RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

CERT-FR

23 ANS D'HISTOIRE
15 ANS D'OPÉRATIONS

MATHIEU FEUILLET
ANSSI

Au programme

1. Du CERT-A au CERT-FR

2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Au programme

1. Du CERT-A au CERT-FR
2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

Du CERT-A au CERT-FR : 23 ans d'histoire

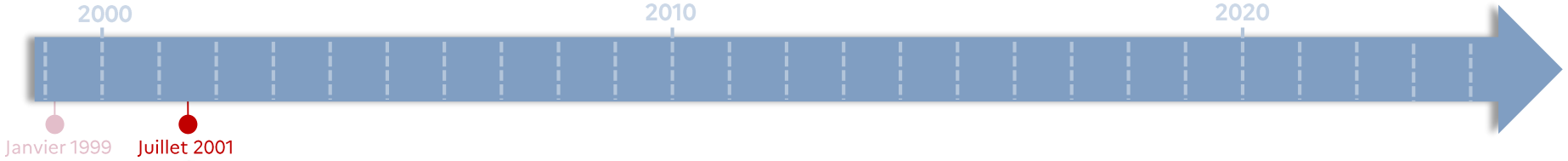
2000 2010 2020

Janvier 1999

Création d'un **CERT** dédié aux « ***systèmes informatiques*** » des **administrations de l'Etat**

- Anticipation d'actions malveillantes opportunistes en marge du « ***bug de l'an 2000*** »
- **Missions toujours d'actualité**

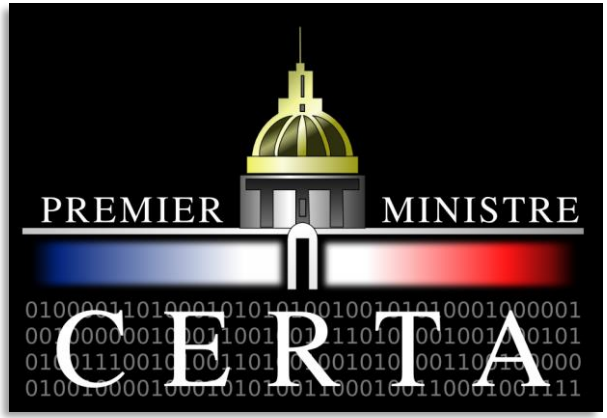
Du CERT-A au CERT-FR : 23 ans d'histoire



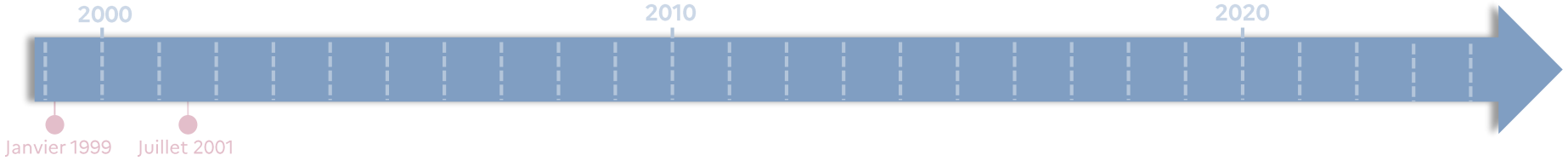
Création de la **DCSSI**

- Stratégie de protection des **infrastructures vitales**

Le CERTA passe de **2 personnes en 1999** à **14 en 2001**



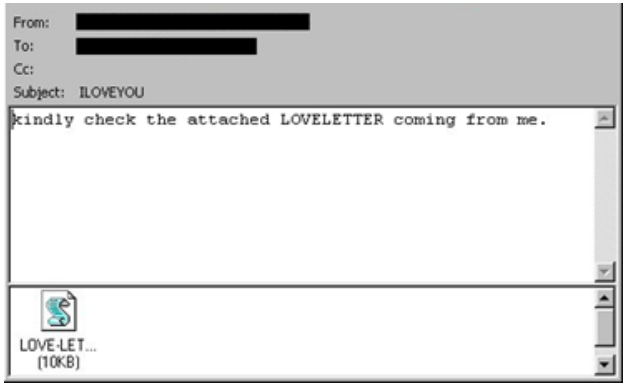
Le CERT-A en l'an 2000 ?



