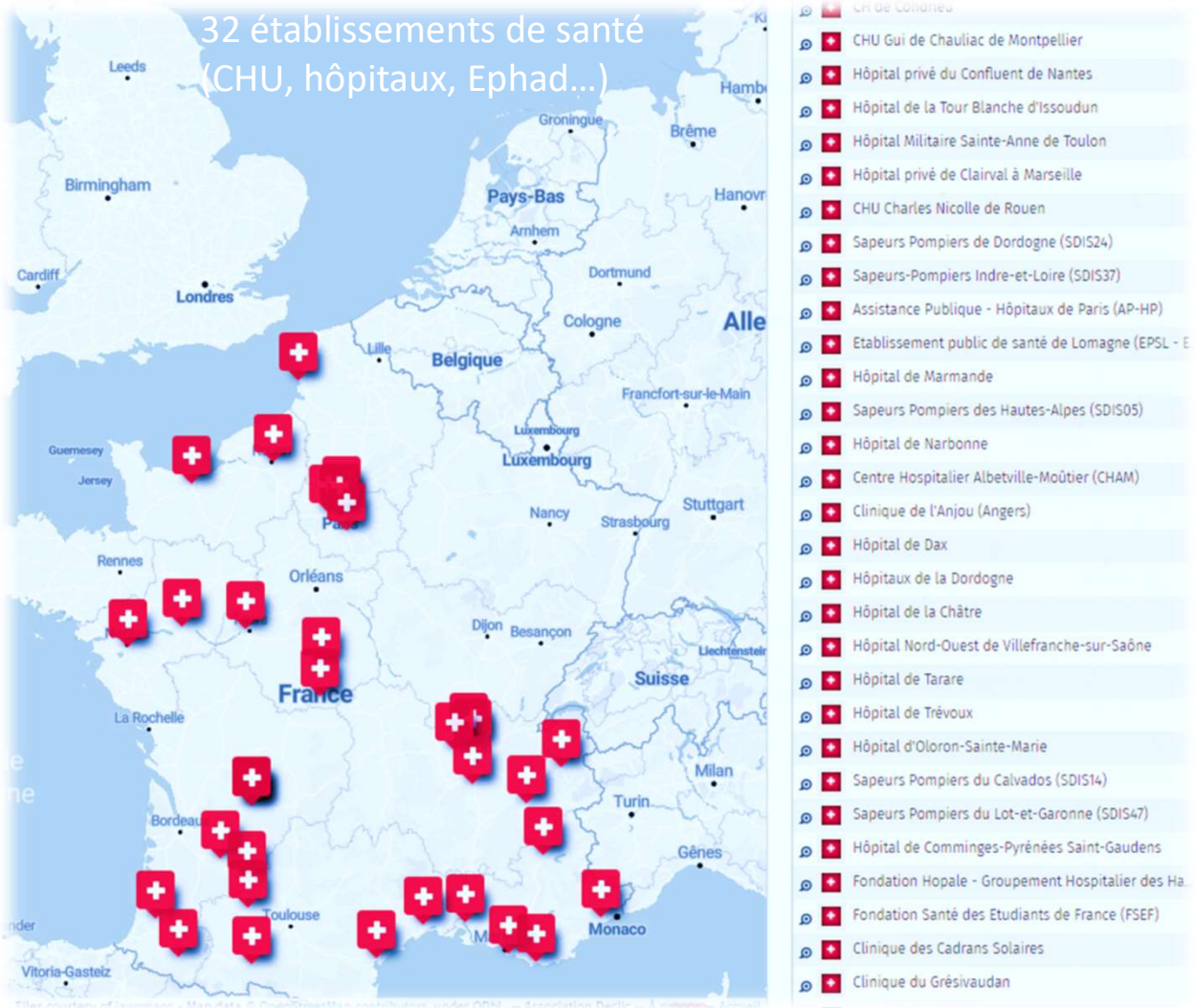
Source : LeMagIT

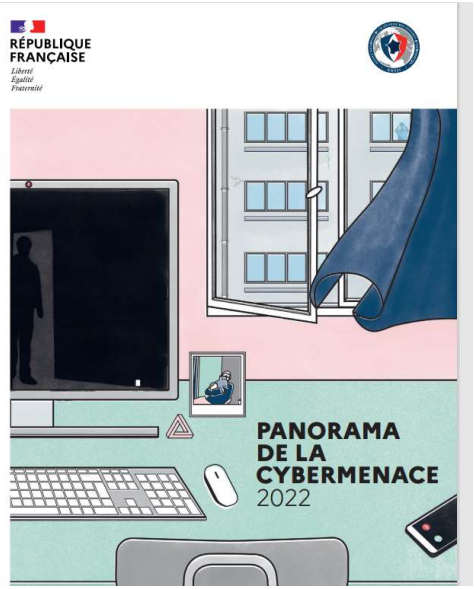
Convention de Genève Article 18 ***: Les hôpitaux*** *civils organisés pour donner des soins aux blessés, aux malades, aux infirmes et aux femmes en couches* ***ne pourront****, en aucune circonstance,* ***être l'objet d'attaques****…*

Les établissements de santé particulièrement visés ?



Carte des attaques touchants les organismes de santé en France depuis quatre ans

(*source* Declic - Réseau d'échange d'informations entre structures (asso-declic.fr))



Panorama de la cybermenace 2022 – CERT-FR (ssi.gouv.fr)

Les établissements de santé particulièrement visés ?

