Février 2023 - Août 2023

Projet Network

Miracle (by jedha)

INvestigations POST-ACCIDENT

Rayan Benhamana

# **Sommaire**

[**Sommaire** 1](#_Toc147280819)

[**Introduction** 2](#_Toc147280820)

[Contexte 2](#_Toc147280821)

[Objectifs 2](#_Toc147280822)

[Ressources Mobilisables 2](#_Toc147280823)

[**Phase de reconnaissance** 3](#_Toc147280824)

[Historique 3](#_Toc147280825)

[Environnement 3](#_Toc147280826)

[Analyse du jeu installé 4](#_Toc147280827)

[**Risques encourus : Analyse des fichiers malveillants** 5](#_Toc147280828)

[ComicSans.ttf 5](#_Toc147280829)

[AriaBold.ttf 6](#_Toc147280830)

[**Attaque subie : Analyse du réseau** 7](#_Toc147280831)

[Analyse des interfaces réseaux 7](#_Toc147280832)

[Analyse du trafic réseau 7](#_Toc147280833)

[Analyse des données extraites 9](#_Toc147280834)

[**Conclusion** 10](#_Toc147280835)

[Réponses aux objectifs 10](#_Toc147280836)

[Aller plus loin 13](#_Toc147280837)

[Résumé 14](#_Toc147280838)

# **Introduction**

## Contexte

Miracle est une entreprise de services informatique reconnue pour la sécurité de ses produits et services. Elle compte parmi ses produits un logiciel nommé « TransX ». Ce logiciel permet de traiter les données des entreprises clientes afin de les aider à prendre des décisions stratégiques. La grande majorité des clients de l’entreprise Miracle sont des multinationales dont certaines font parties du CAC40. Le logiciel « TransX » doit donc être extrêmement sécurisé car il accède et traite des données clientes très sensibles. D’autant plus que le produit est aussi bien utilisé par les Directions, que par les services de Ressources Humaines, de Comptabilité ou de Communication.

La célèbre société informatique pense avoir subi une attaque informatique et a besoin d'une équipe experte en réseaux pour analyser leur réseau. Ce réseau est utilisé pour développer et déployer le produit « TransX », et est composé de postes de travail Linux. Le Centre des Opérations de Sécurité interne à Miracle a détecté des indices de compromission sur leur réseau privé. Le problème est que l’un des postes de travail semble faire des requêtes suspectes permettant d’automatiser le transport et le chiffrement de données.

## Objectifs

Miracle a fait appel à une équipe d’experts en cybersécurité afin de mieux comprendre l’accident s’étant produit. L’entreprise souhaite limiter les conséquences de cette attaque, et si possible apporter une solution à la situation actuelle.

Les objectifs de cette investigation réseau sont multiples et progressifs, il faut :

1. Trouver la source de l’accident
2. Analyser le comportement de l’attaque
3. Identifier une potentielle fuite de données ou perte de données
4. Apporter une solution à mettre en place par la Direction des Services Informatiques de Miracle

Le déroulé du projet, ainsi que les résultats de l’investigation sont présentés dans le rapport. En autres le trafic réseau est disponible sous format .pcap, et les fichiers malveillants sont accessibles en clair.

## Ressources Mobilisables

Le Centre des Opérations de Sécurité suspecte le poste de travail 10.10.2.16 d’avoir un comportement malveillant. Un compte utilisateur est disponible sur ce poste de travail et est accessible avec les identifiants suivants :

**Nom d’utilisateur :** tserge  
 **Mot de passe :** Miracle2022

La commande suivante permet de se connecter au serveur :

$ ssh tserge@10.10.2.16

Avant de commencer les investigations, Miracle a fourni quelques indications techniques pour le bon déroulement du projet. Par exemple l’utilisation de sudo est autorisée. De plus, Miracle conseille d’analyser le trafic réseau du poste de travail avec tcpdump.

# **Phase de reconnaissance**

Les requêtes suspectes identifiées par Miracle peuvent être la source de l’attaque ou une conséquence directe de celle-ci. Il est donc important de prendre du recul, d’étudier tout l’environnement de travail et de ne pas uniquement se concentrer sur le trafic réseau.