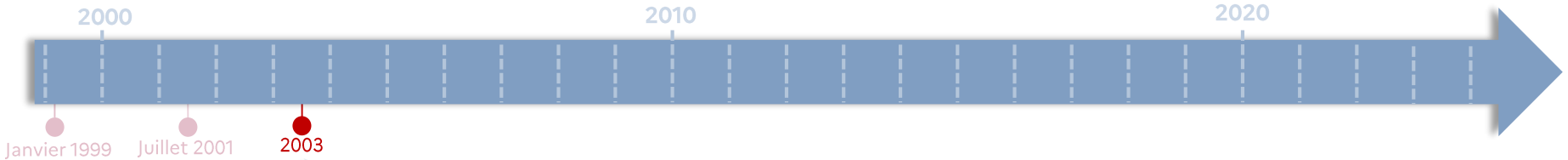
Faibles impacts des incidents traités

Attaquants motivés par le **défi**, **l'atteinte à l'image** des instituions

Alertes, avis sur les vulnérabilités, information sur les menaces



Naissance du COSSI



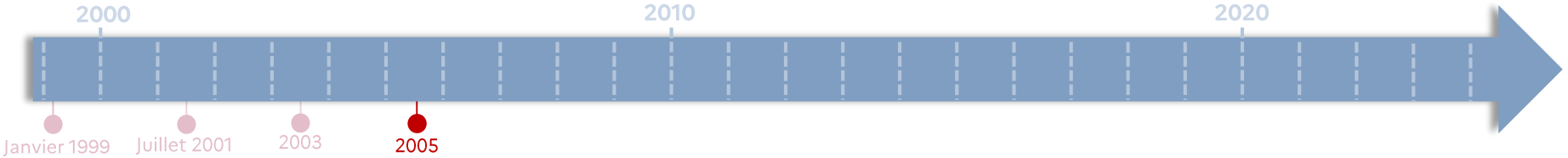
Création du COSSI dans le cadre du **plan VIGIPIRATE**

- **Veille**
- Expertise en **réponse à incidents**
- Conduite de **crise**

<10 personnes à la création

Naissance du COSSI

Quels incidents en 2005 ?

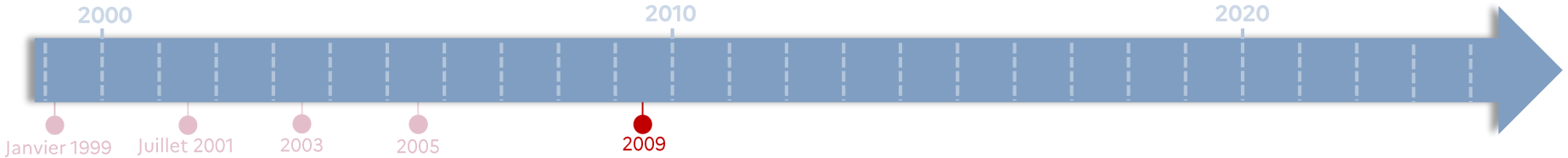


Traitement d'incidents liés à des **attaques non ciblées** ou de **fraude**

Augmentation du nombre d'attaques traitées sur le périmètre gouvernemental

2006 : premières attaques majeures **ciblant** des systèmes gouvernementaux français

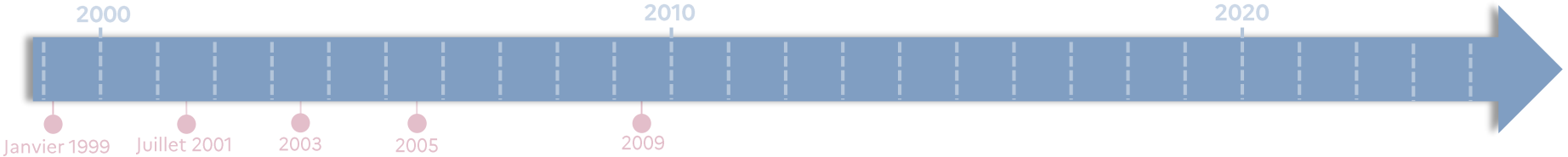
Évolution du COSSI



Création du **service de détection** au bénéfice d'administrations centrales

La DCSSI devient … l'ANSSI !

Quelle menace à la création de l'ANSSI

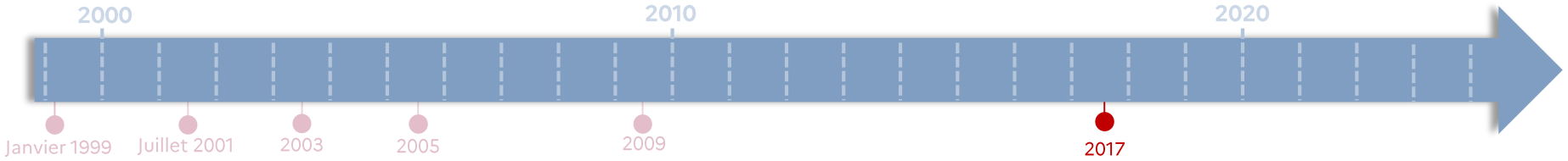


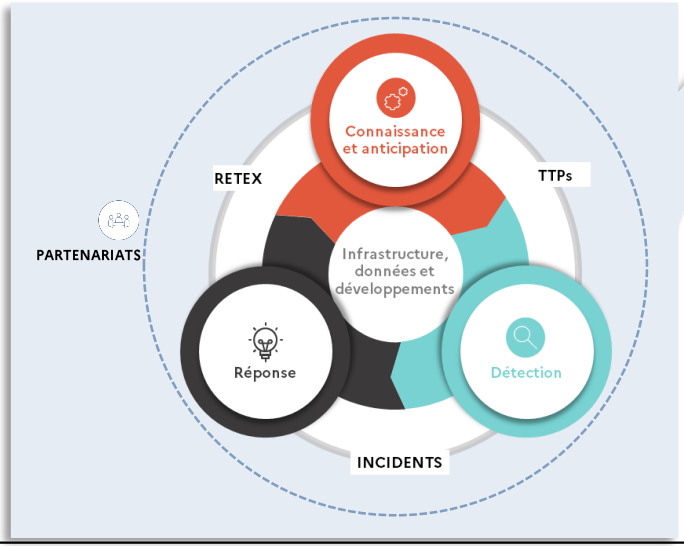
Développement de la **cybercriminalité** et **hacktivisme**