- Comme en 2021, les principales victimes françaises d'attaques par rançongiciels observées par l'ANSSI en 2022 demeurent les TPE, PME, et ETI, suivies des collectivités territoriales et **des établissements publics de santé en troisième position.**

- Le nombre d'attaques par rançongiciel est en baisse sur l'année 2022, mais leurs **conséquences demeurent très importantes** dans le **secteur critique de la santé**. Outre les conséquences financières, ce type d'évènement peut également avoir **un impact sur le suivi des patients et la confidentialité de leurs données de santé.**

Les contacts en cas d'alerte :

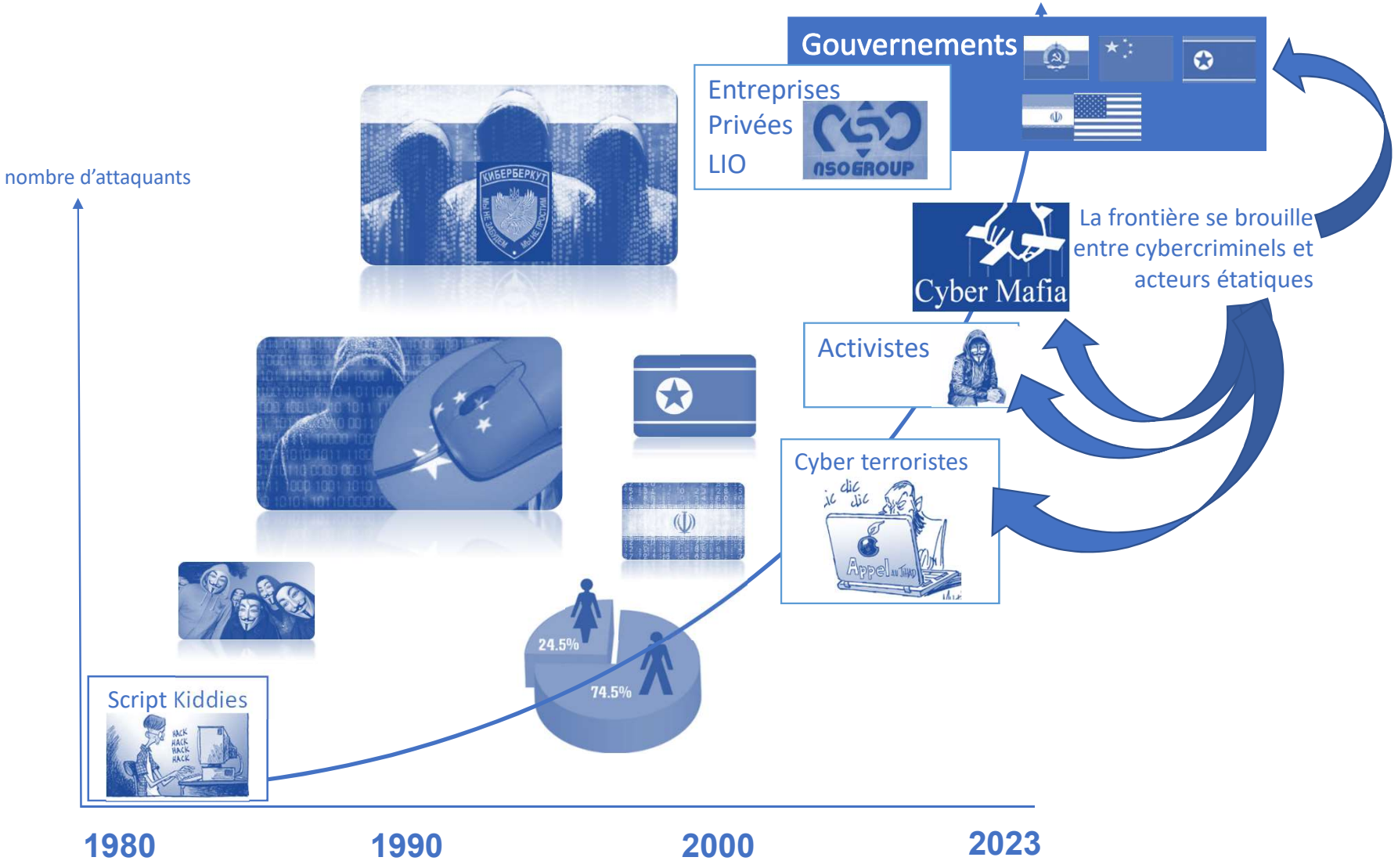
-> www.cyberveille-sante.gouv.fr
cyberveille@esante.gouv.fr

