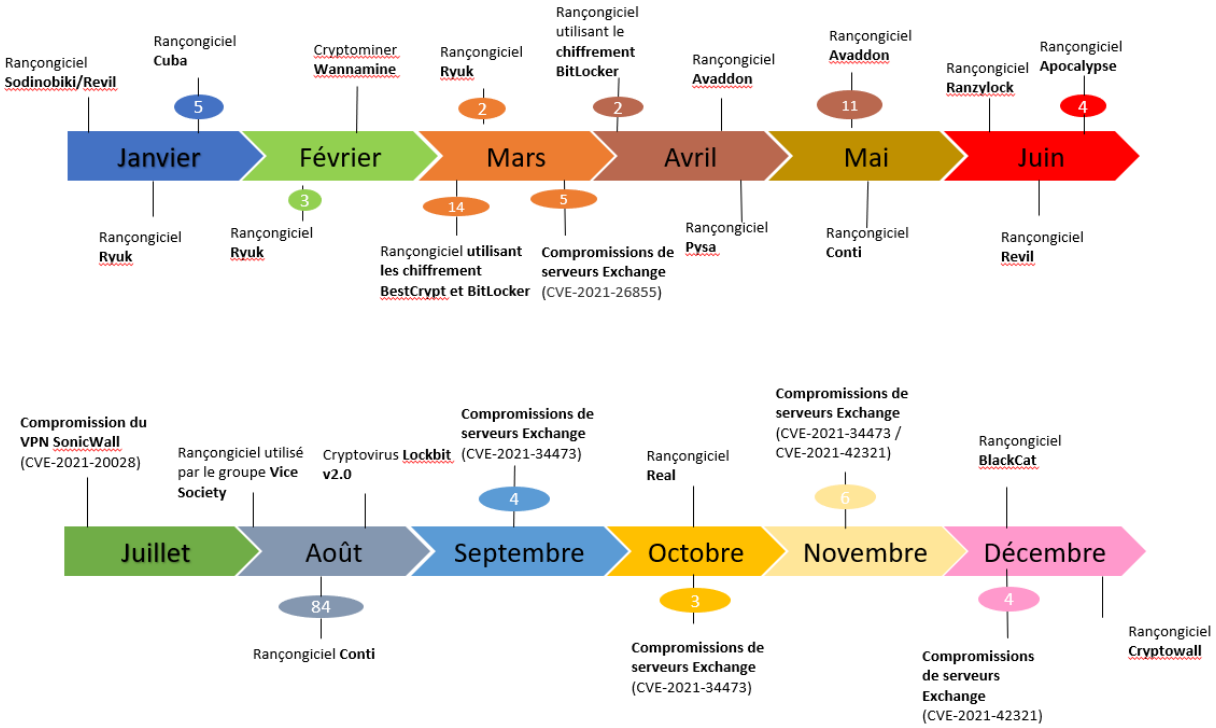



*Figure 17 - Chronologie des cyber-menaces identifiées en 2021*

En 2021, le CERT Santé s'est fixé comme objectif de proposer aux structures un accompagnement dans la durée dans la mise en œuvre du plan préventif de durcissement présenté plus haut. Les actions proposées sont basées sur des recommandations issues des guides de l'ANSSI. Le support de cette démarche est présenté sous la forme de fiches et de questions permettant d'identifier les mesures à mettre en œuvre et de prendre en compte leur mise en œuvre dans le temps.