Administrations et organisations bénéficiaires touchées par des **vers** (CONFICKER)

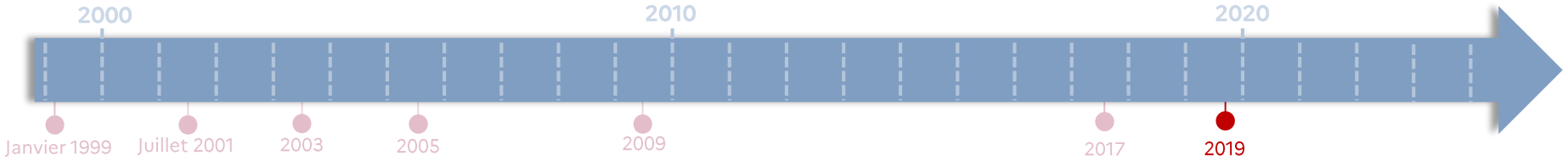
2007-2008 : Premières opérations touchant à de l'espionnage stratégique

Du COSSI à la SDO – CERT-FR



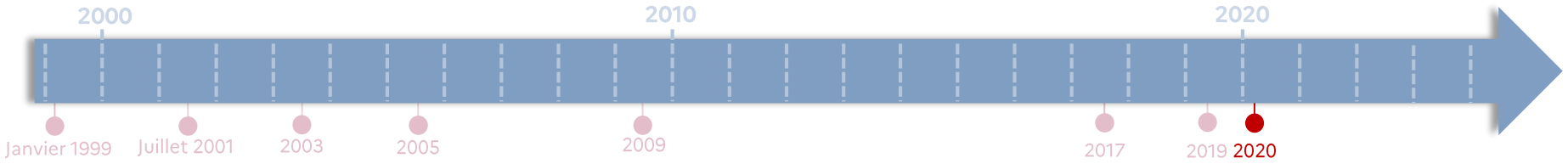


Un écosystème qui se structure



Première intervention conjointe sur un incident avec un **PRIS**

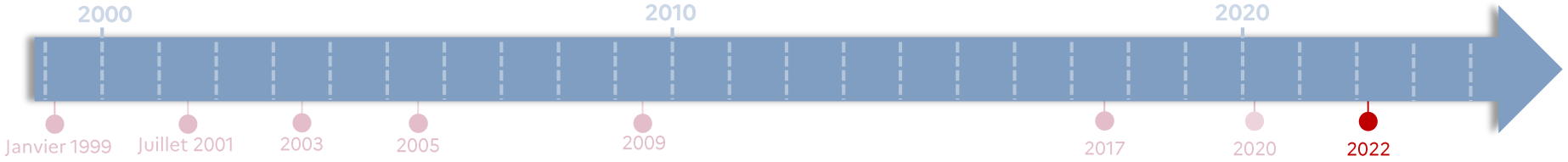
2020 : le chaos… comme pour tout le monde



Crise sanitaire

➢ Développement du **télétravail** (des équipes et des bénéficiaires)

Les nouveaux enjeux du CERT-FR



Paris

CAMPUS CYBER

Rennes

Travail **multi-sites**
- Paris
- Rennes
- Campus Cyber

Densification de l'**écosystème de CSIRTs** (ministériels, sectoriels, régionaux …)

Au programme

1. Du CERT-A au CERT-FR
2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

Au programme

1. Du CERT-A au CERT-FR
2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

Compromission de Bercy en 2011 : la mère des batailles

Une première opération d'ampleur, structurante pour le COSSI

Exfiltrations d'informations **sensibles** sur **plusieurs années**

Ciblage des informations relatives au **G20**

Campagnes similaires attribuées à la **Chine**

Attaquants **professionnels**, mais **peu discrets**

Attaquants actifs au moment de l'intervention de l'ANSSI

Compromission de Bercy en 2011 : la mère des batailles

Une première opération d'ampleur, structurante pour le COSSI

Investigations sur un **périmètre large**

Bascule de l'**Active Directory**

Opération **structurante**

Traitement en **crise**

Ciblage structurel d'entités stratégiques

Et ça continue, encore et encore…

Ciblage constant des intérêts politiques, diplomatiques, économiques et industriels français.

Réponse à des **intérêts stratégiques d'Etats**, parfois non identifiés.

