

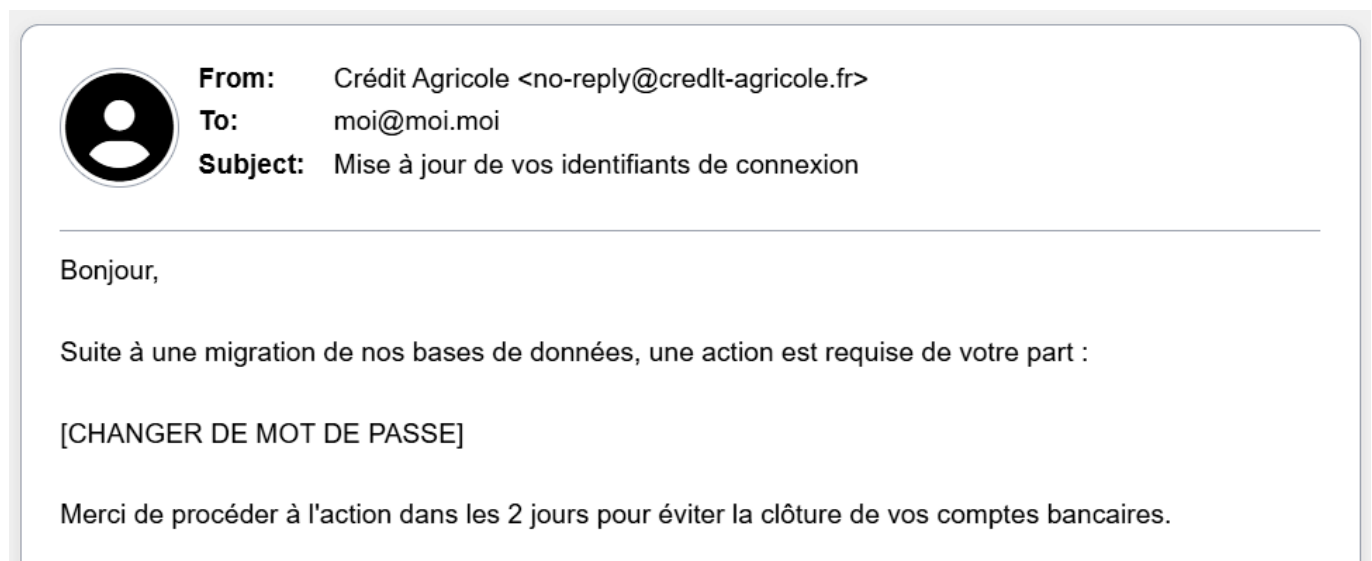
Laboratoire 04 - Gauvain BOICHÉ - 11/02/2026

Hameçonnage

Les exemples ne manquent pas. Banque, client, ami, femme très chaude dans ma région... bref. De mon expérience professionnelle, l'hameçonnage "Service IT" est un fléau bien réel.

Je vais générer de faux courriels d'hameçonnage avec l'outil [Email Screenshot Generator](#).

La Banque



Classique des courriels génériques, s'appuyant sur divers leviers :

- la peur (fermeture des comptes en 2 jours)
- le côté officiel (credlt-agricole.fr)
- la personnalisation (Prénom + Nom)

Le lien emmènera vers "https://shatrzzaer.amstrack.ru/credit-agricole.php" et le client ne verra rien, la page sera un clone parfait du Crédit Agricole.

Détection

- l'adresse courriel => credlt-agricole.fr et pas credit-agricole.fr, mais là comme ça, on s'en rend pas compte forcément tout de suite
- le côté urgent
- l'hyperlien louche

Le nom de domaine n'étant pas spécialement usurpé, le filtre à hameçonnage ne se déclanche pas forcément et demande une vigilance spécifique.

Vérifications

- Survoler l'hyperlien et regarder la racine

- Aller depuis un moteur de recherche ou un favori sur la page de connexion de la banque et vérifier sa messagerie interne
- Contacter par téléphone sa banque et/ou son conseiller pour contre-vérifier

Le collègue



From: John BIGBOSS <john.bigboss@gmail.com>
To: jonathan.berbier@gcourriel.fr
Subject: Demande d'assistance

Bonjour Jonathan,

J'ai besoin que tu m'ouvres cette pièces jointes et que tu traitent les information contenus dedans. Peut-tu me faire ça dans la journée stp ? C'est urgents.