-> ssi.gouv.fr
cert-fr@ssi.gouv.fr

Quels sont les impacts d'une attaque cyber dans un établissement de santé ?

- Un fonctionnement en mode dégradé (3 mois pour restaurer 95% du SI et un an pour retourner à une situation nominale),
- Une perte de confiance du public,
- Une tension supplémentaire sur le personnel médical,
- Une demande de rançon 300 000 € à 3 000 000 €,
- Risque d'attaques par déni de service distribué (DDoS),
- Des données médicales revendues qui démultiplient les risques de vol d'identité,
- Un coût de gestion de la crise et de remédiation important,
- Le risque de provoquer des incidents et des erreurs impactant la santé des patients.

Evolution des profils attaquants



Des cybercriminels éthiques ?...

KILLNET *hacktivistes pro-russes*

Ciblent en DDOS des hôpitaux au Royaume-Uni, en Allemagne, en Pologne, en Scandinavie et aux États-Unis. (environ 50…) :

« Nous sommes de simples citoyens russes défendant leur pays»

Selon le groupe **BlackCat** : *« nous n'attaquons pas les institutions médicales de l'État, les ambulances, les hôpitaux. Cette règle ne s'applique pas aux sociétés pharmaceutiques, aux cliniques privées. »*

L'argument ? *« On ne tue pas les patients on vole seulement leurs données médicales »*…et s'attaquer au secteur privé permet d'être payé…En France les hôpitaux ont ordre de ne pas accepter la rançon.

Un décès lié à une attaque au ransomware sur un hôpital

La patiente, simplement identifiée comme une femme ayant besoin de soins médicaux urgents, est décédée après avoir été réorientée vers un hôpital de la ville de Wuppertal, à plus de 30 km de sa destination initiale, l'hôpital universitaire de Düsseldorf.

En 2020 l'attaque d'un centre hospitalier était une « erreur » aujourd'hui » c'est un scénario récurent.

