AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Intervention et suivi des cyberincidents

LA E-SANTÉ FRANÇAISE
CERT Santé

Olivier Cros - 18 avril 2023

TLP : CLEAR

Les missions du CERT Santé

Réponse sur Incidents

- Intervention d'urgence
- Traitement des déclarations d'incidents de sécurité

Intelligence de la menace

- Veille en vulnérabilités
- Actualité de la cybersécurité

Communication

- Animation d'une communauté autour de la SSI en santé

Audits

- Exposition sur Internet des SI Santé

Les grandes étapes de la réponse à incident

QUALIFICATION

1

Réaliser une première **évaluation d'un incident** et de ses impacts avérés ou potentiels, et de le partager si nécessaire

CONFINEMENT

2

Partager un ensemble de recommandations pour **isoler une partie du SI** en cas d'incident de cybersécurité

INVESTIGATION

3

Rechercher les origines et les modalités d'une attaque informatique, ainsi que les éléments du SI qui sont compromis

REMEDIATION

4

Mettre en place les premières mesures permettant de sécuriser à nouveau le système d'information afin de bloquer l'attaquant

En fonction du contexte, ces étapes peuvent être réalisées simultanément

DURCISSEMENT

5

Renforcer la sécurité afin d'**être plus résilient face** à la menace cyber existante et éviter de nouvelles compromissions

Accompagnement optionnel et dépendant du niveau de sécurité du SI

En fonction de la criticité de l'incident et du diagnostic défini, le CERT Santé peut éventuellement accompagner sur la reconstruction du système d'information compromis

Les étapes de l'appui à la réponse à incident proposé par le CERT Santé

Le périmètre d'intervention du CERT Santé

Actions réalisées systématiquement

1 Qualification*

Prise de contact suite à la déclaration d'un incident afin d'**identifier les risques** et diffusion d'une **alerte vers les autorités compétentes** de l'État selon la nature de l'incident**.**

2 Confinement*

Préconisation de mesures de confinement afin d'**empêcher la propagation de l'activité malveillante**

Actions réalisées selon les cas et la criticité des actes de cyber-malveillance

3 Investigation*

Mise à disposition d'outils de recherche de compromission et d'investigation afin d'analyser les résultats et d'**identifier le scénario de compromission**

4 Remédiation*

Proposition d'un plan d'actions pour **protéger le SI contre une nouvelle attaque** et relancer les services numériques essentiels

Actions réalisées selon les cas et la criticité des actes de cyber-malveillance

5 Durcissement**

Le rapport de gestion de l'incident contient des **recommandations complémentaires pour renforcer le SI** (au-delà de la réponse à incident)

* En fonction du contexte, ces étapes peuvent être réalisées simultanément
****** Optionnel - Dépend de la criticité de l'incident

Postures d'incident

Aide au confinement	Appui technique	Suivi de remédiation	Pilotage et suivi
• Qualification d'incident • Mise en place de mesures de confinement adaptées	• Investigation • Collecte • Analyse de l'incident	• Application de mesures de remédiation, durcissement • Renforcement du SI post-incident	• Interlocuteur pour les prestataires et acteurs impactés par l'incident, • Suivi de l'application du confinement

Exemple d'accompagnement « post-crise »

DÉFINITION D'UN PLAN DE REMÉDIATION ET ACCOMPAGNEMENT DU CERT SANTÉ

/ Les principaux **axes mises en œuvre** sont :

- **Segmentation réseau** du système d'information
- **Limitation** de **l'obsolescence** du parc informatique (plus particulièrement sur les machines/équipements critiques)
- **Durcissement** des machines/équipements
- **Changement** des **pratiques** d'administration du système d'information
- Déploiement de nouveaux **outils de sécurité**

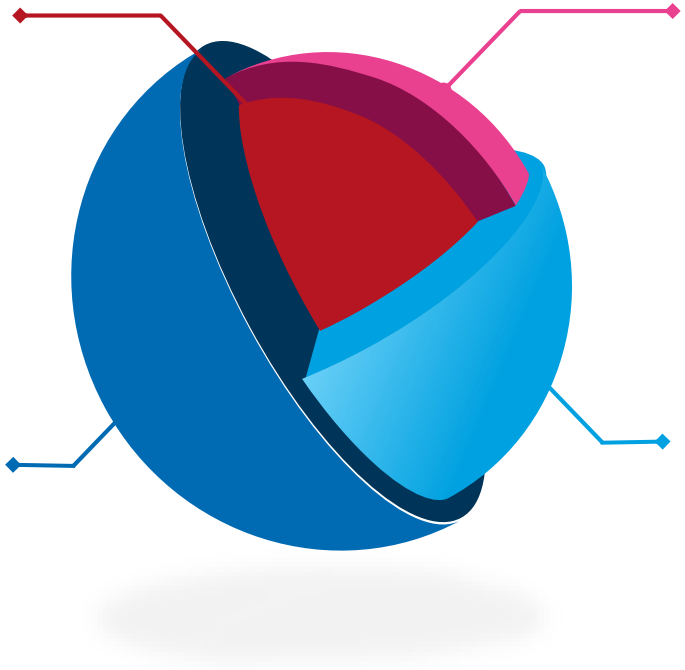
Les étapes du déploiement du plan de remédiation