John

[0facturation2025fournisseurs.xlsx.bat]

Des variantes existent : l'ouverture d'un fichier, d'un lien pour signer un document alléchant (parts dans la boîte), urgent (document RH ou lié au travail), demande de service ("j'ai besoin de régler une transaction en bitcoin, peux-tu aller acheter des coupons TransCash ?") etc.

Les leviers sont là encore très humains :

- le côté hiérarchique (c'est le patron et on est un soumis)
- le côté urgent ("c'est urgents")
- les possibilités ("si j'aide le patron, il s'en souviendra à la prochaine revue de performances...")

Détection

En soit, les gros fournisseurs de services courriels détectent les scripts/codes et bloquent les réceptions. J'ai envoyé de vrais pièces de code légitimes à des collègues et je me suis fait bloquer les envois, faute d'avoir de clients de messagerie instantanée à disposition. Mais partons du principe que le courriel a été reçu.

- le fichier => majoritairement, les gens sont sur Windows, et la majorité des utilisateurs Windows ont l'option "afficher l'extension dont le type est connu" décoché et ne verront donc pas le .bat, juste le .xlsx, auquel il suffit de coller une icône d'Excel. C'est facile.
- le côté urgent
- l'adresse courriel qui est extérieure. Pourquoi pas depuis une adresse d'entreprise ?
- les fautes (cela dit, quand je vois comment écrivent certains chefs/clients/grands avocats, ce n'est plus tellement une cause de détection...)

Vérifications

- Le mieux c'est d'aller contacter le patron, soit par messagerie instantanée, soit par téléphone, soit en levant son derrière de sa chaise et en traversant le couloir pour aller demander

Le client/fournisseur



From: Farida AL MANSOUR <f.almansour@client.fr>
To: jonathan.berbier@gcourriel.fr
Subject: Facture n°385765-fe

Bonjour monsieur BERBIER,

Suite à votre commande du 3 janvier, veuillez trouver ci-joint la facture idoine. Merci de procéder au virement selon les modalités convenues à 45 jours FDM sur le compte suivant :

Nom : Farida AL MANSOUR
IBAN : FR76 1659 8205 0000 3591 1345 585
BIC : FPELFR21XXX

[invoice_385765_fe.pdf]

Celui-là est vache et correspond à du vécu. On parle de préjudices par dizaines de milliers d'euros chaque semaine.

Tout est plutôt crédible :

- la personnalisation => nom, mais aussi date précise, référence précise, termes précis
- pièce jointe légitime => le PDF est vrai
- ton formel et attendu
- compte de virement crédible => IBAN français, nom de la personne qui est le bon

Détection

Tout est quasi parfait, et la vérification demande de l'instinct. Le compte n'a à-priori rien d'anormal. Et pourtant : c'est un compte Nickel. N'importe qui peut ouvrir un compte sous n'importe quel nom, puisque ce droit au compte bancaire universel n'exige pas de carte d'identité ni d'adresse. Il s'ouvre en bureau de tabac en 1 heure à peine. Pas de traces, rien. Le virement se fait, mais sur le mauvais compte.

Vérifications

Il faut utiliser, si on en a le réflexe, un "Iban checker" et s'alerter de la banque retournée.

Si on appelle madame AL MANSOUR, elle répondra qu'elle a bien envoyé la facture à l'heure correspondante. Rien d'anormal alors. SAUF QUE, ce qu'elle ne sait pas, c'est que sa boîte a été compromise.

Elle-même victime d'un hameçonnage passé, le pirate a son mot de passe, une instance IMAP sur son PC, et que chaque courriel envoyé est systématiquement supprimé, et renvoyé DEPUIS SA BOÎTE LÉGITIME avec le nouvel IBAN.

