Anatomie des attaques de rançongiciel récentes

un retour d'expérience

Christophe Renard

SGDSN/ANSSI/SDO/DR

10/11/2020

Plan

Plan

Qui suis-je ?

- Consultant, développeur, admin-sys (presque) repenti
- Agent de la Division Réponse de l'ANSSI
  - Qui fait partie de la Sous-Direction Opération
  - De l'ANSSI, qui est une partie du SGDSN
  - Qui est un Service du Premier Ministre

Que fais-je ?

- Responsable d'investigation sur les opérations
  - Responsable de la qualification des incidents importants
  - Participe aux mesures d'endiguement
  - Pilote le volet enquête
  - Fait la jonction entre l'analyse forensique et les mesures de défense
- L'ANSSI recrute :

  `https://talents.ssi.gouv.fr/offresdemploi/`

  `pilote-technique-specialise-en-traitement-d-incidents-informatiques`

Ce que je ne vais pas aborder

- Des incidents précis
  - Même publics, ils sont souvent couverts par le secret de l'instruction
- Des recommandations de défense
  - Je n'ai pas le temps
  - Le guide des 42 mesures de l'ANSSI couvre bien les risques évoqués
- Des détails sur les attaquants
  - Voir le point sur le secret de l'instruction
  - Ça ne sert pas à grand chose pour se défendre

Face aux rançongiciels 1/2

- Le rôle de l'agence est la protection des intérêts de l'État contre les menaces de sécurité informatiques :
  - Prévention
  - Réponse à incident
  - Partage de la connaissance
- L'objectif de l'ANSSI est d'empêcher ou résoudre l'incident, pas d'arrêter un criminel.
- Nous travaillons avec :
  - Acteurs publics : Parquet, Police, Gendarmerie, ACYMA...
  - Acteurs privés : PRIS, CERTs, prestataires de la victime...

Face aux rançongiciels 2/2

- Explosion des attaques de rançongiciel :
  - 104 attaques traitées entre le 1er janvier et le 1er septembre 2020
    - Forte augmentation par rapport à 2019
    - Sujet mineur pour l'ANSSI avant 2018 (hors Wannacry/NotPetya)
    - Pas de corrélation visible avec la crise sanitaire
  - L'ANSSI ne traite qu'un ensemble restreint :
    - Fonction publique
    - Acteurs critiques (OIV, OSE...)
    - Impacts stratégiques, économiques ou humains majeurs
  - La plupart sont des crises aiguës pour les victimes
    - Destructions importantes
    - Arrêt de production
    - Parfois pas de scénario évident de retour à la normale

Communication

- Guide orienté directions avec le ministère de la Justice

  https://www.ssi.gouv.fr/guide/

  attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/
- Renseignement sur la menace - https://www.cert.ssi.gouv.fr/cti/
  - Emotet - https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-010/
  - TA505 - https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-006/
  - Dridex - https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-005/
  - PYSA - https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
  - Revue des MOA - https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/
  - C1OP - https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-009/
  - Bitpaimer - https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-006/
- Alertes du CERT-FR - https://www.cert.ssi.gouv.fr/alerte/
- Guides de bonnes pratiques -

  https://www.ssi.gouv.fr/administration/bonnes-pratiques/
- Action des coordinateurs régionaux et sectoriels

Plan

Les attaquants

- Attaquants criminels
  - Pas d'autres motivation que le profit
    - Cherche à tirer le plus possible, le plus vite possible de la victime
    - Escalade dans les attaques et dans les rançons
  - Adaptation rapide aux changements de situation
    - Initialement rançongiciels autonomes
    - Passage aux rançongiciels déployés manuellement
    - Escalade de la pression: fuite de données, dénis de service...
  - Tendance à la structuration croissante:
    - Groupes experts fournissant outillage, infrastructure voire blanchiment
    - Vendeurs de comptes et accès piratés
    - Attaquants qui vont déployer le rançongiciel
    - Négociateurs qui font payer
  - On trouve des acteurs de tous les niveaux de sophistication