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

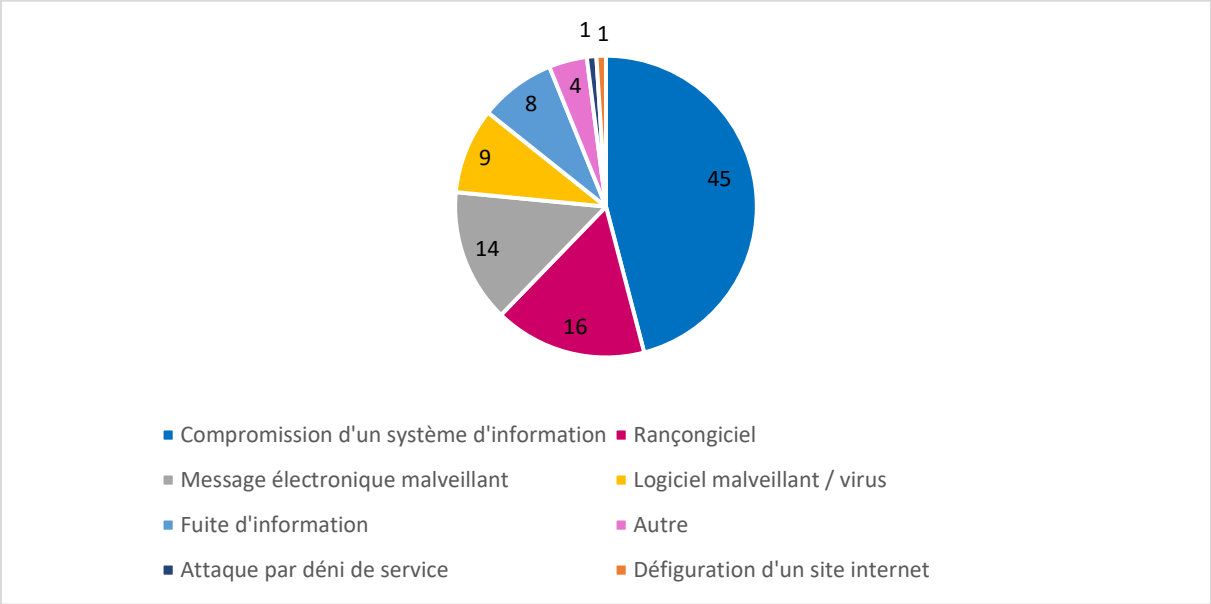



*Figure 18 - Origine des incidents pour lesquels un appui technique a été apporté par le CERT Santé*

## ●● Accompagnement global des structures de santé ●●

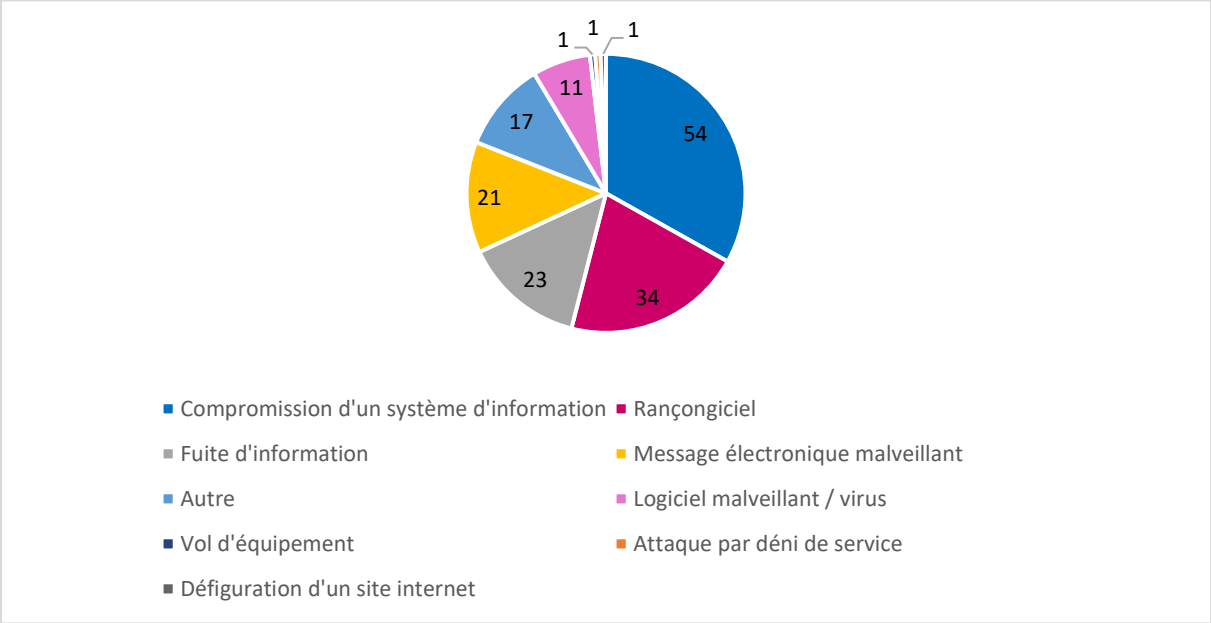



*Figure 19 - Origine des incidents pour lesquels des recommandations ont été émises par le CERT Santé*

Le nombre de déclarations d'incident pour lesquels une demande d'accompagnement est formulée a doublé par rapport à 2020. Elle concerne généralement une demande d'appui pour identifier l'origine d'une compromission avérée ou potentielle du SI et la validation des mesures

visant à endiguer la propagation de la menace et corriger les failles de sécurité. Ce sont les ES publics (65%) qui ont le plus sollicité le CERT Santé et en particulier les ES supports de GHT (29%).