Il peut se passer des mois avant qu'on ne s'en aperçoive. Généralement quand les comptables signalent qu'un virement n'a pas été reçu, et que madame AL MANSOUR appellera le client pour lui demander de régler la facture :

- On l'a déjà réglée.
- Oui mais nous n'avons rien reçu.
- On a fait le virement tel jour sur tel compte.
- Quel compte ?
- Oh.

Former les gens

- il n'y a pas de mystère. Contourner une sécurité informatique, c'est toujours possible. Et des sécurités trop fortes peuvent même bloquer des courriels légitimes, et porter atteinte au commerce.
- il faut former les gens encore et encore, répéter encore et encore les mêmes infos, et organiser des campagnes d'hameçonnages avec des partenaires dédiés. La faille c'est l'humain. C'est l'humain qu'il faut entraîner.

Attaque rançongiciel

L'attaque

Pièce jointe vérolée, site douteux sur le lieu de travail, propagation par ver... les vecteurs ne manquent pas. Toujours est-il qu'on est tombé, il faut maintenant se relever.

La réaction

"confidential_data.docx" est crypté, et une demande de rançon est demandée.

Premières étapes

1. Débrancher le PC infecté du réseau pour l'isoler
2. Conduire un audit interne (vérification des PCs avec en parallèle reconstruction d'une ligne temporelle de l'attaque) pour vérifier l'état de propagation

Secondes étapes

1. Désinfection du poste
2. Vérifier l'état de sauvegarde du document (sauvegarde dans un service nuagique)
3. Vérifier l'état de sauvegarde du poste (TimeMachine, Point de Restauration, Snapshot, etc)

Ne pas faire

1. Laisser le PC connecté au réseau interne
2. Payer la rançon :
 - les bandits n'ont pas forcément de clef de décryptage
 - on se fait fichier comme "un bon client" et on va être de nouveau victime
 - aux yeux de la loi, peut valoir comme "financement du terrorisme". On préfère éviter...
3. Engueuler le rançonné. C'est mieux d'avoir sa confiance et sa collaboration plutôt que ne pas le laisser assumer sereinement et passer à côté d'informations cruciales.

A faire

1. Utiliser des outils dédiés pour la désinfection

2. Utiliser un service de protection antivirus en temps réel avec capacités de détection de comportement
3. Faire une copie 3-2-1 régulière (au moins mensuelle) des données sensibles, simple sauvegarde du poste pour les utilisateurs finaux
4. Utiliser un pare-feu sévère qui bloque les sites malveillants (établis et potentiels)

Atelier de la politique de sécurité

Politique de sécurité informatique

Les utilisateurs seront amenés à manipuler des appareils électroniques dans l'exercice de leur fonction. Par conséquent, et pour l'hygiène informatique de l'entreprise :

- il est interdit d'employer sur le réseau interne tout appareil électronique qui n'a pas été fourni à cet effet
- il est interdit de connecter sur tout appareil de l'entreprise un équipement venu de l'extérieur
- il est interdit de procéder à la connexion intermittente d'appareils nomades (exemples non exhaustifs : clefs USB, disques durs externes, smartphones, écouteurs à connexion numérique, vapoteuses, etc)

Pour respecter la confidentialité des informations, merci aussi de respecter les préconisations suivantes :

- ne pas utiliser votre terminal professionnel sur un réseau ouvert au public
- garder toujours en vue votre matériel informatique dans une poche fermée, même en espace fermé
- verrouiller votre session à chaque départ de l'écran, avec mot de passe ou identification biométrique activé
- utiliser, si un usage en public le demande, un filtre de confidentialité sur vos écrans

Usage des logiciels

Pour garder une sécurité du réseau suffisante, l'environnement logiciel doit être contrôlé. Aussi, les utilisateurs s'engagent :