Sophistication constante des attaques

Adaptation à la défense des bénéficiaires

Polycompromissions fréquentes

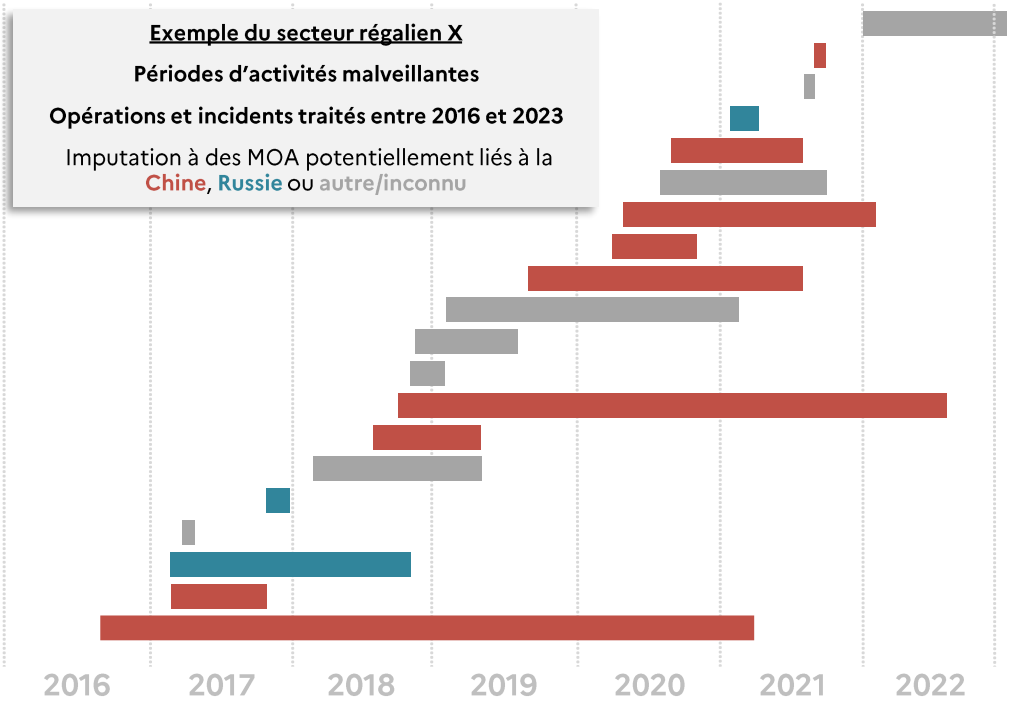
Ciblage structurel d'entités stratégiques

Et ça continue, encore et encore…

Espionnage de long terme

Fort investissement de l'ANSSI et des victimes

Nécessité de **discrétion**



Ciblage constant des secteurs industriels stratégiques 1/3

2011-2014 : les attaques frontales

Ciblage visant un **secteur industriel** entier

Tentatives de **prise de contrôle total** des réseaux ciblés

Recherche et exfiltration de **données stratégiques**

Groupes d'attaquants liés (en sources ouvertes) à la **Chine**

Ciblage constant des secteurs industriels stratégiques 1/3

2011-2014 : les attaques frontales

Série d'opérations de cyberdéfense de **grande ampleur**

Multiples opérations de **bascule**

Enjeux **d'outillage** et de **gestion de collectes massives**

Enjeux de **périmètre d'intervention** : de l'administration aux OIV

Ciblage constant des secteurs industriels stratégiques 2/3

2017-2020 : ciblage des ESN et chaînes d'approvisionnement

Série d'attaques visant **l'écosystème** des cibles finales

Rebond vers les machines des cibles finales *via* les interconnexions

Exfiltration de données industrielles

Retour en force des **MOA liés à la Chine**

Attaquants **discrets, efficaces et préparés**

Nouvelle typologie de **bénéficiaires**

Possibilité de **remédiation complète ?**

Ciblage constant des secteurs industriels stratégiques 3/3

2021- présent : intervention auprès de prestataires de plus en plus petits

Cibles (sous-traitants et prestataires) de **plus petite taille**

Compromissions larges et de longue durée

Bénéficiaires souvent très **mal sécurisés**, très **peu conscients de la menace**

MOA **non observés jusqu'ici** et liés en sources ouvertes à la **Chine**

Recherche d'**informations industrielles stratégiques**

Secteur **structurellement ciblé** : déplacement des attaquants vers le **maillon le plus faible** ?

Ciblage d'équipements embarqués

2011-… : ça va couper !