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.

## Les signalements d'origine non malveillante

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

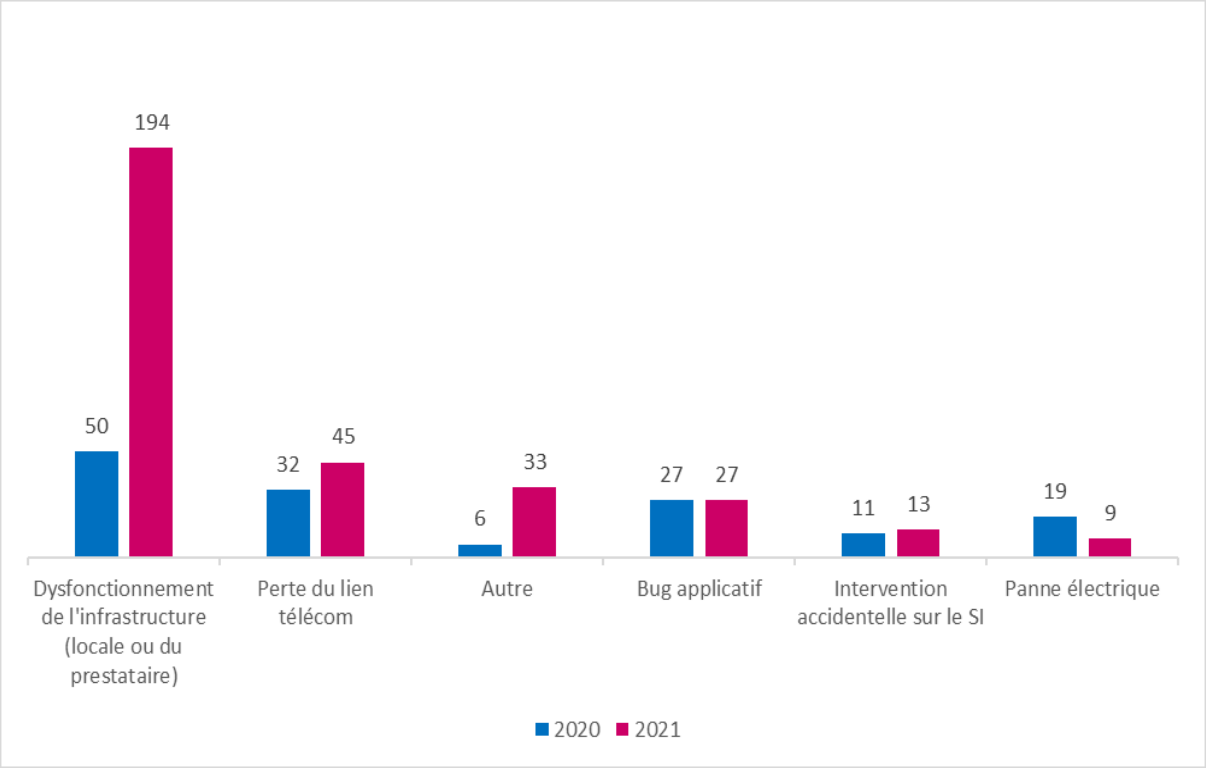



*Figure 20 - Origine non malveillante des incidents*

L'augmentation du nombre d'incidents ayant une origine non malveillante est principalement lié à des sinistres majeurs rencontrés par des hébergeurs ou prestataires de solutions métier en mode SaaS. Cela a provoqué des interruptions prolongées de service ou des applications hébergées. **La part d'origine non malveillante et lié à un dysfonctionnement de l'infrastructure est de 60%**.

La **perte du lien télécom** est la deuxième source d'incident d'origine non malveillante (14%). 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.

Le nombre de déclarations lié à un **bug applicatif** est stable. 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.

Dans la catégorie « Autre » on retrouve principalement des déclarations de failles de sécurité qui n'ont pas fait l'objet d'une exploitation par un acteur malveillant mais également des évènements informatiques à l'origine de comportements imprévus de systèmes mais qui se sont révélés être des « faux positifs » après une investigation du CERT Santé.

**48%** C'est la part d'incident d'origine non malveillante en 2021 des incidents, ce chiffre a augmenté de 8% par rapport à 2020.