## Historique

Dans un premier temps, il est intéressant de consulter l’historique des commandes pour retrouver les dernières exécutées. Si un attaquant s’est connecté au poste de travail pour y exécuter des commandes, alors elles sont probablement conservées dans l’historique.

Une image contenant texte, Police, capture d’écran

Description générée automatiquementUne image contenant texte, capture d’écran, Police

Description générée automatiquement

Après consultation le fichier .bash\_history ne contient pas d’informations suspectes, cependant le fichier .history semble contenir un premier indice. En effet, une commande curl permettant de télécharger une ressource disponible à l’adresse 10.10.11.6 a été exécutée. **Il est probable que le logiciel malveillant identifié dans la suite du rapport soit issu de ce téléchargement.**

## Environnement

Dans un second temps, le dossier utilisateur a été exploré afin d’obtenir des indices complémentaires sur l’attaque ayant eu lieu. Une cartographie de l’environnement de travail a pu être dressée.

Une image contenant texte, diagramme, capture d’écran, Parallèle

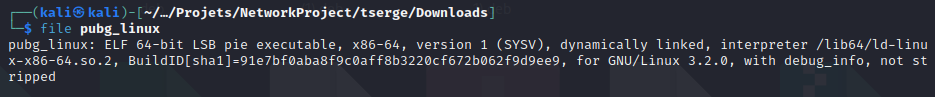
Description générée automatiquement

En vue de la précédente découverte, le dossier Download est intéressant car il contient les fichiers téléchargés par l’utilisateur. Le premier fichier COMPANIES\_IBAN.csv peut être considéré comme une donnée sensible mais est très probablement interne à l’entreprise. Ce fichier ne semble pas avoir été impliqué dans l’attaque et est disponible en annexes.

## Analyse du jeu installé

En revanche le second fichier pubg\_linux également disponible en annexes est plus suspect. **En effet quelques recherches sur internet ont permis de comprendre que pubg est un jeu mobile.** Il est possible que l’utilisateur ait téléchargé le jeu sur son poste de travail intentionnellement. Et il est intéressant d’analyser un peu plus en détails cette application pubg\_linux.

Les métadonnées de l’exécutable peuvent être récupérées à l’aide d’une simple commande file.



Les résultats confirment qu’il s’agit effectivement d’un exécutable ELF, et qu’il n’est pas obfusqué. Ensuite la commande strings permet de recueillir plus de détails sur le fonctionnement de cet exécutable. Toutefois, le résultat de cette commande renvoie beaucoup trop d’informations. Le premier élément à déterminer est si cet exécutable échange avec un serveur externe. Par conséquent, la commande est filtrée avec le mot-clé « http:// » suivi d’une regex permettant de prendre en compte toutes les adresses IPv4 existantes.

**1**

**2**

Une image contenant texte, capture d’écran, Police, Bleu électrique

Description générée automatiquement

L’analyse de l’exécutable permet de déterminer que pubg\_linux effectue notamment deux actions :

1. Il télécharge un fichier de police ComicSans.ttf depuis le port 110 du serveur externe 10.10.2.200
2. Il exécute le fichier de police ComicSans.ttf sur le serveur ciblé

Il est suspect qu’un fichier de police soit exécuté, il est donc très probable qu’il s’agisse d’un fichier malveillant déguisé. Par conséquent, le serveur externe peut être comparé à un serveur Commande & Control (C2C).

Le chemin d’accès au fichier ComicSans.ttf peut être retrouvé dans la seconde commande. Le fichier est situé dans le dossier /usr/share/fonts/truetype. L’inspection de ce dossier permet de compléter la cartographie existante de l’environnement de travail. Le dossier contient deux fichiers distincts : ComicSans.ttf et AriaBold.ttf. Le fichier ComicSans.ttf est suspect, mais le fichier AriaBold.ttf semble similaire au premier fichier. D’autant plus que ces deux fichiers de police sont codés en base 64.L’analyse de ces deux fichiers dans la prochaine partie permet de comprendre l’attaque ayant eu lieu.

# **Risques encourus : Analyse des fichiers malveillants**

La partie précédente a permis de comprendre qu’un faux logiciel de jeux mobile a été téléchargé par l’utilisateur. Lorsqu’il a essayé d’y jouer, un fichier malveillant a été secrètement téléchargé sur le poste de travail depuis un serveur malveillant. Un second fichier similaire au premier semble également avoir été téléchargé.