Ciblage d'**équipements « non-conventionnels »**

Ciblage du **secteur des télécommunications** au sens large

Intérêt constant pour les groupes d'attaquants aux **intérêts stratégiques**

Surface d'attaque large

Expérience de l'ANSSI sur l'investigations numérique sur ce type d'équipements

Création de **relations** avec les opérateurs de télécommunications

Campagnes de compromission à large échelle

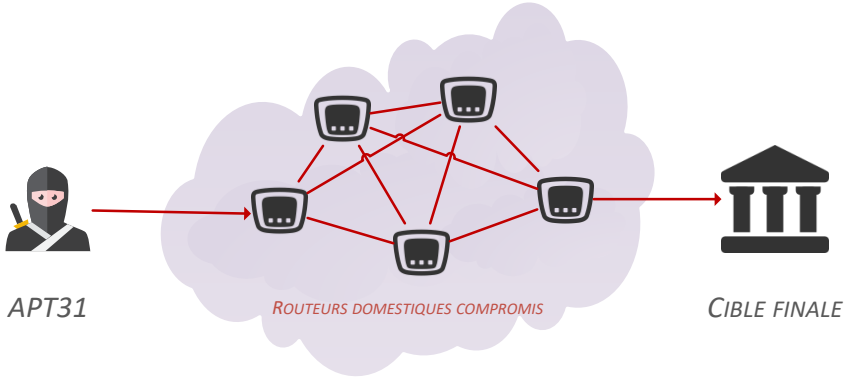
2021 : *annus horribilis*

Espionnage de **nombreuses entités stratégiques**

- Au moins **100 cibles** françaises identifiées
- **20 compromissions** avérées

MOA APT31 réputé lié aux intérêts stratégiques chinois

Espionnage d'entités publiques et privées d'intérêt



Campagnes de compromission à large échelle

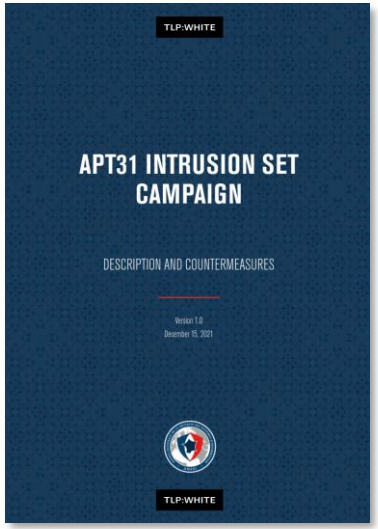
2021 : *annus horribilis*

Forte implication des équipes du CERT-FR

- **8** opérations/incidents majeurs

Stratégie d'entrave **:**

- **Campagnes de partage de marqueurs de compromission** auprès des administrations, OIV, OSE
- **Publication** sur le site du CERT-FR de mémos détaillants les codes et TTPs du MOA APT31



Nouvelles formes d'espionnage

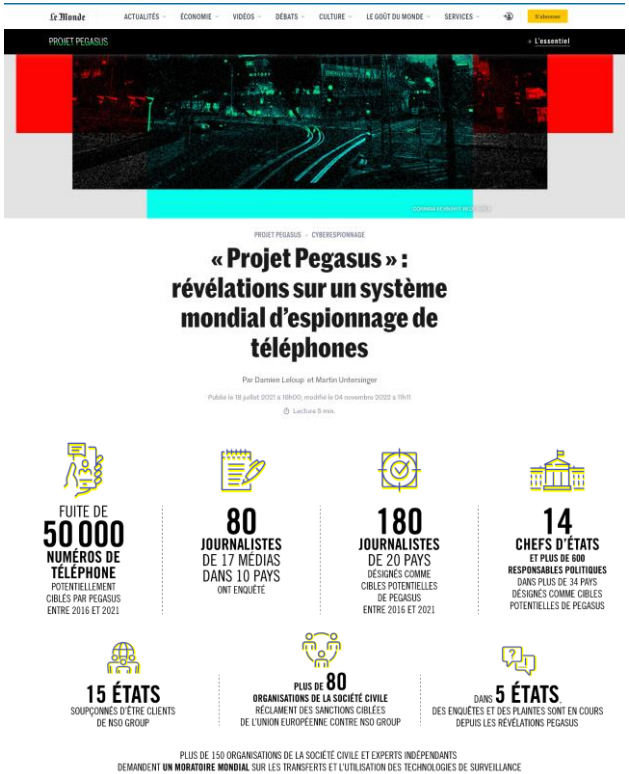
Un bourriquot ailé dans ton téléphone !

Compromission de **téléphones individuels** de **personnalités publiques**

Mise en œuvre rapide de capacités de dépistage et investigations

LIO privée : ajout d'un **intermédiaire** entre le commanditaire de l'attaque et la cible, **complique l'imputation d'une compromission**

Code malveillant très sophistiqué : Pegasus



Sources : Le Monde, Amnesty International France

Opérations d'anticipation : Solarwinds, Log4j et autres

Agir avant la compromission (si on peut)

Campagnes de recherches de marqueurs

Injonctions aux entités du périmètre ANSSI

Compromission d'un **acteur de la *supply chain* logicielle** (Solarwinds) ou **vulnérabilité exploitée** (Log4j)