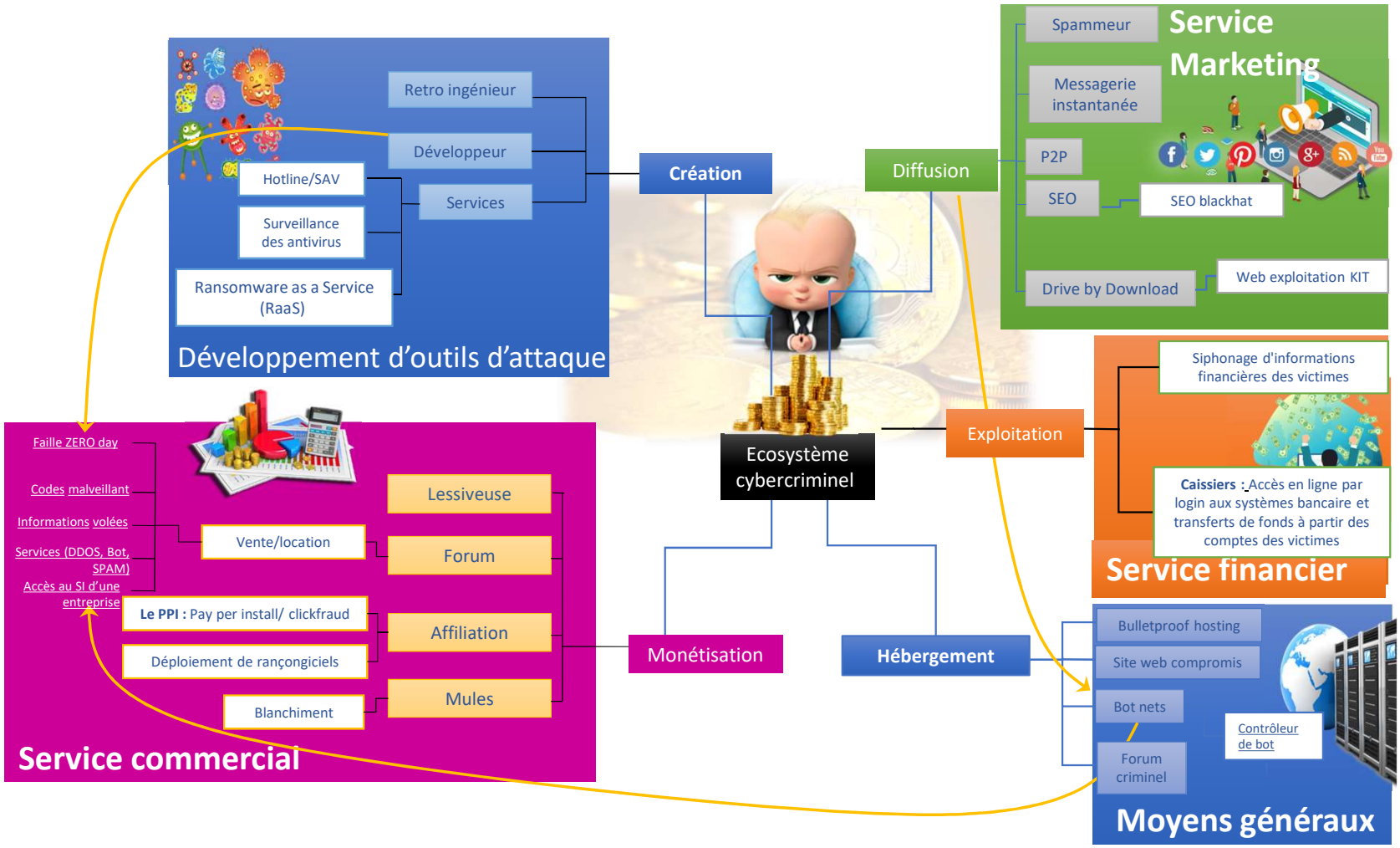
Qu'est-ce qui a changé?

Le 31 décembre 2022, LockBit, un groupe cybercriminel qui diffuse un rançongiciel à ses affiliés, a publiquement présenté des excuses pour la cyberattaque dont a été victime l'hôpital pour enfants malades de Toronto.

« Le partenaire qui a attaqué cet établissement a enfreint nos règles, est bloqué et ne fait plus partie de notre programme d'affiliation ».

Le groupe a fourni une clé de déchiffrement pour récupérer les données bloquées par le rançongiciel.