Les victimes

Les victimes

- Pas de vrai typologie
  - Choisie pour la combinaison d'accès et de rentabilité estimée
- Certains attaquants semblent faire des campagnes thématiques
  - Si un type d'organisation a payé
  - Autant attaquer les autres du même type
- Êtes vous ciblé ?
  - **Oui**

Plan

Plan

Le patient 0

- Souvent par un système exposé
  - *Combustible :* un point d'accès accessible depuis Internet
  - *Comburant :* une faille ou un compte
- Ou par courriel
  - *Combustible :* poste utilisateur
  - *Comburant :* généralement un document Ms Office piégé

Bestiaire des points d'entrée

- Exploitation des failles majeures
  - Exemples (liste non exaustive) :
    - CVE-2019-11510 sur PulseSecure
    - CVE-2019-19781 sur Citrix
    - CVE-2019-0604 sur Sharepoint
  - Failles faisant l'objet de scans massifs sur tout IPv4 dès publication d'un exploit
- Enumérations de mots de passe sur services exposés sur Internet
  - RDS de serveurs du domaine
  - Machines virtuelles du domaine dans les grandes infrastructures nuagiques
  - Comptes acquis dans des fuites de données ou par hameçonnage
- Campagnes de mailing de botnets
  - Emotet
  - Dridex

La messagerie reste une valeur sure

Latéralisation

- Un fois entrés les attaquants cherchent à étendre leur emprise
  - Balayages réseaux
  - Explorations systèmes par RDP, RCP et mount SMB
  - Utilisations de cadriciels offensifs sur étagère
    - *Powershell-Empire*
    - *Cobalt Strike*
    - *Metasploit*
  - Souvent détectés par les logiciels de sécurité
    - et ignorés
  - Adresses de serveurs de contrôle et commandes
    - VPN et TOR : peu pratique pour des connexions inverses
    - Serveurs piratés : fastidieux se prêtant mal à un usage soutenu
    - Serveurs et VPS : loués à des revendeurs *bulletproof* ou peu regardants

Pourquoi élever les privilèges ?

- Les privilèges élevés sont nécessaires pour :
  - Impacter le plus de systèmes possibles
  - Désactiver les sécurités
  - Stopper les processus qui pourraient verrouiller les fichiers
- Donc il faut devenir au moins administrateur des serveurs importants
  - Voire administrateur de tous les systèmes
  - Et souvent, administrateur du domaine
- **Attention**: un compte utilisateur normal peut souvent faire beaucoup de mal
  - Sur les serveurs de fichiers en particulier

Acquisition triviale des privilèges

- L'attaquant va aller au plus simple
  - Réutilisation de couples login/mot de passe non privilégiés
    - quand `adm_toto` et `usr_toto` utilisent le même mot de passe
    - ou extrapolation à partir de règles de génération
  - Enumération en force brute sur des applications non bloquantes
  - Pêche dans le SI:
    - Le Excel de l'infogérant avec tous les mots de passe
    - Les raccourcis de connexion avec mot de passe sauvé
    - Les fichiers texte contenant les commandes à copier/coller sur le bureau des administrateurs
  - Piégeage de point d'eau
    - Applications web internes
    - Bonus si c'est le portail du VPN

Acquisition pour l'attaquant technicien

- La meilleure source c'est la mémoire des serveurs
  - Mimikatz ou Procdump, puis Mimikatz à la maison
  - Chasse aux administrateurs avec *Bloodhound*
  - Il faut trouver une machine non patchée pour une faille avec un code d'exploitation public
- Les attaquants suivent les sorties d'outils offensifs et les testent très rapidement
  - Il y a une course entre la publication et la correction

ROP or not ROP ? (not)

Pérenniser ses accès

- L'attaquant a besoin de temps
  - Pour déployer son attaque
  - Pour revendre les accès
  - Pour prendre la victime à la gorge à un bon moment
- Quand une anomalie est détectée
  - Le réflexe le plus courant des défenseurs est de réinitialiser les mots de passe
  - Les attaquants le savent et s'adaptent

Comment pérenniser ses accès ?