MOA susceptibles d'agir **au profit d'acteurs stratégiques**

Diminuer le retard ou prendre de **l'avance** sur les attaquants

Estimer mieux l'impact d'une exploitation de vulnérabilité

Sensibiliser les bénéficiaires de l'ANSSI à la menace

Au programme

1. Du CERT-A au CERT-FR
2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

Hacktivisme : de l'État islamique aux pro-russes

Toujours en toile de fond : de 2015 à 2023

2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023

Vagues de **défigurations** et **DDoS de sites internet**

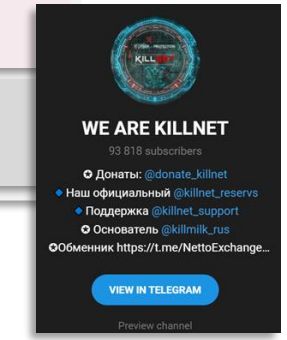
Acteurs hacktivistes **pro-EI**

Inquiétude et **pression politique**
Traitement en **mode crise** au COSSI

Vagues de **DDoS** et quelques **défigurations**

Acteurs hacktivistes **pro-russes**

Forte **attention médiatique**
Gestion **plus maîtrisée**



Sabotage : de TV5 Monde à Ka-Sat

2015 : TV5Monde, Je suIS IS

Sabotage du **système de diffusion**, de la **messagerie interne**

Détournement des comptes de réseaux sociaux pour diffuser de la propagande pro-EI

Attaquants agissant sous **faux-drapeau**

Indicateurs techniques liant le MOA à **APT28**

Sabotage : de TV5 Monde à Ka-Sat

2015 : TV5Monde, Je suIS IS

Intervention en **contexte de crise, pression importante, médiatisation**

Impact majeur sur l'organisation victime

Illustration de la **sensibilité / difficulté d'une attribution**

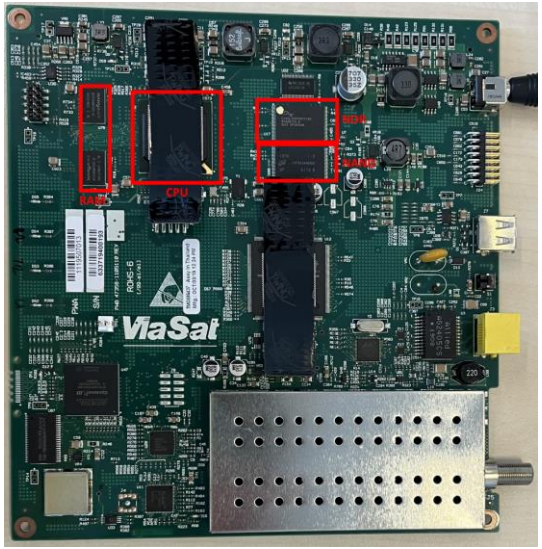
Sabotage : Ka-Sat / Viasat

Février 2022 : l'ANSSI dans l'espace

Ciblage l'infrastructure de Ka-Sat (Viasat) opérant les communications militaires ukrainiennes

Opération de **sabotage** menée la **nuit de l'invasion de l'Ukraine** (23-24 février 2022)

Attribution au **gouvernement russe** par les **Etats membres de l'UE** en mai 2022