Une fois le vecteur d’attaque identifié, la suite est d’étudier l’attaque plus en détails. L’analyse des fichiers ComicSans.ttf et AriaBold.ttf serait intéressante. L’utilitaire base64 est utilisé pour les décoder. Les deux fichiers malveillants décodés sont disponibles en annexes.

## ComicSans.ttf

Le premier fichier malveillant ComicSans.ttf commence par établir une persistance en se téléchargeant lui-même chaque minute, puis télécharge le fichier AriaBold.ttf sur le poste de travail. L’exécution du fichier se termine par la détection et l’extraction de données sensibles définies au préalable.

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

Ce fichier est décomposé en 4 étapes possédant chacune une fonction associée au sein de ComicSans.ttf :

* **La fonction persist** : Une tâche est inscrite au sein de la crontab, elle permet de télécharger et d’exécuter le fichier ComicSans.ttf. La persistance de l’attaque repose sur l’automatisation discrète de cette tâche répétée chaque minute.
* **La fonction stage1** : Cette fonction télécharge le fichier ComicSans.ttf depuis le serveur malveillant
* **La fonction stage2** : Cette fonction télécharge le fichier AriaBold.ttf depuis le serveur malveillant
* **La fonction stealer** : Une liste de fichiers sensibles est recherchée sur le serveur ciblé et les fichiers retrouvés sont exfiltrés vers un serveur malveillant. Les fichiers sensibles sont passwd, crontab, shadow et sshd\_config.

L'utilisation d'un tel script pose de sérieux problèmes de sécurité car il implique des activités malveillantes potentielles telles que l'exfiltration de données et l'exécution non autorisée de commandes.

Son objectif est d’assurer le bon déroulement de l’attaque et d’effectuer un premier niveau de reconnaissance pour l’attaquant. Ce code permet entre autres d'exfiltrer les données et d'exécuter des commandes non autorisées. Les données ainsi exfiltrées seront détaillées dans la prochaine partie du rapport.

## AriaBold.ttf

Le second fichier malveillant AriaBold.ttf a deux missions principales : chiffrer tous les fichiers compris dans le dossier /home, puis les extraire. Les données sont chiffrées à l’aide de l’algorithme DES en mode ECB. De plus, la clé de chiffrement est étonnamment faible : ‘11111111’. Il est clair que l’objectif de l’attaque n’est pas de rançonner Miracle.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Le chiffrement DES est l’ancêtre du chiffrement AES, et a depuis été reconnu comme vulnérable. Il s’agit d’un chiffrement symétrique par blocs, par conséquent la clé identifiée sert à chiffrer et déchiffrer les données. De plus, le mode ECB permet de spécifier plus précisément la méthode de chiffrement mais la rend encore plus vulnérable. En effet, chaque bloc de données est chiffré de la même manière sans vecteur d’initialisation.

Finalement les fichiers chiffrés sont envoyés vers le serveur malveillant de l’attaquant.

# **Attaque subie : Analyse du réseau**

Après la phase de reconnaissance de l’environnement, il est important d’analyser également le réseau. Les requêtes enregistrées permettent de vérifier si les risques identifiés précédemment ont été exploités. Il est intéressant de relier ces requêtes aux actions effectuées par les fichiers malveillants analysés à l’étape précédente.

En effet, la lecture du code permet de comprendre les potentielles conséquences de l’attaque. Tandis que l’analyse du réseau permet de confirmer les réels dégâts subis lors de l’attaque. Dans certains cas, l’attaque prévue initialement ne s’exécute pas totalement.

## Analyse des interfaces réseaux

L’analyse réseau commence par un scan des ports ouverts et des interfaces réseaux actifs. Une interface réseau suspecte ou un port ouvert inattendu pourraient être des indices de compromission.

Le scan de port effectué permet de conclure que seul le port lié au service SSH est disponible. Aucun autre port n’est ouvert. Les interfaces du poste de travail sont à leur tour identifiées à l’aide de tcpdump.