Le cybercrime …une industrie fleurissante



Le 31 janvier 2023: *les* équipes de sécurité de Microsoft suivent plus de 100 groupes criminels déployant des rançongiciels et surveille plus de 50 familles de rançongiciels *Lockbit Black*, *BlackCat* (alias *ALPHV*), *Play*, *Vice Society*, *Black Basta* et *Royal*

Le cybercrime …une industrie florissante

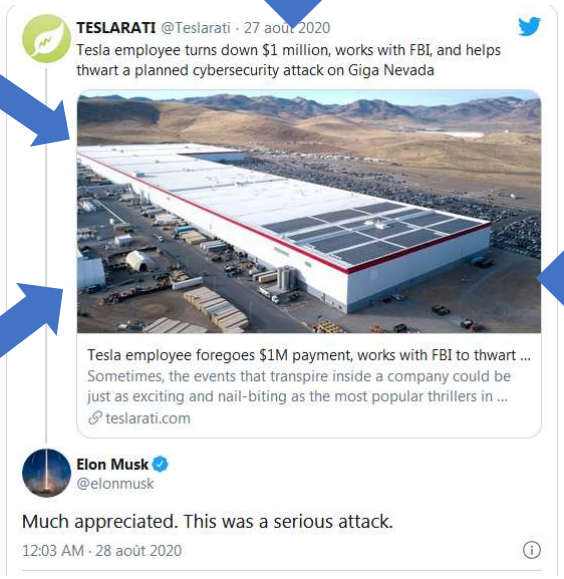
La taupe

1 000 000 $

Le BOSS

2 000 000 $

Helpdesk- SAV



750 000 $

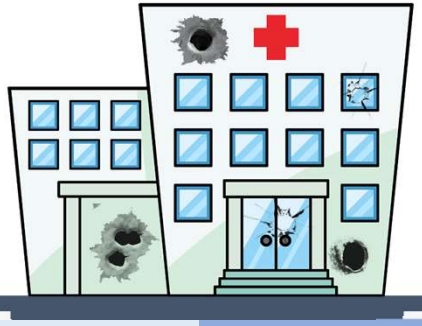
Hébergement admin forum

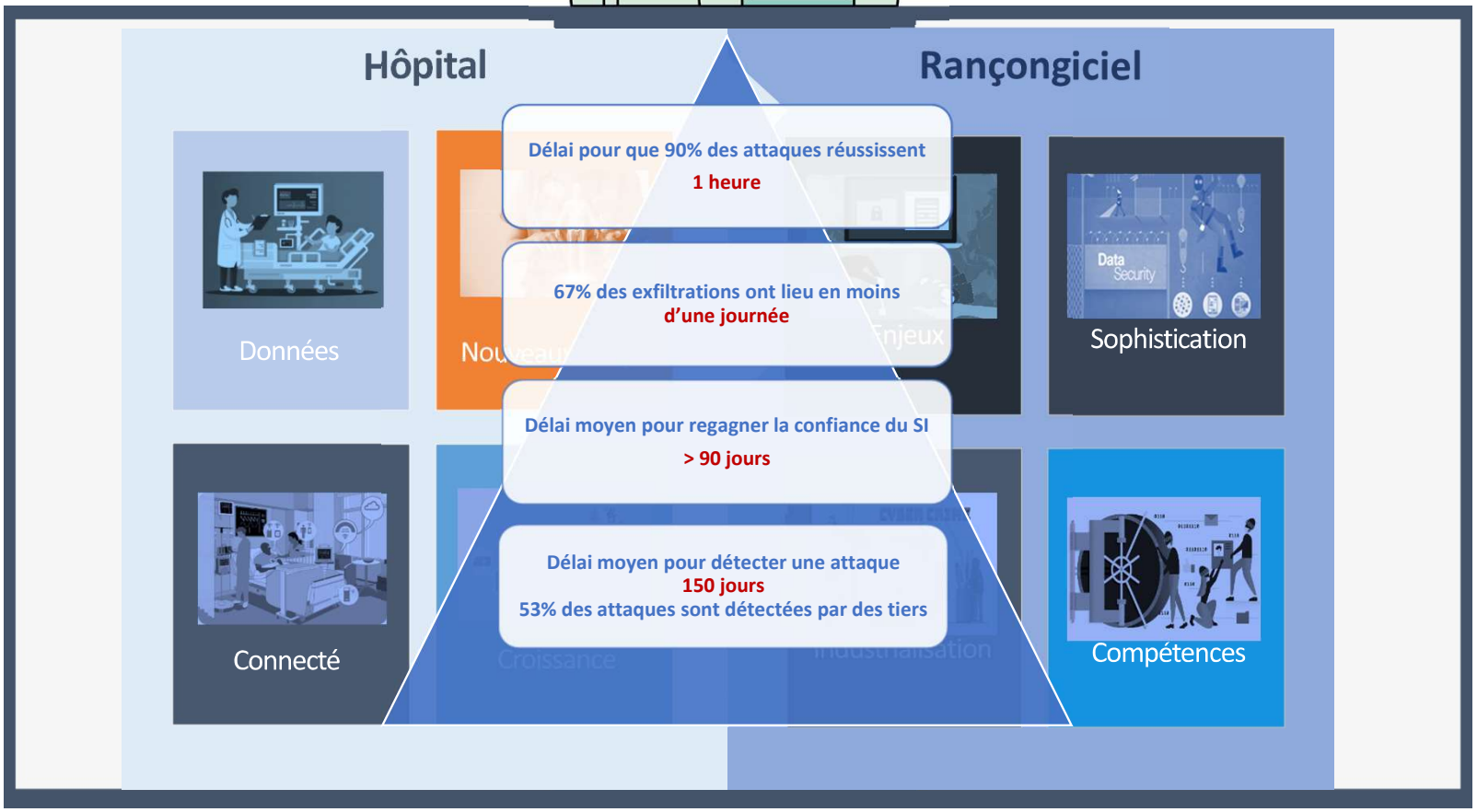
250 000 $

Développeur

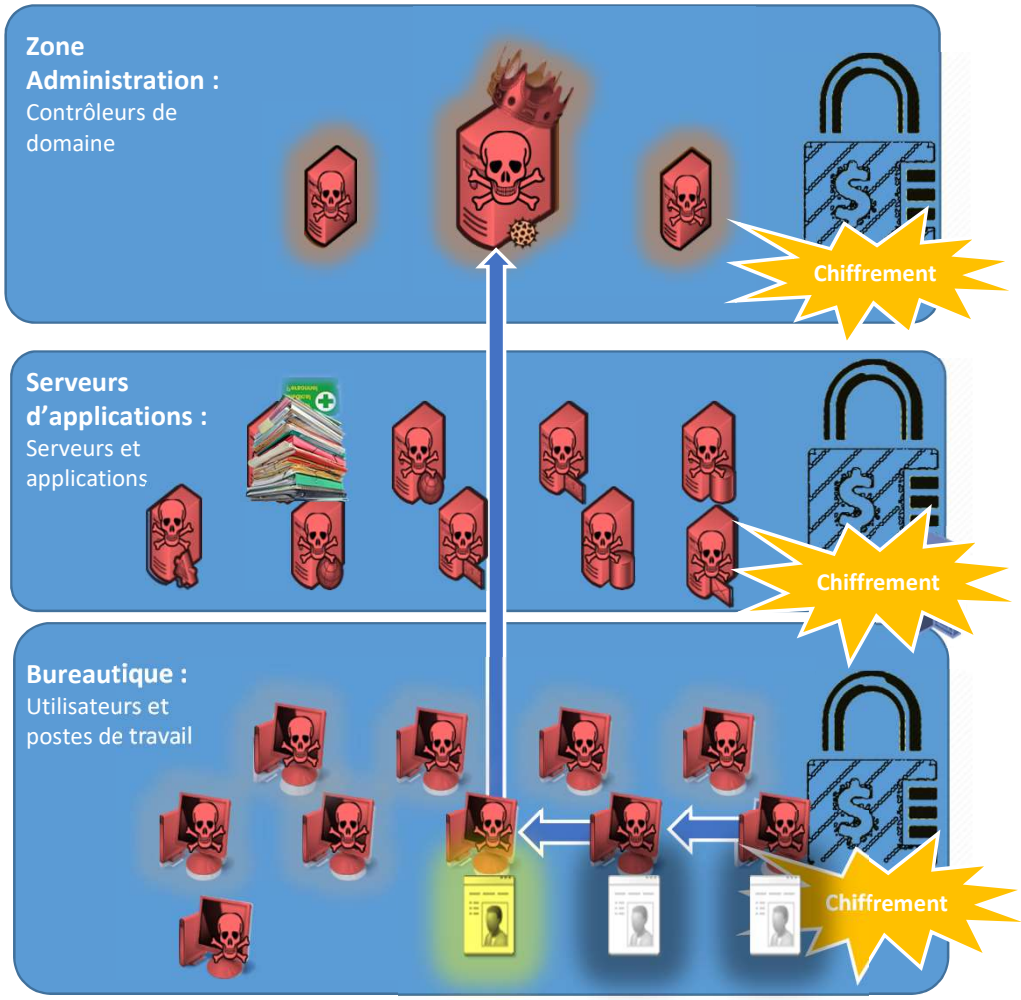
Lessiveuse

Compromission: découverte tardive de la scène de crime !





Etapes d'une attaque par rançongiciel