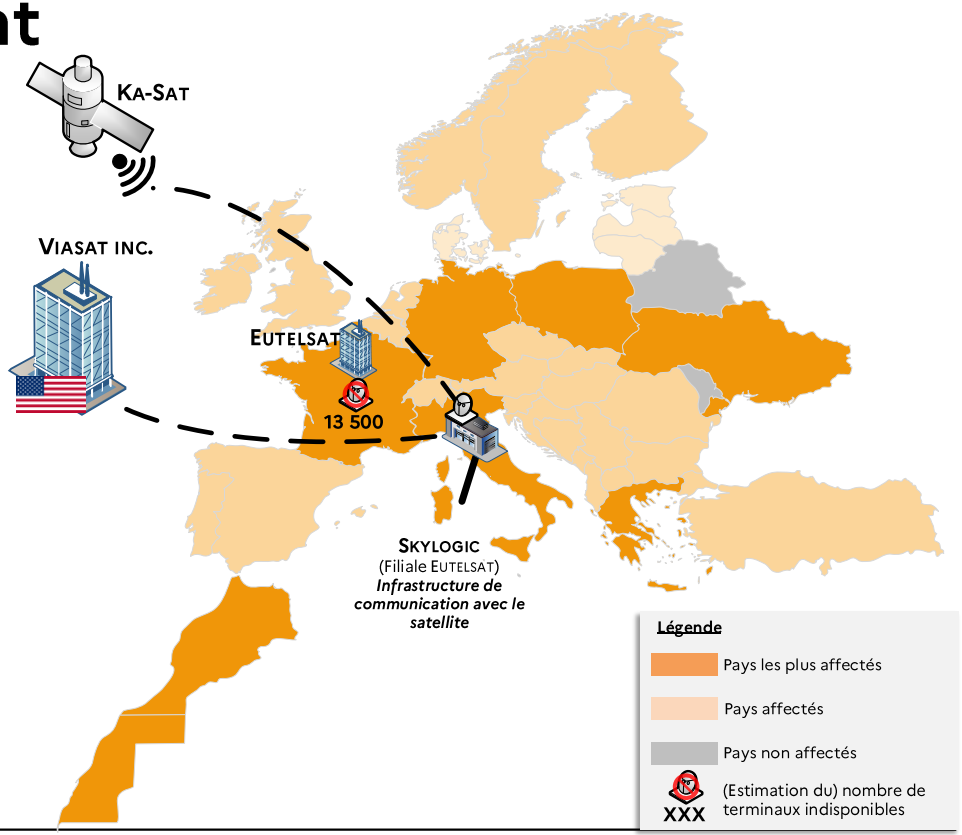


Sabotage : Ka-Sat / Viasat

Février 2022 : l'ANSSI dans l'espace

Impact cyber d'un conflit terrestre

Illustration du « **débordement** » d'une attaque par sabotage



Opérations de Hack & Leak

2017 : impact sur la vie démocratique française

Divulgation de milliers de courriels et documents internes du mouvement En Marche!

Veille du 2e tour des élections présidentielles de 2017

Diffusion *via* des avatars sur des **forums de discussion, Twitter** puis **Wikileaks**

Attaque attribuée par les États-Unis à APT28

Tentative de déstabilisation des institutions et de la vie démocratique

Importance de la **sensibilisation des organes politiques et citoyens**


Libération «MacronLeaks» : tentative de déstabilisation à la dernière minu...

élections 2017

BOULE PUANTE

«MacronLeaks» : tentative de déstabilisation à la dernière minute

Par Aurélie Delmas — 6 mai 2017 à 08:11

Prépositionnement

2017 – 2023 : ils sont là, mais pourquoi ?

Ciblage d'entités **sensibles ou intermédiaires** (rebond)

Sensibilité particulière de certains secteurs, comme l'**énergie**

Activités de **reconnaissance**

Intentions des attaquants **peu claires** : espionnage, sabotage ?

Prépositionnement

Ils sont là, mais pourquoi ?

Difficultés d'intervention : discrétion nécessaire au cas où l'attaquant cherche à saboter le SI de la cible

Stratégie de réponse qui peut passer par une **exposition publique**.

Au programme

1. Du CERT-A au CERT-FR
2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

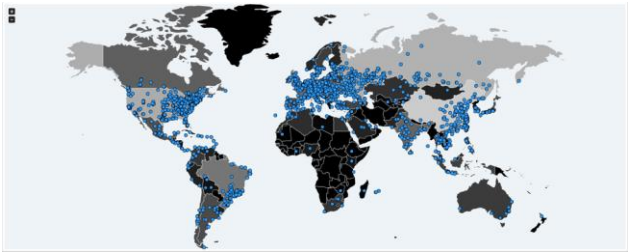
L'émergence des rançongiciels comme menace structurelle