Une image contenant texte, capture d’écran, Police

Description générée automatiquementUne image contenant texte, capture d’écran, Police

Description générée automatiquement

Après l’analyse des interfaces et des ports, il semble qu’aucune trace de l’attaque n’y soit visible. Il est donc très probable que l’attaquant n’ait pas agit au niveau réseau et que ses actions soit facilement visibles sur le réseau.

## Analyse du trafic réseau

L’analyse des requêtes transitant sur le réseau est primordiale pour suivre l’évolution de l’attaque. Une contrainte du poste de travail étudié est l’absence de l’outil WireShark pour analyser le trafic réseau. Toutefois, l’utilitaire tcpdump présent sur le poste de travail permet de récupérer les requêtes.

Une image contenant texte, capture d’écran

Description générée automatiquement

Les résultats affichés par tcpdump sont difficilement analysables. Néanmoins, il est possible d’extraire les résultats dans un fichier .pcap afin de l’ouvrir avec WireShark. Le nombre de requêtes récupérées dépend de la durée d’exécution de la commande tcpdump.

Toutefois, la commande a été exécutée assez longtemps lors de l’audit pour pouvoir récupérer toutes les requêtes liées à l’attaque. Le fichier .pcap contenant le trafic réseau étudié est disponible en annexes.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

**L’analyse du trafic réseau fait ressortir quelques requêtes suspectes utilisant les protocoles POP et POP/IMF.** Pour rappel, SMTP (Simple Mail Transfer Protocol) est le protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique. Tandis que POP (Post Office Protocol) est le protocole qui permet de récupérer ces courriers électroniques. Autrement dit le protocole POP assure le chemin inverse au protocole SMTP, et sont souvent utilisés de manière complémentaire. En revanche,IMF (Internet Message Format) fait référence au format dans lequel les messages textuels sont transférés au sein d’internet. Le format IMF est souvent lié aux protocoles e-mails.

Chaque communication est fragmentée en plusieurs requêtes distinctes. La communication est plus lisible quand elle est affichée de bout en bout. **Des communications malveillantes sont identifiées et elles impliquent le serveur C2C ayant pour adresse 10.10.2.200** comme conclu précédemment.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquementLa première (resp. la seconde) communication avec le serveur malveillant permet à l’attaquant de télécharger le fichier de police malveillant « ComicSans.ttf » (resp. « AriaBold.ttf ») sur le poste de travail victime. Le contenu de ces fichiers malveillants sont codés en base 64, il suffit donc de les décoder pour analyser les codes qui ont été exécutés.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Ces requêtes ont été exécutées avec succès comme le prouve le code HTTP 200. D’ailleurs la requête permettant de télécharger le fichier « ComicSans.ttf » est répétée plusieurs fois. Par la suite d’autres communications malveillantes sont identifiées, et elles consistent chacune en une extraction de données.

## Analyse des données extraites

L’extraction des fichiers détectés par « ComicSans.ttf » est visible dans les communications réseaux. Par conséquent, il est possible d’affirmer que le premier fichier malveillant a été exécuté et que certaines données sensibles ont fuité. Ces données systèmes peuvent être utilisés ensuite pour préparer une seconde attaque plus conséquente.

1. **Le fichier /etc/passwd**

Il liste les informations des utilisateurs ayant un accès sur le poste de travail. Chaque ligne correspond à un utilisateur et est construite de la manière suivante :

*nom : mdp : userID : groupID : commentaire : dossier personnel : programme de démarrage*

Une image contenant capture d’écran, texte

Description générée automatiquementLe point positif est que l’extraction de ce fichier aurait pu être plus critique. Toutefois, le poste de travail est bien configuré car le mot de passe est remplacé par un x, et son hash est stocké dans le fichier /etc/shadow.

Une image contenant capture d’écran, texte

Description générée automatiquement

**2) Le fichier /etc/shadow**

Ce fichier est une évolution historique du fichier /etc/passwd afin d’offrir une manière plus sécurisée de stocker les informations utilisateurs dont le mot de passe. L’extraction de ce fichier n’a pas été retrouvée sur le réseau, toutefois il est certain que le fichier « ComicSans.ttf » a été exécuté. Il est donc très probable que ce fichier ait également été extrait, ou qu’il n’existe pas.