- Les méthodes de persistance doivent résister aux changements de mots passe et désactivation de compte
- Trois approches sont communes, isolément ou en combinaison
  - Création de comptes privilégiés
    - Création de comptes Active Directory
    - Ou déplacement de comptes existant dans un groupe privilégié
    - Création de comptes administrateurs locaux
  - Ajout d'implants :
    - RAT
    - Webshell
    - ou simples tunnels inverses
  - Création d'un *Golden Ticket*

Plan

Retour de l'attaquant

- Temps long avant le chiffrement
  - Dans la plupart des cas traités par l'ANSSI
    - Souvent des semaines entre compromission initiale et cryptolockage
    - Parfois des mois
  - Sans doute lié à des développement de *porte-feuilles* de victimes
    - Et à leur commercialisation
- Pourrait changer
  - Attaques *flash* relatées en sources ouvertes
  - De la compromission au chiffrement en quelques heures

Exfiltration de données

- Nouveauté 2020
  - Moyen de pression supplémentaire sur la victime
    - Chantage à la divulgation de données
    - Souvent avec révélation progressive
- Ne pas confondre avec :
  - Les sorties de données pour appuyer l'attaque
    - Documents d'architecture et procédures
    - Fichiers contenant des identifiants

Préparation de l'attaque

- L'attaquant veut un déploiement fluide du rançongiciel
  - Nécessite
    - de neutraliser les antivirus
    - D'éteindre au dernier moment les processus serveurs
    - Et de s'assurer que les cibles pertinentes soient atteintes
- Il va souvent faire des tests
  - D'extinction des antivirus
  - De connexion sur des cibles
- Cette phase génère des événements détectables
  - Détections virales
  - Crash des antivirus
  - Arrêts inopinés de services
  - Connexion depuis le contrôleur de domaine

Plan

Plan

Technologie du déploiement

- Objectif
  - Copier et exécuter à grande échelle un programme effectuant le chiffrement
- Utilisation des mécanismes d'administration
  - Fichiers *Batch* de *PsExec* en série
  - Création de tâches à exécution instantanée par GPO
  - Récemment utilisation de BITS
- Certaines attaques utilisent plusieurs moyens simultanément
- Le déploiement peut être très rapide
  - Milliers de machines par minute

Action sur la cible

- Que fait le code déployé ?
  - Effacement de *Shadow Copies*
  - Recherche de fichiers à chiffrer
  - Chiffrement des fichiers
  - Création des messages d'invitation à contacter l'attaquant
    - Dans des fichiers texte
    - En fond d'écran
  - Parfois, le code rend compte de sa mission
    - Télémétrie de l'attaquant
    - Opportunité de mesurer l'ampleur de l'attaque

Actions d'accompagnement

- L'attaquant ne quitte pas toujours le SI qu'il chiffre
  - Vérification de l'effectivité du déploiement
  - Observation des réactions de la victime
  - Effacement des traces
    - Effacement des outils
    - Purge des événements Windows
    - Nettoyage de comptes AD
  - Parfois, le chiffrement coupe l'herbe sous les pieds de l'attaquant

Plan

L'entrée dans la crise

Premiers signes de l'incident

- Le déclenchement est souvent choisi dans une période d'équipes réduites
  - Week-end
  - Jours fériés
- Rarement évidents :
  - Services indisponibles
  - Postes utilisateurs qui redémarrent spontanément
  - Fichiers devenus illisibles
- L'attaque est en général confirmée par la découverte de demande de rançon sur de multiples machines.