- à utiliser un mot de passe unique et temporaire pour se connecter à la session répondant aux exigences minimales de sécurité (12 caractères alphanumérique sans répétition ni reprise partielle des anciens mots de passe)
- à utiliser le tunnel VPN par certificat fourni à son arrivée pour la connexion au réseau interne
- à utiliser des comptes de session enregistrés sur l'annuaire de l'entreprise (LDAP)
- à mettre à jour logiciels et poste de travail dès qu'une notification lui demande, toute affaire cessante
- à n'utiliser que les logiciels présents dans le catalogue applicatif interne (disponible via notre outil IT spécialisé)
- à ne pas utiliser de logiciels téléchargés/compilés depuis une source non approuvée
- à ne pas utiliser d'accès non vérifiés et non approuvés par la chaîne d'approbation (exemples non exhaustifs : clefs APIs, jetons de connexion, compte partagé, etc)
- à ne pas télécharger d'extensions de logiciels non approuvés ou ne venant pas des éditeurs officiels et/ou reconnus

Pour la bonne marche de l'entreprise, il peut être nécessaire d'utiliser des outils annexes. Aussi :

- chaque logiciel hors-catalogue devra faire l'objet d'une approbation préalable par vos supérieurs et le département IT en utilisant le formulaire aggréé

- les accès administrateurs ne seront dispensés que temporairement et sur demande au service IT

En cas de besoin

Merci de contacter le service IT en cas de doute ou de demande particulière.

Gestion des incidents

En cas d'incident, une ligne de communication d'urgence est à disposition :

- soit par le Portail accessible de l'extérieur avec authentification par mot de passe à usage unique envoyé sur le courriel personnel renseigné le jour de l'entrée dans les effectifs de l'entreprise
- soit par téléphone sur la ligne interne
- soit par téléphone sur un numéro international en cas de déplacement
- soit par messagerie privée WhatsApp pour être mis en relation avec un Chatbot redirectif

Mise en place interne

Le service IT se compose de différents canaux de communication :

- Chatbot WhatsApp pour la création de tickets (@Assistance_CybershieldIT)
- Adresse courriel pour la création directe de tickets (assistance@cybershield-it.fr)
- Hotline basée en France **8h-20h - 5j/7** (+33.(0)1.23.45.67.89)

Equipe de 4 personnes (1 SysAdmin, 2 Tech IT et 1 alternant/stagiaire pour 85 personnes au siège). Le SysAdmin ne prend pas d'appel téléphonique mais est d'astreinte soir et WE sur les tickets P1 par courriel.

Politique de sécurité technique

- annuaire LDAP (OpenLDAP ou Windows AD DS) avec mots de passe à changer tous les 3 mois, 12 caractères [A-Z0-9@-!]

Tests de mots de passe

Les 4 sont nuls.

Générer des mots de passe forts

Avec [Bitwarden Password Generator](#) :