Ce fichier est construit de la même manière que le fichier /etc/passwd, toutefois le format des lignes est modifié :

*nom : hash : dernière date de MàJ : jours min : jours max : période d’avertissement : délai de désactivation : date de désactivation : flag*

**3) Le fichier /etc/crontab :**

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquementCe fichier est moins sensible que les autres. En effet, l’attaquant peut simplement consulter les tâches s’exécutant à intervalles régulières sur le poste de travail victime. Toutefois, cela permet à l’attaquant de vérifier que la crontab a été correctement modifiée pour rendre l’attaque persistante.

**4) Le fichier /etc/ssh/sshd\_config.**

Ce fichierpermet de configurer le service OpenSSH gérant l’authentification des connexions SSH.A l’aide de ce fichier, l’attaquant pourrait analyser la configuration du serveur OpenSSH afin de détecter une mauvaise configuration à exploiter ou alors retrouver une liste des clés autorisées. Par conséquent, les risques liés à la seule extraction de ce fichier n’est pas obligatoirement critique. Toutefois, il faut surveiller que le fichier contenant la liste des clés ssh autorisées ne soit pas également extrait.

Une image contenant texte, capture d’écran, Parallèle, conception

Description générée automatiquement

Les indices de compromission permettent d’affirmer que le fichier malveillant « ComicSans.ttf » a été exécuté. Néanmoins, l’exécution du second fichier « AriaBold.ttf » aurait représenté un plus gros danger pour Miracle.

Heureusement pour Miracle aucune trace de l’extraction du dossier /home ou l’exécution du fichier n’ont été trouvées. Il est très probable que le pire ait été évité pour Miracle, mais il est impossible de l’affirmer. Par conséquent, il est important que Miracle émette l’hypothèse que le dossier /home ait été extrait. Il faut lister les données sensibles présentes dans ce dossier afin d’agir en conséquence.

# **Conclusion**

Pour conclure, le rapport revient sur l’atteinte des objectifs avant de de présenter d’autres vulnérabilités rencontrées lors des investigations puis de proposer un court résumé du projet. Les remédiations à apporter au réseau afin de supprimer toute trace de l’attaque et en limiter les impacts sont présentées dans les réponses aux objectifs.

## Réponses aux objectifs

Les résultats obtenus lors des investigations permet d’affirmer que les objectifs du projet ont été remplis. Une réponse détaillée pour chaque objectif est proposée ci-dessous.

1. **De quels processus/fichiers émanent les requêtes malveillantes ?**

Dans un premier temps, une unique requête a été initiée par l’exécution d’un faux jeu mobile « pubg\_linux » par l’utilisateur. Le résultat de la requête est le téléchargement de deux fichiers malveillants. Le premier fichier téléchargé « ComciSans.ttf » est responsable des requêtes malveillantes enregistrées. Le second fichier malveillant devrait envoyer des requêtes, toutefois il ne semble pas avoir été exécuté lors de l’attaque.

Le serveur C2C utilisé par l’acteur malveillant a pour adresse 10.10.2.200, et les données sont envoyées sur le port 110.

1. **Que fait le logiciel malveillant ? Comment l’attaque s’est-elle déroulée ?**

Après analyse, il apparait que le logiciel malveillant pubg\_linux imite un célèbre jeu mobile. Il est très probable que l’utilisateur tserge ait été trompé et qu’il pensait simplement télécharger un jeu mobile. Néanmoins, lorsque le logiciel a été exécuté, un fichier malveillant a été téléchargé et exécuté sur le poste de travail depuis le port 110 du serveur 10.10.2.200.

Le rôle de ce fichier malveillant ComicSans.ttf est d’établir une persistance de l’attaque en inscrivant une nouvelle tâche dans la crontab. Cette tâche s’exécute chaque minute, et consiste à télécharger de nouveau le fichier ComicSans.ttf puis l’exécuter. Par conséquent, la persistance de l’attaque est améliorée car même si les fichiers malveillants sont supprimés, l’attaque se répètera chaque minute si la tâche crontab n’est pas supprimée. Ensuite, l’exécution de ce fichier permet à nouveau de télécharger ce même fichier malveillant ComicSans.ttf, ainsi qu’un second fichier malveillant AriaBold.ttf. Ensuite, la dernière action effectuée par ce fichier est l’identification de 4 fichiers sensibles prédéfinies sur le poste de travail victime avant de les extraire.