Escalade

- Quelqu'un doit décider du passage en crise
  - La crise est anormale et coûteuse
  - Donc l'information doit prendre le temps de remonter la hiérarchie
    - Avec confirmation à chaque étape
    - Plusieurs heures peuvent s'écouler
- La mobilisation des externes est plus longue
  - Les infogérants en quelques minutes à quelques heures
  - Les intervenants en investigation numérique ou gestion de crises, de quelques heures à quelques jours
  - Les experts en reconstruction, plusieurs jours
- L'ANSSI
  - Prend l'appel instantanément
  - Rappelle normalement en moins d'une heure
  - Qualifie sur plusieurs heures

L'entrée dans la crise

Plan

Mesures d'endiguement réseau

- Extinction de l'accès Internet
  - Efficace contre les attaques "interactives"
    - Wannacry reste une exception
  - Mais difficile à l'échelle d'un groupe
    - Et va contrarier la reconstruction
- Filtrage réseau
  - Niveau 2 ou 3
  - Efficace, mais necessite d'en garder trace
- Coupure des accès tiers
  - Attention aux accès des sous traitants indispensables
  - Activer le multifacteur sur les VPN est efficace, mais lourd
  - Pose la question de la communication avec clients et fournisseurs

Mesures d'endiguement système

- Désactivation des comptes de l'attaquant
  - Peut couper l'attaque, mais rarement les persistances
- Extinction des systèmes
  - Efficace, sur l'instant
  - Mais attention au redémarrage
  - Et certaines applications supportent mal les extinctions d'urgence
  - Très efficace pour les serveurs de fichiers
- Extension des couvertures antivirales et XDR
  - Intéressant si l'outil bloque bien le chiffreur
  - Penser à remonter les échantillons à l'éditeur
  - Mais l'attaquant les a éteint une fois...

Plan

Plan

Organisation de la crise

- Désignation des personnes en charge
  - Décisionnaires
  - Responsables des différents fils de travail
  - Contacts externes
  - Gestionnaire du projet de crise
    - C'est le rôle crucial souvent oublié
- Organisation de la logistique de crise
  - Moyens de communication
    - Hors SI compromis de préférence
    - Accès Internet haut débit indispensable
  - Personnels et suivi des temps
    - Attention au surmenage et horaires excessifs
    - Et aux retours en voiture après 16h intensives
  - Nourriture, boisson, couchage...
- Communication de crise
  - Déterminant pour la confiance
  - Beaucoup de ratés

Déclarations

- Question récurrente: la CNIL
  - La CNIL prend les pré-déclarations *initiales* `https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles`
  - Même en l'absence de preuve de fuite de données personnelles
  - Vous pourrez corriger ultérieurement si vous estimez que finalement rien n'est sorti
- L'assurance
  - Même si vous ne vous pensez pas couvert
  - Le T0 de couverture commence souvent à la déclaration
  - Les assureurs ont souvent des prestataires à recommander
- Déclarations trimestrielles
  - Les attaquants adorent les périodes sensibles
- Toutes réglementations spécifiques au métier de la victime
  - Quasiment toutes ont maintenant un volet *Cyber*