1. Services critiques / socle SI

S'assurer que le cœur de l'infrastructure est sécurisé

2. Services métiers

Contrôler les périmètres métiers et reprendre peu à peu un usage standard



4. Interconnexions et services exposés

Rétablir les connexions extérieures et les solutions de surveillance

3. Postes de travail

Remettre en service les postes de travail pour tous les collaborateurs

Le CERT Santé en quelques chiffres (données 2022)

592
incidents déclarés

170
demandes d'accompagnement

103
interventions d'appui technique

112
audits réalisés

303
Bulletins de veille partagés

2200
alertes envoyées

76
cas de compromission

20
Interventions d'assistance

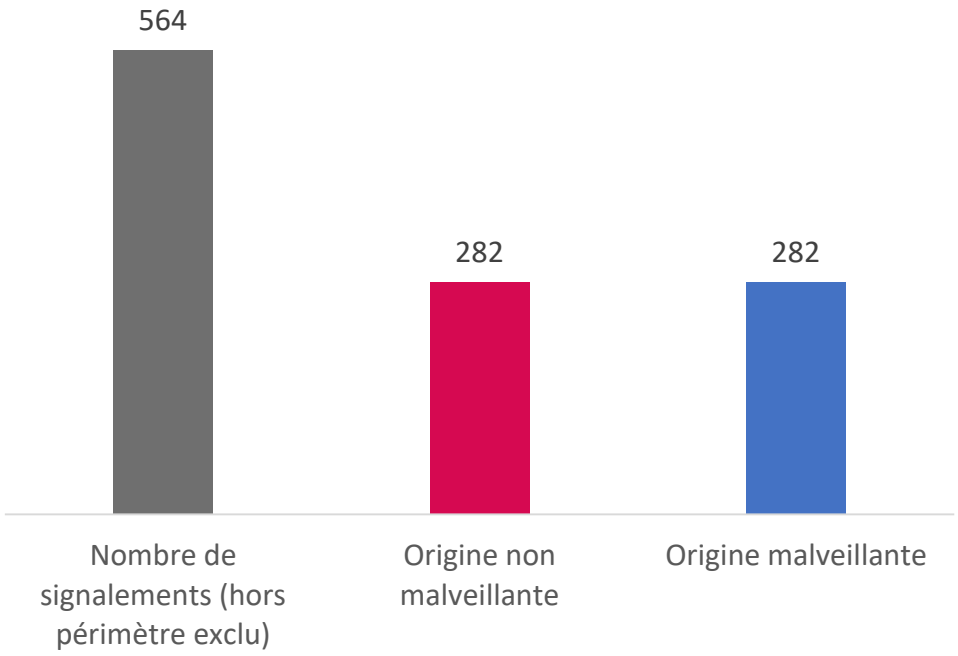
Rapport d'activité 2021 du CERT Santé :
https://www.cyberveille-sante.gouv.fr/index.php/rapport-de-l-observatoire

Gestion des incidents 2022 - National

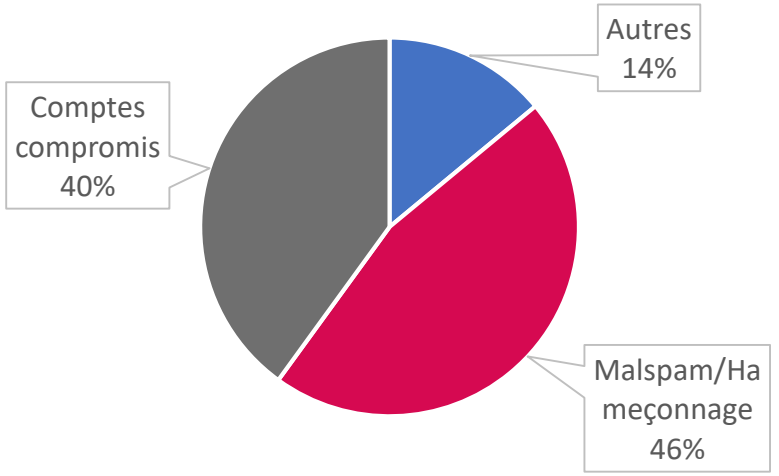
432 **(+33%)**
structures ont déclaré
au moins un incident

27 **(-49%)**
Attaques par rançongiciels

Origine des incidents



Types de compromission



Les attaquants récupèrent les identifiants selon plusieurs modes opératoires :
- Hameçonnage (phishing)
- Identifiants mutualisés
- Mots de passe faibles
- Exploitation de vulnérabilités sur des équipements non mis à jour
- Technique de brute force : test d'un grand nombre de mots de passe

Objectifs d'investigation

Reconstruire la chaîne de compromission

Vulnérabilités exploitées, failles, connexions

Recherche d'indicateurs

Adresses IP, domaines, fichiers, comptes, ...