2017 : **WANNACRY**

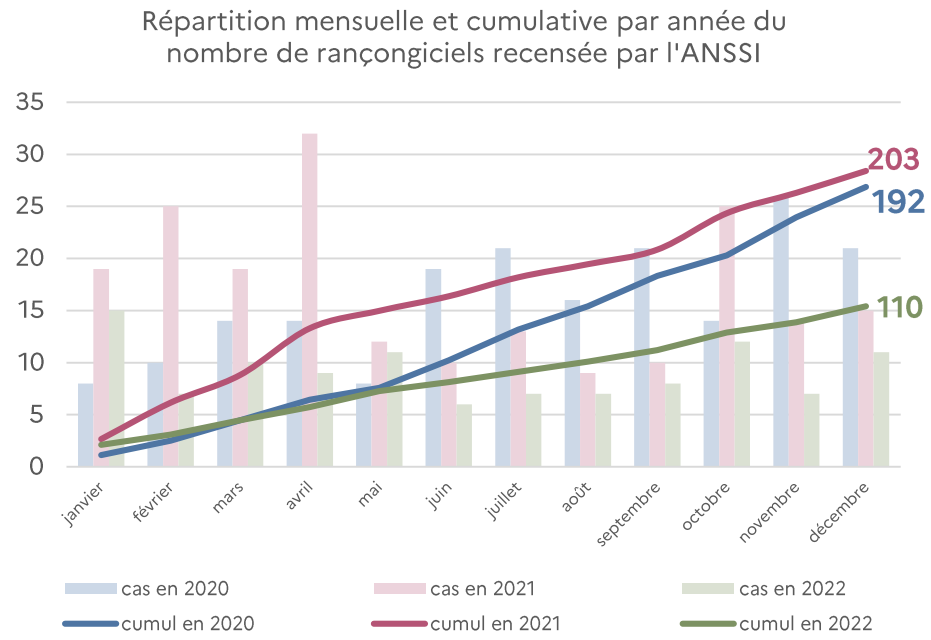
À partir de 2018 : big game hunting

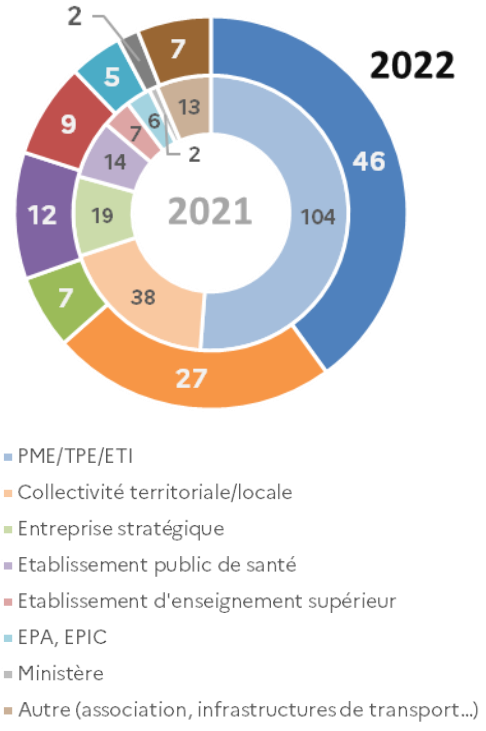
Écosystème cybercriminel de plus en plus **professionnel et réactif**

Chiffrement & chantage à la divulgation de données (2020 - …)



Rançongiciels : des victimes et impacts variés

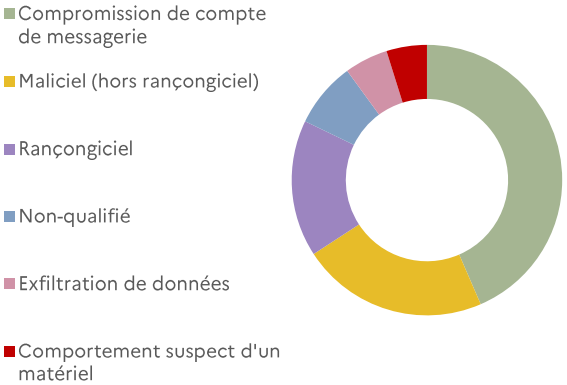


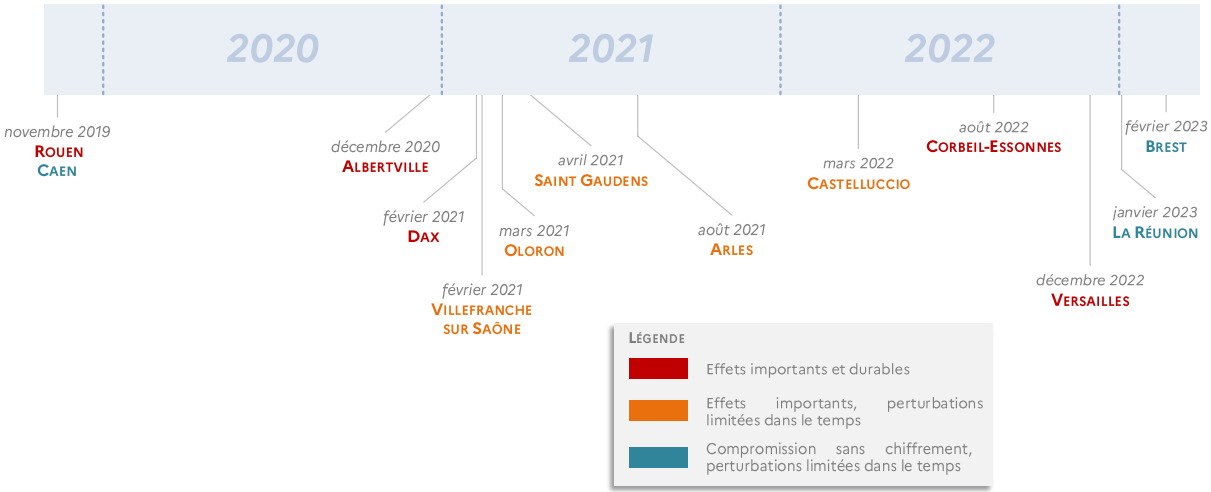


La menace rançongiciel

Un secteur de la santé structurellement à risque

Types d'incident affectant les établissements de santé depuis 2020





La menace rançongiciel

Quelle stratégie ?

Anticiper

- Production de **connaissance de masse**
- Echanges **partenaires**
- Alertes sur des **vulnérabilités**

Répondre

- Prise en charge de victimes sur l'ensemble du territoire
- Appui sur des **relais** (prestataires, CSIRT)
- **Interventions** avec équipes dédiées si nécessaire

Cybercrime : émergence de l'anticipation

Agir pour « **prendre une longueur d'avance** » sur les attaquants

Alerter les victimes potentielles au plus tôt

Travail sur les **fournisseurs** (*Bullet Proof Hosters*, etc)

Travail en **coopération avec les services enquêteurs** français et européens

Anticipation sur les actions des attaquants

Automatisation des actions de détection et d'alerte

Au programme

1. Du CERT-A au CERT-FR
2. 15 ans d'opérations

Espionnage : toujours au cœur des actions du CERT-FR depuis sa création

Déstabilisation : sabotage, prépositionnement, hacktivisme

Irruption du **cybercrime**

Conclusion

MERCI POUR VOTRE ATTENTION