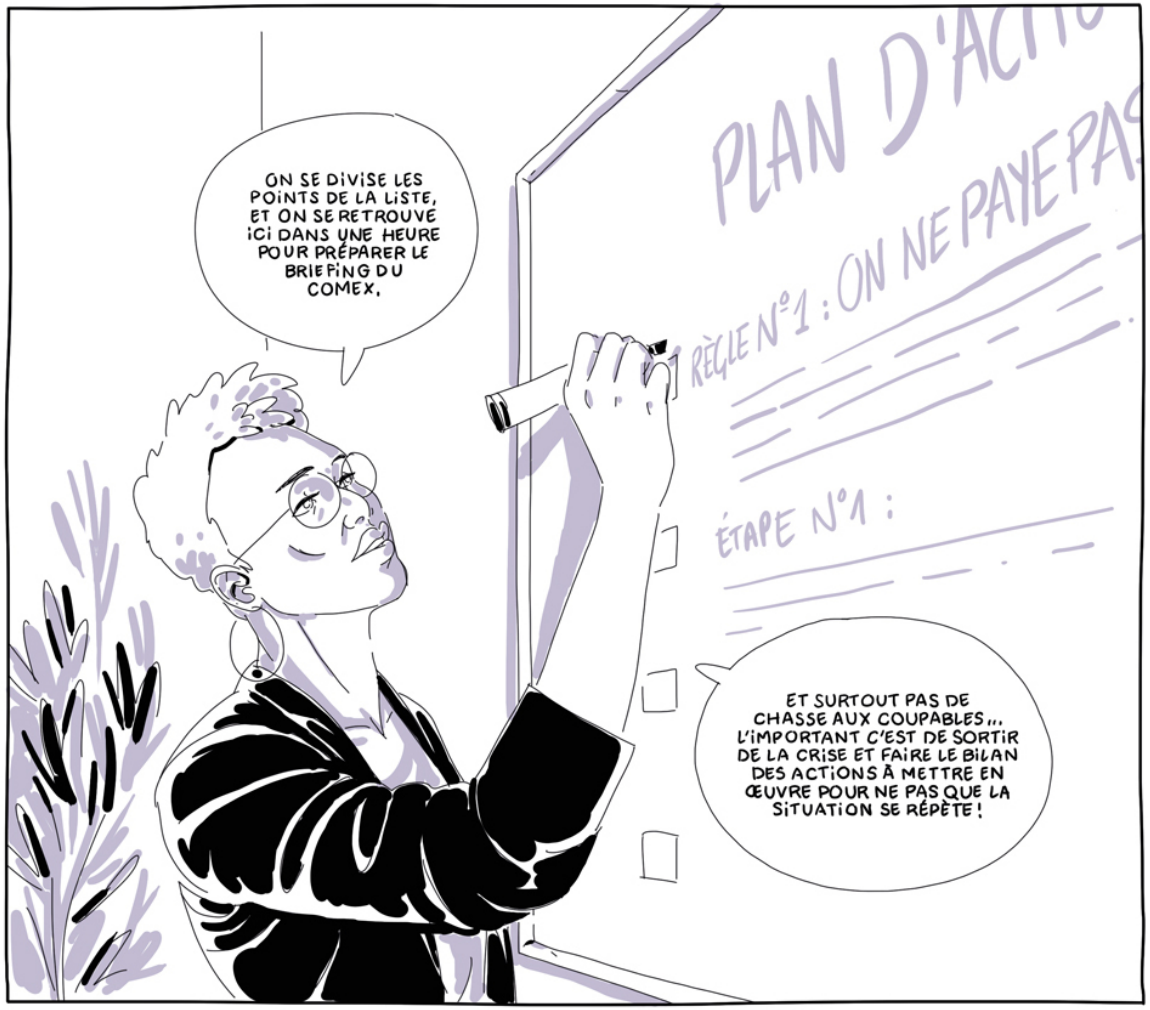
Communication

- Communication interne
  - Que dire aux employés ?
  - Et aux sous traitants internes ?
  - L'information part souvent sur les réseaux sociaux
  - Attention à la circulation de conclusions intermédiaires
- Communication aux partenaires
  - Fournisseurs
  - Clients
  - Attention aux engagements de retour à la normale précoces
- Communication publique
  - Une crise se voit
  - Le mutisme est anxiogène et suscite des rumeurs
  - Les prétentions de maîtrise excessives créent une pression supplémentaire au redémarrage rapide à tout prix

Dépôt de plainte

- Porter plainte
  - Souvent demandé par l'assureur
  - Permet de démarrer des poursuites judiciaires
  - Plainte à un service généralement local
  - Un service enquêteur pertinent est ensuite désigné par le parquet
- Les services de police et gendarmerie ont une expertise rançongiciel conséquente
  - Mais sont très sollicités
  - N'attendez pas des résultats d'enquête dans le temps de la crise

Le plan


ON SE DIVISE LES POINTS DE LA LISTE, ET ON SE RETROUVE ICI DANS UNE HEURE POUR PRÉPARER LE BRIEFING DU COMEX.
PLAN D'ACTI
RÈGLE N°1 : ON NE PAYE PAS
ÉTAPE N°1 :
ET SURTOUT PAS DE CHASSE AUX COUPABLES... L'IMPORTANT C'EST DE SORTIR DE LA CRISE ET FAIRE LE BILAN DES ACTIONS À METTRE EN ŒUVRE POUR NE PAS QUE LA SITUATION SE RÉPÈTE !