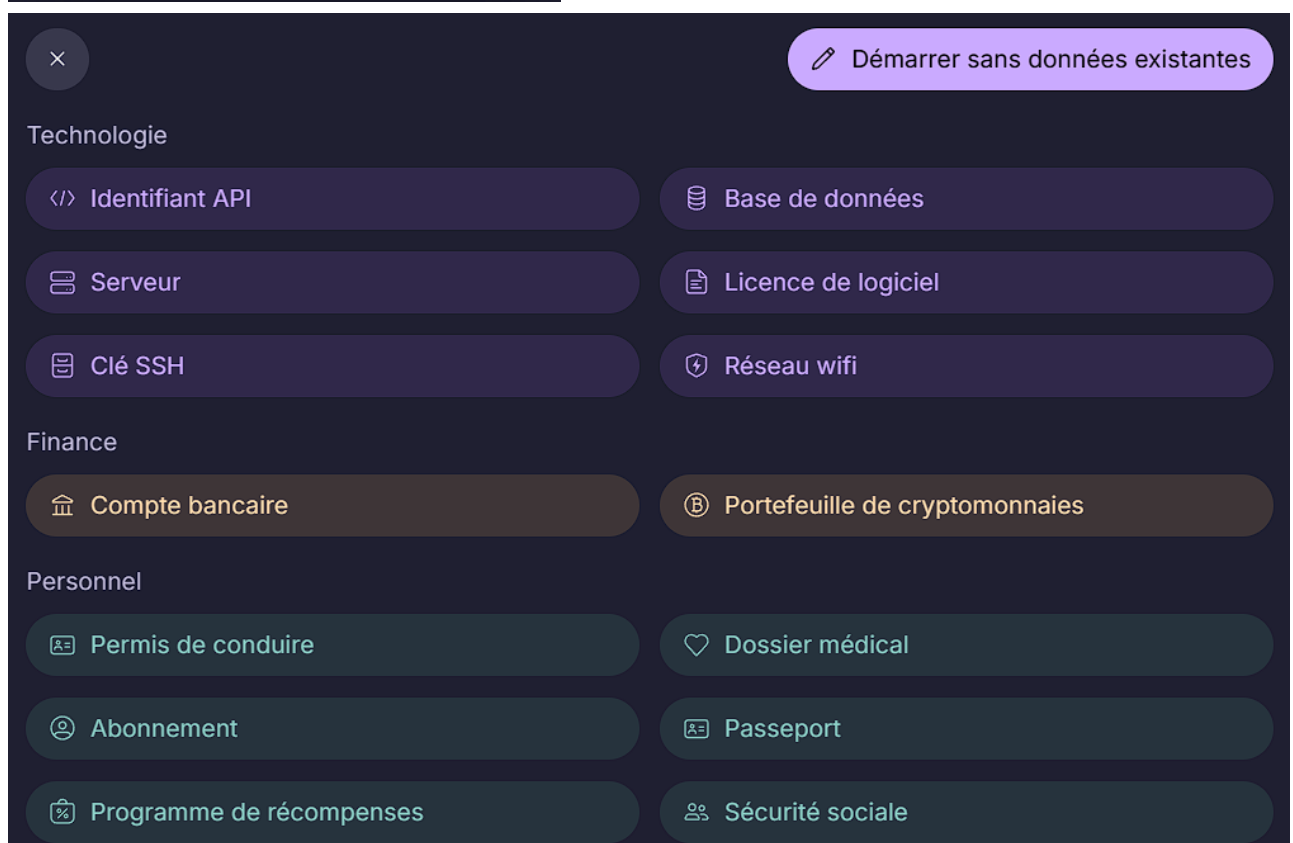
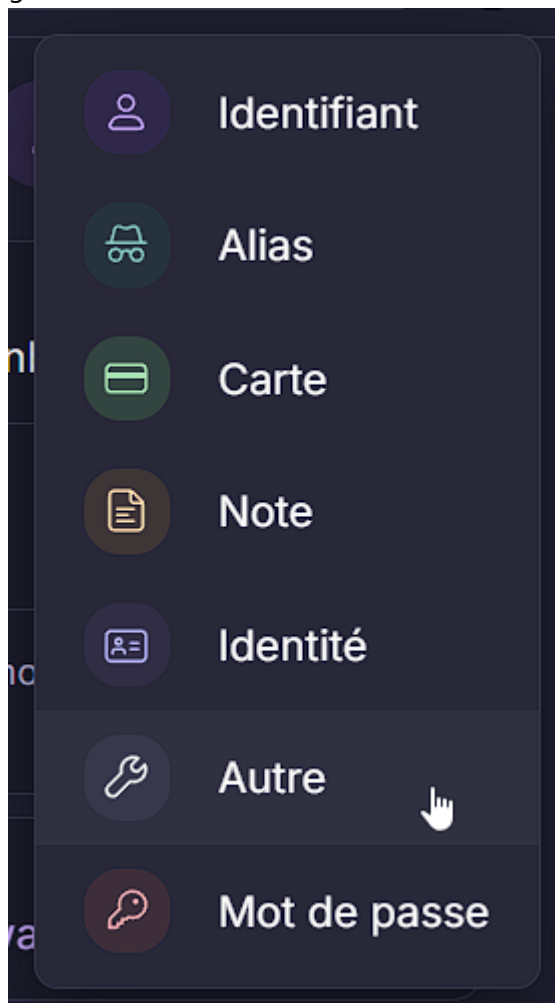
- eoHHt&5mT4QgAu7f
- 5%Gtg5c5DFSBUeyV
- C5hk#zV!TBAvSYFx
- jJGj26p\$ATff5Sdj

12 caractères, c'est devenu trop faible. 16 est le nouveau minimum.

