SisID alcyconie

LE GRAND HACK DE NOËL

Récit d'une cyberattaque sophistiquée mêlant fraudes et ingénierie sociale. Bonnes pratiques pour gérer la crise et communiquer efficacement.

LE GRAND HACK DE NOËL

Il était une fois un flocon de neige virevoltant un beau jour de décembre.
Ce n'était pas un flocon comme les autres car il abritait la petite commune de Noëlcity et les ateliers du Père Noël. Les habitants, lutins et rennes y vivaient dans la joie et la bonne humeur et attendaient chaque année avec impatience la période de Noël.

À l'écart de toutes les habitations, une colline surplombait Noëlcity.
Sur cette colline vivait le Grinch et son fidèle acolyte Max. Contrairement aux habitants de Noëlcity, cet abominable personnage vert et poilu haïssait Noël.
Et cette année était l'année de trop.

Son objectif ? Hacker Noël !

Le Grinch

Max

Le Père-Noël

La Mère-Noël

Lutin

01 CHAPITRE 1 : LE GRINCH HACKE NOËL

METTRE FIN À NOËL N'EST PAS CHOSE FACILE, SURTOUT LORSQUE L'ON VIT À NOËLCITY.

Noël est la fête la plus attendue et la plus sécurisée de toutes. Un véritable challenge pour le Grinch qui veut à tout prix empêcher Noël d'avoir lieu. Il décide de mettre en place une cyberattaque d'une envergure inédite. Mais par où commencer ?

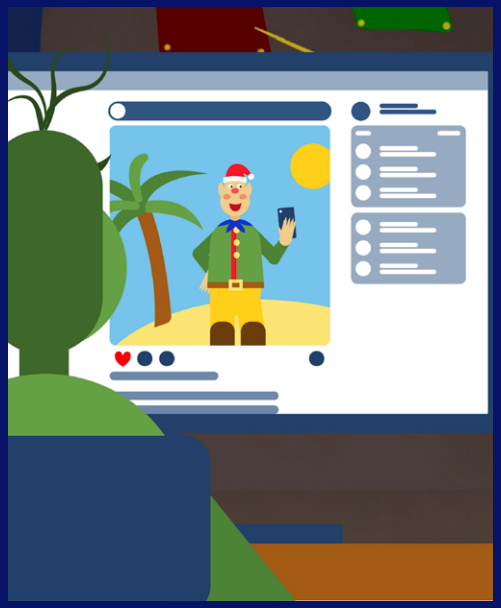
Le Grinch choisit de s'attaquer directement au Père Noël pour détourner tous les cadeaux. Une phase importante de recherche d'informations démarre : avec une telle cible, il sait que ce ne sera pas une mince affaire mais l'objectif final en vaut la peine.

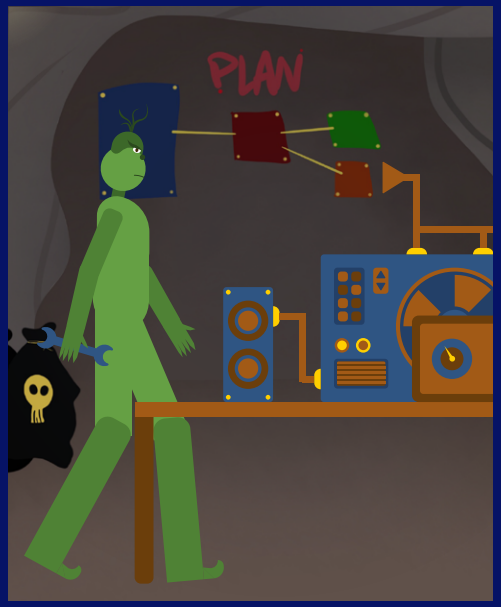
La première étape est d'enquêter sur le fonctionnement de l'atelier du Père Noël. Le but étant de cartographier l'entreprise et d'établir un organigramme des lutins salariés occupant des postes stratégiques. Ensuite, il lui faut découvrir la nature des relations entre eux ainsi que leurs périodes de congés.