Le second fichier malveillant AriaBold.ttf est plus simple à analyser mais a un comportement plus compromettant. En effet son rôle est de chiffrer et envoyer au serveur malveillant le dossier /home et tous ses sous-dossiers. Néanmoins, l’analyse du trafic réseau laisse penser que le dernier fichier AriaBold.ttf n’ait pas été exécuté.

1. **Des fichiers ou données ont-ils été volés/chiffrés/supprimés ? Et si oui lesquels ?**

L’étude a permis de déterminer l’objectif de l’attaque consistant à extraire certaines données systèmes et un maximum de données métiers. En effet, l’attaque fait intervenir deux fichiers malveillants distincts devant chacun récupérer des données de nature différentes.

Le premier fichier malveillant « ComicSans.ttf » détecte la présence de quatre fichiers différents permettant de configurer le système. Puis ces fichiers sont exfiltrés vers le serveur malveillant contrôlé par l’attaquant. La liste de ces fichiers est :

1. /etc/crontab
2. /etc/ssh/sshd\_config
3. /etc/passwd

Le second fichier malveillant AriaBold.ttf ne semble pas non plus avoir été exécuté. En effet, il est sensé chiffrer et extraire tous les fichiers contenus dans /home et ses sous-dossiers. Toutefois, aucune trace de l’extraction de ces données n’a été retrouvée lors de l’investigation réseau. L’attaque aurait pu être plus dommageable pour Miracle si AriaBold.ttf avait rempli son rôle.

1. **Procédure pour remédier à l’attaque à l’intention des administrateurs systèmes de Miracle**

La compréhension de l’attaque ayant eu lieu sur le réseau de Miracle a permis de déterminer les actions à entreprendre pour s’en protéger. Les recommandations données ci-dessous permettent d’arrêter l’attaque, d’en limiter les conséquences et de se protéger contre une future attaque similaire. Toutefois, le mode opératoire n’est pas exhaustif et ne garantit pas la sécurité absolue du système informatique de Miracle.

Arrêter l’attaque :

La priorité est d’arrêter l’attaque en cours. En effet, il est dangereux que le poste de travail continue à communiquer avec le serveur malveillant. Le contenu du fichier malveillant « ComicSans.ttf » peut très bien être modifié au cours de l’attaque, afin d’aboutir à une seconde attaque.

Un mode opératoire composé de 5 actions permet d’arrêter l’attaque le plus rapidement possible :

1. Bloquer les communications du poste de travail, et plus particulièrement celles faisant intervenir le serveur malveillant 10.10.2.200

iptables -A INPUT -s 10.10.2.200 -j DROP

iptables -A OUTPUT -d 10.10.2.200 -j DROP

1. Supprimer manuellement la tâche ajoutée dans la crontab afin de supprimer la persistance de l’attaque, et s’assurer qu’elle ne se déploie pas à nouveau
2. Retrouver et arrêter les processus correspondant à l’exécution des deux programmes « ComicSans.ttf » et « AriaBold.ttf »

ps aux | grep ComicSans.ttf

ps aux | grep AriaBold.ttf

kill -9 ${PID}

1. Supprimer les fichiers malveillants « ComicSans.ttf » et « Ariabold.ttf »

rm /usr/share/fonts/truetype/\*

1. Supprimer l’exécutable malveillant « pubg\_linux » du poste de travail

rm /home/tserge/Download/pubg\_linux

Limiter les impacts :

L’objectif secondaire après les investigations est de limiter les conséquences de l’attaque s’étant produit. Trois chantiers listés ci-dessous permettent de cadrer les risques à venir.

1. Etudier en profondeur les données récupérées par l’attaquant afin de prévoir et cadrer les risques
2. Changer tous les mots de passe et clés présents dans les fichiers récupérés par l’attaquant
3. Vérifier tous les postes de travail accessibles par un utilisateur dont les informations ont fuité.