1. Emails piégés et ciblés ou vulnérabilité logicielle

2. Un utilisateur administrateur de sa machine est compromis. Vol des identifiants et installation de porte dérobée

3. L'attaquant utilise ces identifiants pour se déplacer latéralement ou élever ses privilèges

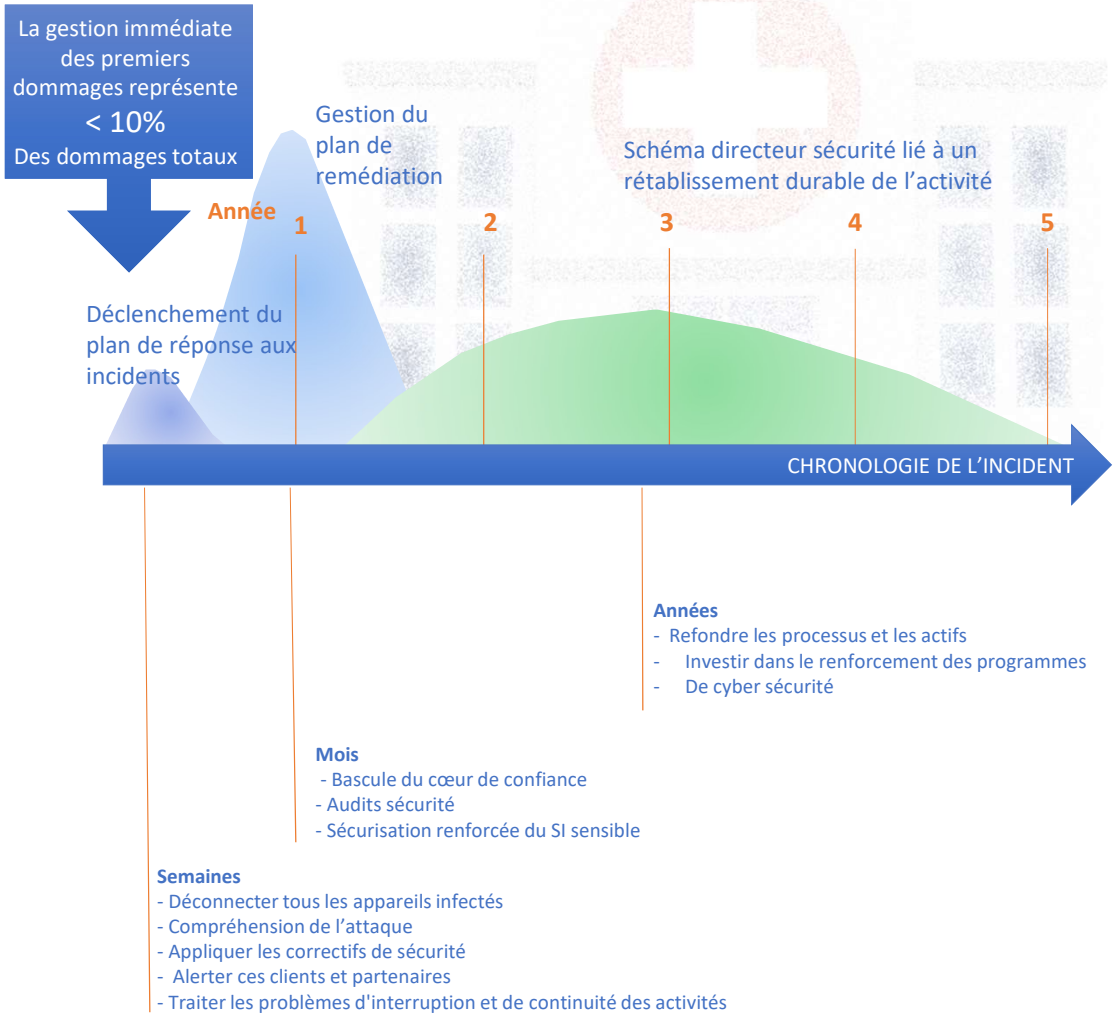
4. L'attaquant récupère un compte administrateur du domaine