Les recherches bien entamées, le Grinch et Max décident de mettre en place plusieurs cyberattaques. Les méthodes existantes sont nombreuses, ils ont l'embarras du choix : ransomware, phishing, usurpation d'identité, fraude bancaire...

Le choix se porte sur une attaque par hameçonnage (phishing) à l'encontre de certains lutins afin de s'introduire dans le système informatique de l'usine. Ensuite une fraude au faux lutin pour détourner toute la chaine d'approvisionnement et enfin une fraude au Père Noël.

02 CHAPITRE 2 : LES PREPARATIFS DU GRAND HACK





LE GRINCH A BIEN AVANCÉ DANS SES RECHERCHES ET S'ATTÈLE À LA PRÉPARATION DES ATTAQUES

Tout d'abord, le phishing. Grâce aux informations qu'il a trouvées, il sait que les lutins adorent les bonbons. Il rédige alors l'email suivant :

« Objet : OFFRE EXCEPTIONNELLE – VOUS AVEZ ÉTÉ SELECTIONNÉ POUR UNE DISTRIBUTION PRIVÉE DE GIMAUVES ! »

Cette année le Père Noël a décidé de récompenser les lutins les plus impliqués dans leur travail par leur poids en bonbons. Pour bénéficier de ce cadeau, inscrivez-vous en cliquant sur le lien suivant : Xmasrewards.noelcity.com ».

Pour ne pas éveiller les soupçons, il l'envoie à des lutins de services différents et maximise ses chances d'infiltrer le système. Max lui rappelle alors que les guimauves sont également le péché mignon de la Mère Noël. Pourquoi ne pas lui envoyer l'email de phishing ?

L'email rédigé, il lui reste à préparer un malware qui lui permettra de s'introduire dans le système informatique de ses cibles. Si le Grinch est familier de l'informatique, il n'en est pas un expert. Il contacte alors un black hat hacker qui négocie 5% des cadeaux pour le lui créer. Quelques jours plus tard, le hacker lui renvoie le produit fini, la première attaque est prête à être lancée.

Il s'attèle ensuite à la fraude au faux lutin. Afin d'identifier les lutins financiers, leurs collègues et les relations qu'ils entretiennent entre eux, la définition d'un organigramme précis est nécessaire. Le Grinch entame une une vaste campagne de social engineering, véritable filature sur les réseaux sociaux et les différentes plateformes sur lesquelles sont inscrits les lutins. Le Grinch se renseigne également sur les fournisseurs de matière première des ateliers, permettant la fabrication des cadeaux. Une fois qu'il aura investi le SI des ateliers, il pourra récupérer des informations plus pointues : coordonnées, factures, coordonnées bancaires (des fournisseurs et des lutins...).

Ces étapes terminées, il choisit l'identité du lutin et du fournisseur dont il va usurper l'identité et remplacer les RIB.

Pour finir, le Grinch met en place une fraude au Père Noël. Il n'est pas un expert en informatique mais est un ingénieur hors pair. Pour usurper l'identité de sa cible comme il se doit il a développé une machine qui transforme sa voix, appelée Deepvoice. À l'aide d'enregistrements audios, il peut imiter le timbre de voix du Père Noël et l'utiliser pour tromper ses interlocuteurs. Spécialisé en ingénierie sociale, le Grinch est prêt pour prendre la place du Père Noël.

« Tiens-toi prêt Max ! Demain on sabote Noël. », s'écrie le Grinch.

03 CHAPITRE 3 : LE GRINCH (ET MAX) PASSE(NT) À L'ATTAQUE

LE JOUR DU GRAND HACK EST ARRIVÉ !

Les premiers mails de phishing sont envoyés aux lutins ciblés et à la Mère Noël. Max et son maître attendent avec impatience le premier clic sur le lien infecté…

La première personne à se laisser tenter par les guimauves est la Mère Noël. Elle est redirigée vers une page de destination sur laquelle elle renseigne ses identifiants personnels pour ensuite donner son poids, qu'elle assume pleinement pour une fois. Puis elle part se servir un café, heureuse de ne pas avoir fait de régime le mois dernier. Vient le tour des lutins, le gestionnaire de paie suit la même démarche que sa supérieure et tombe lui aussi dans le piège. À la fin de la journée toutes les personnes ciblées ont cliqué sur le lien et renseigné leurs informations.