Erreurs communes 1/2

- Gérer la crise sur un plan purement technique
  - **La crise rançongiciel est une crise stratégique**
  - Il ne faut pas la piloter uniquement sous l'angle informatique.
- Penser que la crise va se gérer en une poignée de jours
  - **Aucune crise rançongiciel que j'ai observée n'a duré moins de 3 semaines**
  - Comptez plus d'une semaine d'interruption partielle ou totale de service
- Tenter de tout gérer en interne
  - Il va falloir enquêter, reconstruire, déployer des mesures temporaires, restaurer des sauvegardes
  - **Personne n'a les équipes interne pour tout faire**

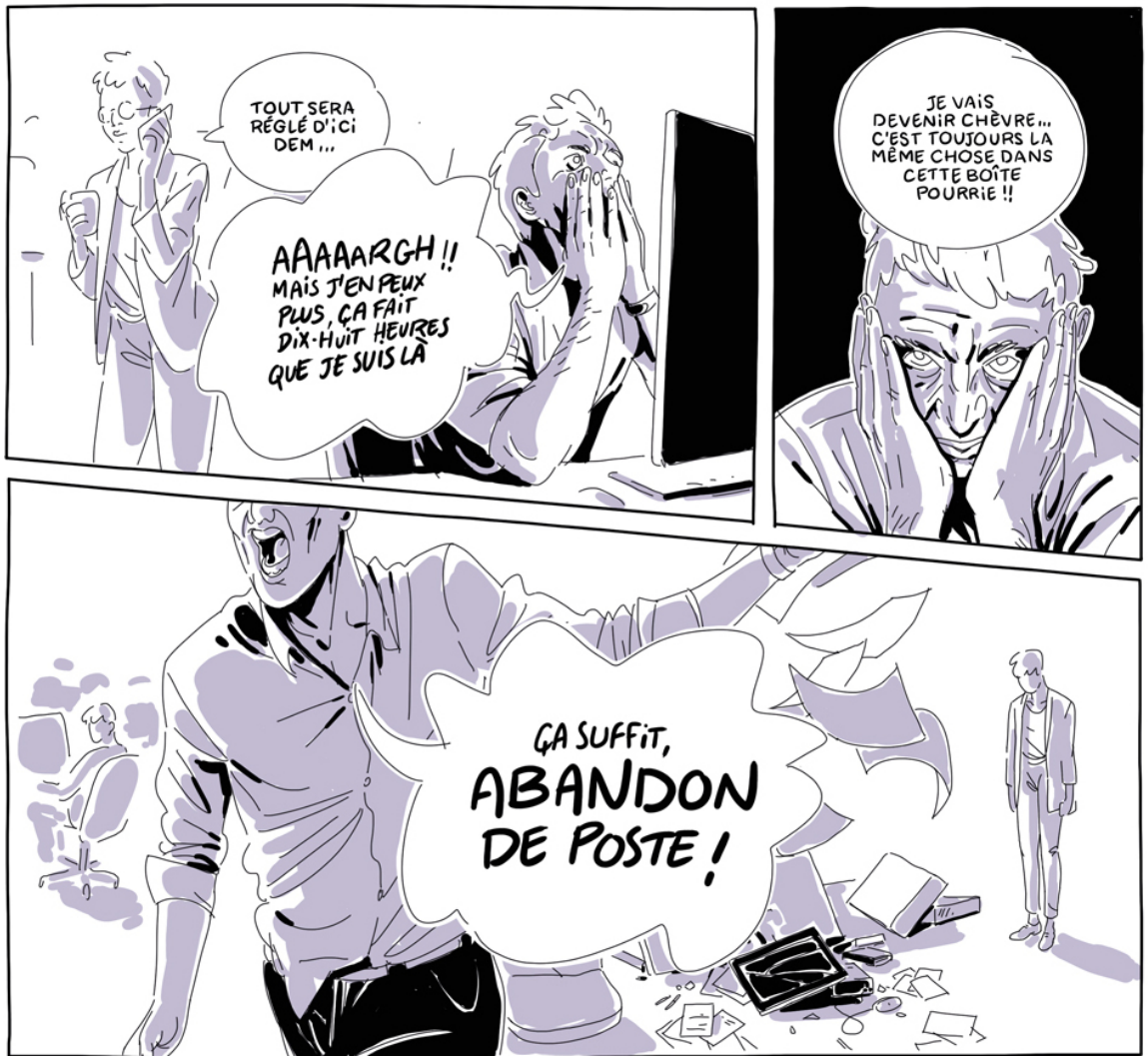
Erreurs communes 2/2

- La chasse aux sorcières
  - **Chercher un coupable en cours de crise est suicidaire**
  - Mais ça se fait quand même
- Faire reposer l'organisation sur une seule personne
  - Personne ne tient 3 semaines de crises sans repos
  - **Les *burnouts* en cours d'incident arrivent**

Temps intense et temps long

- Pour les équipes des victimes
  - La crise est un événement exceptionnel
    - Ils ne devraient pas en voir plusieurs dans leur carrière
  - Il faut mettre en oeuvre des mesures de sécurité dans un temps anormal
  - Mais aussi, liberté de l'allégement des procédures et des actions qui s'accomplissent vite
  - Elles traversent
    - Désorientation
    - Crainte
    - Une certaine ivresse
    - Épuisement

Attention au *burnout*



Plan

Pourquoi enquêter ?

- L'objectif de l'enquête n'est pas seulement un rapport
  - Identifier des marqueurs pour nourrir la détection
  - Recherche des persistances
  - Identifier le chemin de compromission
    - Neutraliser le chemin d'escalade de privilège
    - Et si possible, le point d'intrusion initiale
  - Donner des éléments aux acteurs externes
    - Justice
    - Éditeur de logiciel d'AV ou EDR