5. L'attaquant accède à tous les systèmes et exfiltre des dossiers des patients et les données de l'organisation

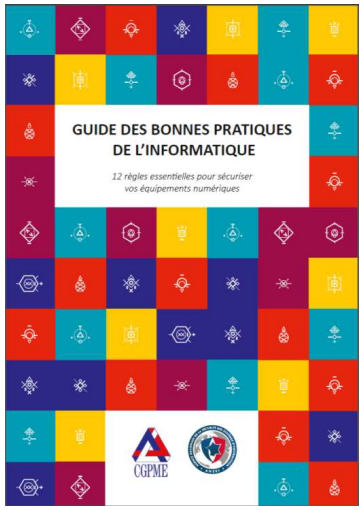
6. L'attaquant chiffre les espaces de stockage et les sauvegardes du SI

Compromission et latéralisation par des attaquants

Réagir à une cyberattaque : les décideurs sous estiment souvent le coût de l'incident



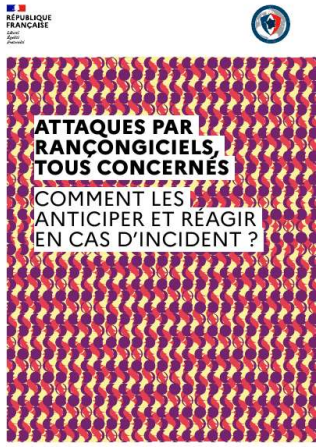
Les conséquences d'une attaque peuvent se répercuter sur des années sous la forme de coûts *cachés*, dont la plupart sont beaucoup moins facilement mesurables : atteinte portée à l'image de l'organisation, perte d'informations confidentielles, entre autres.



La sécurité n'est pas un coût mais un investissement…

www.ssi.gouv.fr/administration/bonnes-pratiques
www.ssi.gouv.fr/administration/guide/guide-d'hygiene-informatique

Pourquoi ces attaques fonctionnent ?



Un rapport établi en 2021 par l'ANSSI considérait que le risque sécurité était élevé

- Les équipes informatiques sont souvent :
  - trop restreintes,
  - pas préparées à gérer ce type de crise,
  - Pas assez formées aux systèmes qu'elles gèrent,
  - Pas suffisamment formées au pilotage de projets de reconstruction d'un SI compromis,
- La gestion, au quotidien, de nombreuses situations critiques par le personnel ne facilite pas les efforts de sensibilisation,
- Le niveau de sécurité des logiciels est volontairement diminué à l'installation pour en faciliter l'accès par le personnel soignant, ou pour en permettre la connexion à des SI ne disposant pas de fonctionnalités de cybersécurité compatibles,
- L'intégration de SI communs entre plusieurs sites peut encore compliquer la maîtrise de ces parcs informatiques,
- L'accès par le prestataire aux données médicales n'est pas systématiquement soumis à un contrôle d'accès,
- la connexion à internet des dispositifs médicaux (DM) "participe à la vulnérabilité globale,
- Les sauvegardes sont souvent incomplètes ou parfois non fonctionnelles.

https://www.ticsante.com/story?ID=5589

Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ? | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)