Au même moment, le malware a été introduit avec succès dans le SI de l'entreprise. Le Grinch peut désormais accéder aux bases de données.

En creusant dans le système, il accède à tous les RIB des lutins sur lesquels le Père Noël verse leur salaire.

« Remplaçons-les avec le nôtre Max ! » s'exclame le Grinch.

Ce sont tous les salaires de l'entreprise qui sont détournés. L'exploration continue et la liste des cadeaux défile avec les informations personnelles de toutes les familles de Noëlcity. Les fiches de commandes des rennes se révèlent et là Max a une idée : changer les cadeaux de la liste et modifier les adresses.

L'attaque s'avère encore plus agressive que prévue, le Grinch jubile.

Place maintenant à la fraude au faux lutin, le manager du service achat reçoit un appel d'un fournisseur de jouet en bois. Celui-ci l'informe d'un changement d'établissement bancaire et d'un changement de coordonnées bancaires à effectuer pour les futures factures.
Il ne se doute de rien car au bout du fil, c'est Max qui a transformé sa voix pour usurper l'identité du fournisseur.
Quelques jours plus tard, les malfaiteurs envoient un email au lutin manager afin de demander le règlement de plusieurs factures. Il procède donc aux virements.
Enfin vient l'heure de la fraude au Père Noël. Le Grinch appelle un des lutins financiers en se faisant passer pour le Père Noël. Il joue la comédie, feignant l'inquiétude tandis qu'il prétend avoir oublié de payer un fournisseur pour le cadeau de la Mère Noël.
« Le virement doit absolument être fait tout de suite », dit-il au lutin. « Mais s'il vous plaît, n'en parlez à personne, je ne voudrais pas que ma femme l'apprenne… »
Le lutin s'exécute. Il renseigne le RIB frauduleux et procède au virement. Le Grinch toujours en ligne, attend la confirmation de la transaction tout en continuant de presser son interlocuteur.
Les opérations sont terminées, l'argent détourné a été transféré sur plusieurs comptes à l'étranger pour brouiller les pistes.
Le Grinch et Max ont réussi leur coup ! Noël est hacké, la fête tant attendue ne pourra pas avoir lieu. Ils doivent maintenant disparaître avant que quelqu'un ne s'aperçoive des fraudes.

04 CHAPITRE 4 : PANIQUE À NOËLCITY

LES LUTINS N'ONT PAS ÉTÉ PAYÉS CE MOIS-CI.

Après enquête du lutin financier, il s'avère que tous les RIB ont été modifiés !

Ce ne sont pas les seules modifications qui ont été effectuées. Rudolf, le manager des rennes, a également vu que la liste des commandes au Père Noël a été modifiée.

La liste ne contient plus que deux enfants :

Julia
Cadeaux : 3 sprays anti-moustiques et un lot de sacs poubelle
Adresse : rue Blanchebarbe, Lieu dit Rougehotte.

Amine
Cadeaux : un trognon de pomme écrasé
Adresse : dans ta hotte, allée du gros rougeaud.

Il fait remonter l'information au Père Noël, qui commence à comprendre la supercherie dont lui et ses collaborateurs ont été victimes.

Les fournisseurs n'ont pas reçu le paiement de leurs factures et le signalent à l'entreprise. Le lutin du service achat est consterné, les fraudeurs n'ont quand même pas osé s'attaquer aux factures des fournisseurs... Il vérifie tout de même avec les différents fournisseurs qu'ils ne sont pas à l'origine du changement de leurs coordonnées bancaires. Malheureusement ils n'ont rien changé, c'est bien une manigance du Grinch.

Cerise sur le gâteau, le lutin financier victime de la fraude au Père Noël souhaite vérifier de vive voix avec son dirigeant la demande faite pour le cadeau de la Mère Noël.
Encore une fois ce n'était pas le Père Noël !