## Evolution des incidents d'origine non malveillante

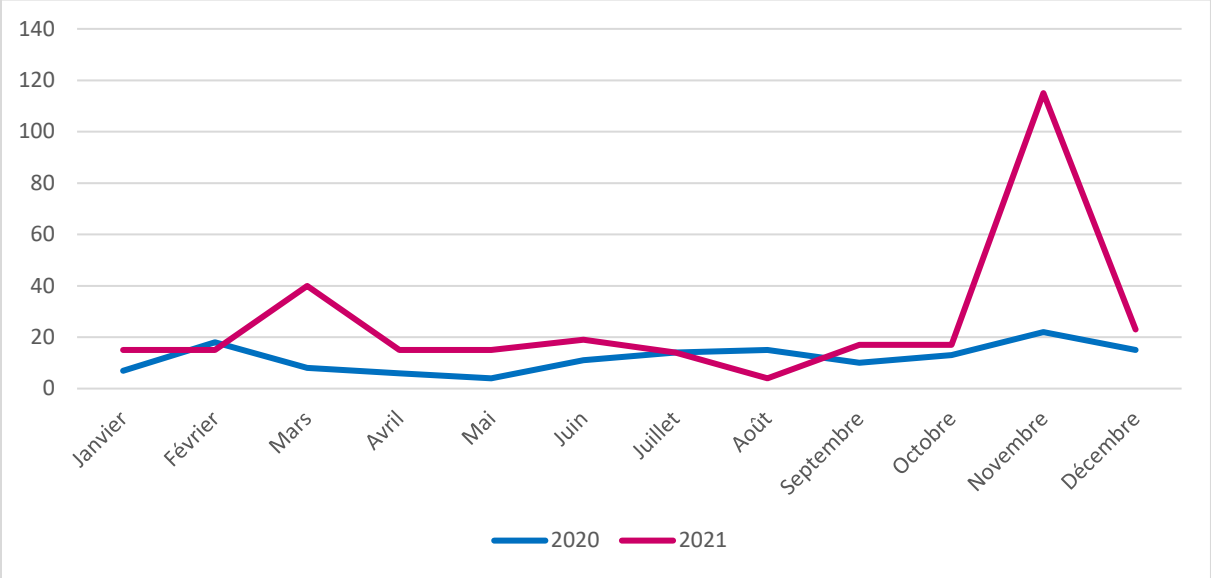



*Figure 21 - Evolution du nombre d'incidents dont l'origine est non malveillante*