Mesures de préventions

L’important est que Miracle puisse apprendre de ses erreurs, et puisse se prémunir contre une nouvelle attaque de ce type. Ces actions sont plus long-terme mais restent indispensables pour cadrer l’élément le plus vulnérable de l’entreprise : l’humain. Par conséquent plus qu’une solution technique, il faut apporter des solutions organisationnelles comme :

1. Mettre en place une politique d’utilisation du matériel professionnel
2. Mettre en place une politique de gestion des données sensibles
3. Mettre en place une politique de mots de passe forts
4. Sensibiliser les employés Miracle sur les risques de cybersécurité

La sensibilisation auprès des collaborateurs est importante pour qu’ils comprennent les enjeux d’une attaque, et qu’ils adoptent les bonnes pratiques. Des règles et des réflexes très simples auraient éviter à Miracle de subir cette attaque. Par exemple, les téléchargements doivent uniquement être effectués depuis des sources de confiance. Et l’ordinateur professionnelle ne doit pas être utilisé pour des activités personnelles.

Finalement une solution technique aurait pu être ajoutée pour mieux contrôler le trafic réseau. En effet, la mise en place d’un pare-feu efficace aurait empêché une telle attaque de se produire.

## Aller plus loin

Un projet sensible mais vulnérable à une attaque a pu être retrouvé sur le poste de travail au cours des investigations. Il s’agit d’une archive .7z protégée par un mot de passe, probablement parce qu’elle contient des données sensibles. Une première tentative d’attaque par force brute a permis de mettre en évidence la faiblesse du mot de passe. Dans un premier temps, il suffit de créer le hash correspondant à l’archive compressée et chiffrée à l’aide de l’outil 7z2john. Finalement, le hash ainsi créé est déchiffré avec l’utilitaire John The Ripper.

**1**

python 7z2john.py file.7z > main\_branch.hash

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

**2**

Une image contenant texte, capture d’écran, jaune, Rectangle

Description générée automatiquementLe mot de passe de l’archive est « jonasbrothers ». Il est donc aisé d’utiliser ce mot de passe pour décompresser l’archive et accéder au projet. Le projet est un programme très important permettant de monitorer la température au sein d’un réacteur nucléaire.

Il s’agit probablement d’une application métier commandée par une entreprise cliente. L’extraction de ce code ne représente pas un risque direct pour l’entreprise Miracle. Toutefois, une étude de ce code par un acteur malveillant peut se conclure par l’attaque d’un site nucléaire. Une telle attaque serait extrêmement critique d’abord pour la société civile, mais aussi pour Miracle qui subiraient des répercussions économiques et médiatiques.

## Résumé

Miracle a subi une attaque à la suite d’un téléchargement de jeu mobile par un employé. Un fichier malveillant se télécharge toutes les minutes automatiquement et extrait des données systèmes. Finalement un second fichier malveillant permettant de récupérer tout le dosser utilisateur est téléchargé. Toutefois, les fichiers sont récupérés dynamiquement depuis un serveur externe. Il est donc possible que l’attaquant exploite les informations extraites pour ajuster l’attaque et modifier le contenu des fichiers. Heureusement pour Miracle, le second fichier ne semble pas être exécuté.

Les informations systèmes ainsi récupérées pourraient servir à compromettre le réseau privé de Miracle, et les informations clients sont tout aussi critiques. En effet les détails bancaires des clients sont disponibles sur le poste de travail. De plus, certaines applications sensibles développées pour les clients auraient pu fuiter. Une de ces applications permet de monitorer la température du réacteur nucléaire, et l’analyse du code source peut être dangereux si une vulnérabilité est trouvée.

Les répercussions pour Miracle auraient pu être terribles. Pour commencer la compromission de son serveur et l’arrêt de son activité auraient représenter un manque à gagner important pour Miracle ainsi qu’un coût de nettoyage conséquent. D’autant plus qu’en cas d’espionnage industriel Miracle perd son avantage concurrentiel. Finalement la plus grosse répercussion pour Miracle se situe dans sa relation avec ses clients. En effet, l’entreprise est sensée être experte en informatique, et une faille dans ses réseaux pourraient rendre ses clients sceptiques. Son image de marque de confiance serait endommagée mais les clients dont les données ont fuité auraient pu poursuivre en justice Miracle.