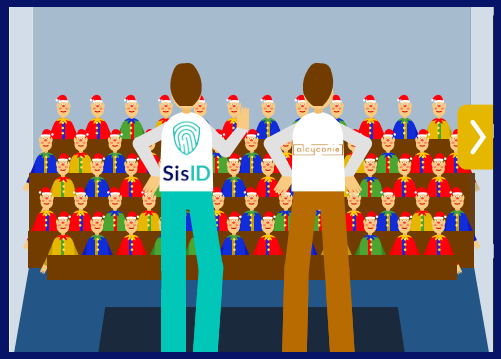
C'est officiel, c'est la panique !

Comment annoncer à toutes les familles de Noëlcity que leurs données ont été dérobées ? Le Père Noël et les juristes n'ont que 72h pour s'organiser.

La nouvelle se propage dans toute la ville. Le Grinch est responsable du Grand Hack de Noël.

NoëlCity est à l'arrêt et les enfants désespérés.

05 CHAPITRE 5 : ENSEMBLE POUR SAUVER NOËL



LE PÈRE NOËL RÉAGIT RAPIDEMENT, IL FAIT APPEL À ALCYCONIE ET SIS ID, DEUX SPÉCIALISTES DE LA LUTTE CONTRE LA FRAUDE.

Les équipes d'Alcyconie arrivées sur place ont une mission : faire sortir les ateliers de cette crise qui paralyse tout NoëlCity. Elles mettent en place un accompagnement auprès des lutins et du Père Noël afin de gérer au mieux cette crise. Le père Noël est débordé, il ne sait plus où donner de la tête. Entre les déclarations aux autorités, les dépôts de plaintes, les lutins qui réclament leur paie, ceux qui restent prostrés chez eux et refusent de revenir travailler, les journalistes de Noëlcity et du monde entier qui ont eu vent de l'affaire et campent devant les ateliers, bien décidés à obtenir une déclaration... Alcyconie va l'aider à définir quelles actions sont prioritaires et sur qui il peut s'appuyer au sein de ses équipes pour répartir les tâches.

Ensemble, ils décident de ne pas baisser les bras : Noëlcity aura son PCA ! La continuité des cadeaux va être assurée, Alcyconie le promet.

Un accompagnement psychologique s'organise pour les lutins qui en ressentent le besoin, heurtés par la cruauté du Grinch.

De son côté Sis ID a équipé le service financier des ateliers du Père Noël de sa plateforme collaborative de vérification de coordonnées bancaires. Maintenant l'ensemble du processus P2P des lutins financiers est sécurisé. Les coordonnées bancaires du Grinch sont signalées sur la plateforme et identifiées comme frauduleuses.

Les autorités ont été prévenues et sont à la recherche active du fraudeur vert.

Dans les ateliers, l'activité reprend car Noël peut encore être sauvé. Les fournisseurs soutiennent le Père Noël dans cette épreuve et se mobilisent pour que les enfants de Noëlcity aient des cadeaux.

C'est un véritable miracle de Noël !

La Mère Noël décide de régulariser les formations et activités de sensibilisation aux risques cyber proposées par Alcyconie pour rassurer ses équipes et éviter une nouvelle cyberattaque.
Noël n'avait jamais été aussi proche de la catastrophe !

Tout est bien qui finit... pas toujours bien.
Le Grinch court toujours ! Et qui sait quel sera son prochain coup ?

À PROPOS DE SisID

FinTech française créée en 2016, Sis ID accompagne les entreprises dans leur lutte contre la fraude aux virements bancaires.

Pensée et créée par des Directeurs Financiers et Trésoriers du CAC 40, la plateforme collaborative My Sis ID propose aux entreprises de partager :

- leurs enjeux de digitalisation de la fonction finance,
- leurs expériences et expertises en matière de fraude,
- leurs données de paiements,

dans un référentiel unique, sécurisé et centralisé, pour protéger leurs opérations bancaires.

La puissance de l'intelligence collective fait la force du réseau Sis ID !

À PROPOS D'alcyconie

Alcyconie, cabinet indépendant pure-player en gestion et communication des crises cyber et numériques, intervient en complémentarité avec l'offre d'outillage contre la fraude développé par Sis ID.