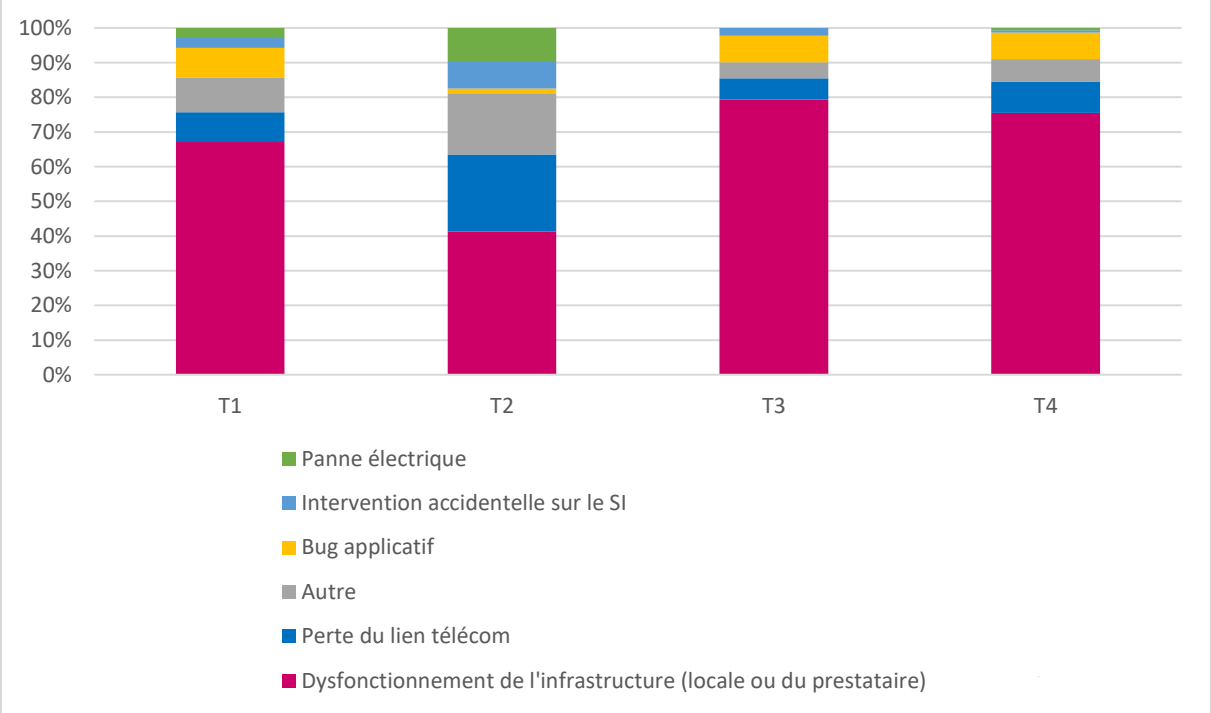



*Figure 22 - Origine non malveillante des incidents par trimestre*

## 4.3 Publication d'alertes sur le portail cyberveille-santé

En 2021, huit alertes ont été publiées sur le portail cyberveille-santé[5] concernant :

- Des campagnes d'attaques :
  - Campagne de phishing visant à diffuser les maliciels Trickbot ou Emotet, maliciels utilisés pour distribuer le rançongiciel Ryuk ;
  - Campagne de phishing visant à diffuser les maliciels Trickbot ou Dridex, maliciels utilisés pour distribuer des rançongiciels – cette campagne est toujours en cours et le CERT Santé partage des indicateurs de compromission sur la partie privée de son portail.

- Des vulnérabilités critiques :
  - Deux alertes concernant des vulnérabilités Microsoft Exchange dont l'exploitation permet à un attaquant de réaliser une exécution de code arbitraire à distance et de prendre le contrôle du serveur de messagerie pour l'une et d'obtenir des privilèges d'administration de domaines pour l'autre ;
  - Vulnérabilité dans le service de file d'attente d'impression Windows (Windows Print Spooler) dont l'exploitation permet à un attaquant local et non-authentifié d'obtenir les privilèges SYSTEM et d'exécuter du code arbitraire sur une machine vulnérable ;
  - Vulnérabilité dans l'hyperviseur VMware Center dont l'exploitation permet à un attaquant de réaliser une exécution de code arbitraire à distance ;
  - Vulnérabilité dans le composant MSHTML de Windows et moteur de rendu d'Internet Explorer dont l'exploitation permet à un attaquant de réaliser une exécution de code arbitraire à distance avec les niveaux de privilèges de l'utilisateur ;
  - Vulnérabilité log4j d'Apache permettant à un attaquant de réaliser une exécution de code arbitraire à distance à partir d'un serveur LDAP.

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

# 5 OBSERVATOIRE DES VULNERABILITES

## 5.1 Service national cyber-surveillance

Dans le cadre du plan de renforcement cyber du ministère, les audits de cyber-surveillance ont été prioritairement orientés vers les groupements hospitaliers de territoire (GHT).

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 ont accès aux résultats détaillés) ;


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[6] 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,

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

- la description de la vulnérabilité,
- la recommandation associée en vue de sa correction.

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[7]. Ces informations permettent d'encadrer les audits de cyber-surveillance lorsqu'ils sont réalisés par des prestataires à la demande des structures.

En 2021, 91 audits ont été réalisés, soit près du double de 2020 (44) : cinquante GHT dont 2 GHT des DOM avec certains ES qui ont été audités unitairement (51 audits), 10 CH dans les DOM-COM (hors GHT), dix-huit établissements des secteurs privés et médico-social, deux GRADeS, un ordre de professionnels de santé.

## 5.2 Service de veille proactive

Le CERT Santé a renforcé son activité de veille proactive au regard du nombre important de vulnérabilités critiques qui ont fait l'objet d'une publication en 2021. Ainsi afin de prévenir la compromission potentielle de SI au travers de l'exploitation de ces vulnérabilités, le CERT a alerté plus d'un millier de structures. Ces alertes ont principalement concerné la messagerie Exchange et les VPN Fortinet et SonicWall.

Cette activité d'alerte est réalisée en étroite coopération avec le CERT-FR. Ainsi le CERT Santé a relayé une soixantaine d'alertes concernant des compromissions potentielles de SI identifiées par l'ANSSI

Vous trouverez ci-dessous un rappel des principales activités de surveillance du CERT 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).

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

## 5.3 Constat et recommandations

Les structures qui ont été auditées 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 auditées 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 OWASP[8]) : 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)

[8] 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.

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 conditions 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 conditions de sécurité ainsi que la possibilité de réaliser des audits.

# 6 GLOSSAIRE

| | |
|---|---|
| **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.<br>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.<br>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 ministérielle 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

## 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
La transformation commence ici