Mon usage perso


J'utilise [ProtonPass](#), très utile, intégré avec le plan Proton Unlimited que j'ai :

- générateur de mots de passe forts
- gestionnaire d'accès, de clefs SSH, d'ID, de documents, champs personnalisés :



- intégration d'un moniteur "Dark Web" pour les fuites de mots de passe

- intégration de "SimpleLogin" créant des adresses courriel tampon, très pratique :

The image shows a dark-themed user interface for SimpleLogin. It features several input fields and buttons. The first field is labeled 'Titre' and contains 'bitwarden.com'. Below it is a button with a key icon and the text 'Vous êtes sur le point de créer bitwarden.com.companion24...'. The next field is labeled 'Préfixe' and contains 'bitwarden.com'. Below that is a field labeled 'Suffixe' containing '.companion240@8shield.net (Domain...' with a dropdown arrow. At the bottom is a field labeled 'Transfert vers' with an arrow icon and '@protonmail.com' with a dropdown arrow.

- Intégration 2FA
- Auto-remplissage intelligent (évite les champs "parasites") et auto-fermeture après 10 minutes (paramétrable)
- Application mobile + extensions navigateur pour un nomadisme total

Quand à éduquer les employés... j'ai essayé. Des années. Sans succès. Maintenant je laisse les gens pleurer sur leur sort en cas de piratage. Je suis pas "L'informatique du coeur".

Analyse des logs de sécurité

Logs fournis

```
192.168.1.100 - - [19/Mar/2025:14:45:32 +0000] "GET /admin HTTP/1.1" 403 500 "-"
"Mozilla/5.0"
192.168.1.101 - - [19/Mar/2025:14:45:33 +0000] "GET /login HTTP/1.1" 200 1200 "-"
"Mozilla/5.0"
192.168.1.102 - - [19/Mar/2025:14:45:35 +0000] "POST /login HTTP/1.1" 200 1500
"login_page" "Mozilla/5.0"
```

Ce qu'ils indiquent

Nous avons trois requêtes HTTP classiques : deux **GET** et un **POST**.

Le **GET** récupère l'information, **POST** la publie. A 3 secondes d'intervalle, c'est un bot automatique qui sonde le site (appelé en général "crawler", parce qu'il "rampe" sur le site) et essaye d'abord la page **/admin** puis **/login**.

On voit une erreur 403 (Accès refusé/interdit) sur **/admin** mais un code 200 (succès) sur **/login**, aussi tente-t-il de rentrer des informations de connexion (sans doute les mots de passe par défaut) pour voir quels sites sont exploitables.

Ce qu'il convient de faire

Le mieux est d'avoir un utilitaire type **fail2ban** qui va récupérer les IPs avec 5 tentatives échouées de connexion pour les bannir pendant 24 heures. Ici il s'agit d'une IP locale, donc soit c'est un test interne et on évite de bannir (sauf pour tester l'outil de bannissement), soit c'est un malin connecté en local et on bannit d'office.

En quoi est-ce important

Les logs c'est la séquence ADN de l'informatique : tout ce qui s'y trouve explique ce qui se passe et s'est passé. C'est essentiel pour retracer un historique et identifier des schémas d'action.

Comment les configurer

Le mieux c'est d'avoir un moniteur dédié (auto-hébergé comme un couple **Prometheus/Grafana**) ou prendre une solution clefs en main genre **Datadog**, et composer des moniteurs chargés de relever des alertes si une chaîne **REGEX** se déclenche trop souvent/en trop grande variation avec les périodes ordinaires.

Stratégie de sauvegarde

3-2-1

La plus connue, et pour de bonnes raisons.

- 3 sauvegardes différentes
- 2 supports différents
- 1 sauvegarde froide hors-site

Clair, net, précis.