Cartographie du périmètre compromis

Liste des machines, serveurs, comptes... compromis

Identifier le type de compromission

Rançongiciel, exfiltration, exploitation, vol d'identifiants, DDoS

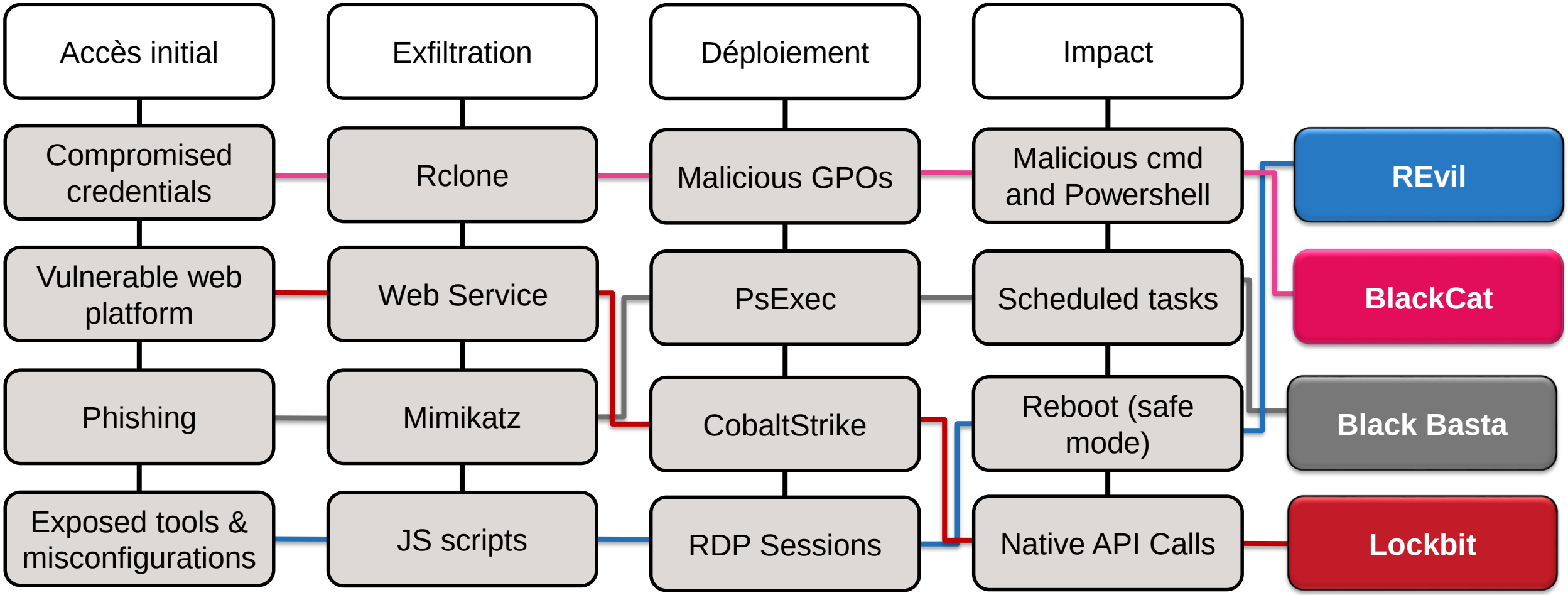
Cartographier les éléments exfiltrés

Nature des données, quantité, criticité

Points de vigilance

Points d'entrée	Brute-force RDP, Vulnérabilité sur système exposé, erreurs de configuration, phishing, Outils de sécurité exposés
Reconnaissance	Scripts powershell, netscan, commandes cmd
Persistence	Nouveaux comptes, changements de GPO, Outils ShadowIT, tâches planifiées, services suspects
Outils de déploiement	Infrastructure dédiée, comptes compromis, infrastructure compromise (interne, externe)
Latéralisation	CobaltStrike, WMI/RDP, outils d'administration, PsExec

Groupes actifs



Comment solliciter le CERT Santé en cas d'incident ?

EN HEURES OUVRÉS (HO)

Déclarez votre incident en heures ouvrées (9h-18h du lundi au vendredi) sur le **portail de signalement des évènements sanitaires indésirables** (interface professionnel de santé) - **signalement.social-sante.gouv.fr** - via un formulaire de déclaration.

EN HEURES NON OUVRÉS (HNO)

En cas d'incident majeur, contactez le CERT Santé par téléphone au **09 72 43 91 25** ou par mail à l'adresse **cyberveille@esante.gouv.fr**

Le CERT Santé **priorise ses interventions** selon la nature de l'établissement et des impacts sur la prise en charge des patients.

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Questions ?

cyberveille@esante.gouv.fr