    - ANSSI
- Ne pas oublier d'alimenter les décideurs en informations à jour, précises et synthétiques.

Plan

Les grandes activités techniques de l'après

- Recréation d'un coeur de confiance
  - D'où gérer les identités et les accès
  - Voir

    `https://www.sstic.org/2017/presentation/administration_en_silo/`
- Nettoyage des systèmes
  - Chasse aux persistances (jamais exhaustive)
  - Augmentation de la supervision de sécurité
- Redémarrage des services
  - Parfois sur des infrastructures temporaires
- **Attention**:
  - Si la remédiation est bâclée
  - Les attaquants peuvent revenir, et rechiffrer

Plan

Restaurations

- **Restaurer n'est jamais trivial**
- Soit depuis les sauvegardes, des reconstitutions, voire depuis un déchiffreur
  - Systèmes et applications désynchronisées
  - Réconciliation des données d'avant et après le chiffrement
  - Temps de redémarrer des applications lourdes (bases de données par exemple)
  - Découverte de dépendances complexes
  - Si restauration de sauvegardes, de quelle date ?
- L'expérience de test de restauration est précieuse
  - Toutes les raisons de ne pas les faire en temps calme sont rendues pires par un environnement dégradé et le stress

Absorption des impacts

- Les impacts sont multiples
  - Image (suivant communication)
  - Techniques
    - Évolutions brutales du SI
    - Bricolages temporaires
  - Financiers
    - Coût de la crise
      (heures supplémentaires, sous-traitance, licences logicielles, logistique)
    - Perte d'activité
    - Coût de la mise à niveau du système d'information
  - Réglementaires
    - Pénalités ou pertes de d'autorisation
    - Pensez aux déclarations obligatoires post-incident
  - Humans
    - Récupérations RH
    - Gestion de l'après émotionnel

Plan

Au plaisir de ne pas vous rendre visite

Questions ?