Plan de Reprise après Sinistre

C'est long de faire un **PRS** (*DRP* en anglais) et ça a été suffisamment pénible en entreprise pour ne pas en refaire un fictif :3

Néanmoins, voici les grandes étapes :

1. Identifier les services critiques (P1)
2. Identifier les services non-critiques et les classer par criticité relative (P2, P3, P4)
3. Identifier la *pipeline* de production pour savoir quel flux est réalisé
4. Sauvegarder les services selon criticité

5. Avoir un plan de relance des services dans le bon ordre pour rétablir les services critiques en premier
6. Avoir un fournisseur de postes de travail ou de composants réactif (genre pour changer des disques durs en livraison 24h)

Les méthodes de sauvegarde

- En local sur un réseau séparé (simple disque partagé sur un VLAN)
- En local avec un logiciel dédié (**Datto**, **00drive**, **VEEAM**, etc)
- Dans le nuage avec des services intégrés (**OneDrive**, **iDrive**)
- Dans le nuage avec des services tiers (**ProtonDrive**, **IceDrive**, **pCloud**, **MEGA**, etc)
- Depuis un support externe (disque dur unique racheté chaque mois et stocké en armoire au domicile personnel du patron)

Les impacts d'une mauvaise sauvegarde

1. Perte de fichiers clients
 - clients mécontents
 - réputation qui baisse
 - faillite
 - crise, larmes, ~~suicide~~
2. Perte de facturation
 - clients et fournisseurs mécontents
 - justifications URSSAF perdues
 - redressement judiciaire
 - réputation en baisse
 - chômage, misère, déprime, bière en cannettes, jonglage devant un LIDL
3. Perte de matériel
 - chômage technique
 - délais de livraison étendus
 - réputation en baisse
 - perte de chiffre d'affaire
 - ~~Licenciements massifs~~ **Plan de Sauvegarde de l'Emploi**
 - Syndrome de l'imposteur, crise, détestation, fourches, torches, ~~guillotine~~

Incidents

Scénario

Une attaque par malware a compromis un serveur critique. Les employés signalent des ralentissements dans le système et des fichiers suspects.

Identification

Ralentissements ? Fichiers suspects ?

1. **Ransomware**
 - les ralentissements sont peut-être causés par le chiffrement des fichiers
 - l'apparition des "fichiers suspects" peut être la transformation des fichiers en leur contrepartie chiffrée

2. Mineur de cryptomonnaies

- les ralentissements sont peut-être causés par le hashage des cryptomonnaies
- les fichiers suspects... je ne l'explique pas dans ce contexte

Identifier en amont

1. Regarder les alertes des antivirus locaux ou des **EDR/WAF/SIEM** en place
2. Regarder les processus anormaux en tâche de fond
3. Récupérer des fichiers infectés et les faire tourner en environnement bac à sable
4. Etudier les logs pour obtenir des adresses IP, des noms de fichier, etc
5. J'ai lu une fois qu'on pouvait retracer l'identité du virus en calculant l'empreinte hachée d'un fichier infecté (à tester)

Contention

1. Isoler les postes infectés (déconnexion physique, mais les laisser tourner !)
2. Isoler les serveurs infectés (déconnecter les câbles physiques, mais encore une fois, les laisser tourner !)
3. Analyser les journaux du système et du pare-feu

Récupération

1. S'assurer d'avoir purgé les postes de l'infection
2. Vérifier les temps des sauvegardes et en prendre une "propre"
3. Si doute, changer les disques durs et réinstaller selon le **PRS** (*DRP*)

Post-Mortem

1. Etablir la ligne temporelle de l'attaque
 1. Cause principale
 2. Les services infectés
 3. L'arrêt de l'attaque et le début de la restauration
2. Récupération
 1. Suivi du PRS
 2. État des services récupérés
3. Les actions à prendre pour éviter une récurrence

Les outils pour analyser un incident

- un **SIEM** (*Security Information and Event Manager*) => personnellement j'utilise Wazuh, qui fait SIEM et XDR en une instance, en open-source et auto-hébergé.
- un outil **Forensic** => je lis qu'on peut utiliser **Forensic** et **Autopsy**, pour analyser respectivement la RAM (c'est pour ça qu'on n'éteint pas les machines infectées tout de suite !) et les Disques Durs.
- un analyseur réseau => **Wireshark** s'il tourne en fond au moment de l'attaque, ou si on le laisse tourner sur un PC infecté pour vérifier les paquets en (tentative de) transmission.