En effet, face à des cyberattaques qui se multiplient et amplifient les opportunités pour les fraudeurs, Alcyconie propose d'accompagner les entreprises à développer :

- Un dispositif de crise cyber intégrant le risque de fraude à toutes les étapes (alerte, mobilisation, gestion de la crise, continuité d'activité...)
- Des formations pour la cellule de crise* afin de travailler sur les méthodologies et bonnes pratiques de la gestion de crise cyber tout en les sensibilisant aux différents risques de fraude facilités par les cyberattaques
- Des formations spécifiques aux risques cyber et de fraude à destination des DAF, équipes trésorerie et compta
- Un PCA/PRA répondant aux besoins de continuité des activités bancaires en cas d'attaque paralysante
- Des exercices de crise cyber construits sur mesure, intégrant dans leur scénario une ou des tentatives de fraude réalistes.

Alcyconie est certifié QUALIOPI au titre de ses activités de formation.

Notre approche exclusive, cybercrisis management as-a-service, couvre l'ensemble des étapes de la gestion de crise : préparation aux crises, formations et simulations de crise cyber, veille et communication de crise cyber, astreinte 24/7, simulateur de crise unique PIA®.

Notre connaissance fine des enjeux et de la menace cyber nous permet de préparer les organisations à gérer une situation complexe et de conseiller et épauler les équipes décisionnelles, techniques et opérationnelles en cas de problème avéré.

PHISHING

Les lutins et la mère Noël ont subi une attaque de phishing.
Cette attaque consiste à adresser un e-mail contenant une pièce jointe ou un lien frauduleux, dans le but de récupérer des informations personnelles ou des identifiants.
Ces données permettent au fraudeur, par exemple, de procéder à des virements avec vos identifiants bancaires.

FRAUDE AU PRÉSIDENT

La fraude au Père Noël a permis au Grinch d'effectuer un virement frauduleux. Il a usurpé l'identité du Père Noël auprès du lutin financier.
Son mode opératoire : faire pression sur l'employé en utilisant le caractère urgent et confidentiel de la transaction. Un nouveau virement frauduleux a été lancé en contournant toute vérification.

FRAUDE AU FAUX FOURNISSEUR

Le Grinch a opéré une fraude au faux lutin.
Grâce à du social engineering opéré en grande partie sur les réseaux sociaux, il peut choisir ses cibles.
Il a usurpé l'identité d'un fournisseur pour entrer en contact avec le lutin manager du service achat et lui demander de changer les coordonnées bancaires de celui-ci. Par la suite c'est le règlement d'une facture qu'il demande et détourne ainsi le virement.

01

BONNE PRATIQUE N°1

Lorsqu'une mise à jour de vos données personnelles est demandée dans un email, vérifiez la légitimité de l'expéditeur ainsi que la nature des données qui sont demandées.

02

BONNE PRATIQUE N°2

Si un e-mail douteux contient un lien ou une pièce jointe, ne les ouvrez pas.

03

BONNE PRATIQUE N°3

Formez vos collaborateurs au respect des procédures de sécurité et contrôle avant d'effectuer une transaction bancaire. Il est très important de ne pas fléchir sur ces procédures durant les périodes de creux et en temps de crise.

04

BONNE PRATIQUE N°4

Sensibilisez vos collaborateurs aux modes opératoires et aux risques de fraude.

05

BONNE PRATIQUE N°5

En cas de doute, confirmez l'identité de l'expéditeur en utilisant des coordonnées différentes.

06

BONNE PRATIQUE N°6

Mettez en place un dispositif de gestion de crise cyber : le jour J, il sera trop tard !

Le dispositif comprend :

- **l'organisation** (membre des différentes cellules de crise…)
- **les processus** (procédures d'alerte, de mobilisation, de gestion de crise…)
- **les moyens** (salle de crise, annuaire de crise, main courante…).

07

BONNE PRATIQUE N°7

Formez les collaborateurs sur le dispositif de crise en place et sensibilisez les à la réalité d'une gestion de crise cyber.

08

BONNE PRATIQUE N°8

Entraînez vos équipes à faire face à une cyber attaque via des exercices de crise cyber, mobilisant vos équipes décisionnelles mais également opérationnelles. La gestion de crise cyber n'est pas juste de la responsabilité du RSSI, c'est avant tout une crise métier !

SisID alcyconie