EDITO

Bonjour à toutes et à tous, En ce mois de décembre, c'est l'heure du bilan ! C'est désormais une tradition : notre sixième édition annuelle est l'occasion pour nous de remettre en avant des articles déjà parus dans nos précédentes productions. Si les sujets présentés dans cette édition s'étalent d'août 2021 à avril 2022, ce type de rétrospective nous interpelle toujours sur le fait que, malgré leurs caractères passés, les articles que nous vous présentons sont toujours d'une effrayante actualité ! Nous vous donnons rendez-vous en 2024 pour de nouveaux contenus. Bonne lecture (ou relecture 😉) et bonnes fêtes de fin d'année !

Christophe Borry CISO (Chief Information Security Officer) du Crédit Agricole Pyrénées Gascogne

BON A SAVOIR
LES PAIEMENTS EN LIGNE

Article paru dans l'édition #17 de février 2021 :

Depuis le 1er janvier 2021 est entrée en vigueur la DSP 2 (Deuxième Directive sur les Services de Paiement) qui, devenant obligatoire à cette date, renforce la sécurité des paiements en ligne afin de lutter contre les fraudes et l'usurpation d'identité. La principale mesure qui s'impose désormais à tous les établissements financiers réside dans l'obligation de mettre en place un procédé d'authentification forte. **Authentification forte :**
L'authentification forte des paiements, (ou « Strong Customer Authentication » - SCA en anglais) est un dispositif destiné à renforcer la sécurité des paiements en ligne ainsi que des conditions d'accès

à un compte bancaire par Internet. Le principe général est de vérifier que vous êtes bien à l'origine d'un paiement par Internet ou de la connexion à votre « espace bancaire » en rendant obligatoire l'utilisation d'au moins 2 des 3 éléments suivants :

Un élément d'identification connu seulement par vous : code secret, mot de passe , question secrète... **L'usage d'un appareil personnel lié à l'utilisateur :** montre connectée, smartphone, carte à puce, Badge Rfid... **Une caractéristique biométrique :** reconnaissance faciale, empreinte digitale...

Alors comment explique-t-on la recrudescence de fraudes qui peuvent survenir malgré ces mesures de sécurité ?
La sécurité des systèmes bancaires étant de plus en plus robuste, les pirates préfèrent s'attaquer au maillon le plus vulnérable : Vous ! Au travers de faux mails, d'offres alléchantes ou d'escroqueries élaborées ils peuvent essayer de récupérer ces informations essentielles d'authentification et agir à la place de leurs victimes outrepassant ainsi les mesures mises en place. Si les cybercriminels arrivent à s'insérer entre vous et les différents systèmes d'authentification sécurisés, ils ont gagné ! Le coffre-fort le plus blindé du monde n'est rien si vous en possédez la clé... Voici quelques mesures simples vous permettant de déjouer ces pièges :

Prendre garde aux offres alléchantes présentées sur des sites méconnus ou provenant de mails issus d'émetteurs inconnus. Toujours privilégier les sites sécurisés disposant du fameux « https:// » limitant les possibilités d'interception des informations échangées. Être vigilant et réfléchir à deux fois avant de saisir ses coordonnées bancaires ou de carte. Se rappeler qu'aucune société ne vous demandera ni par mail ni à l'oral de fournir vos identifiants, mots de passe de connexion ou codes de carte bancaire. Contacter sa banque pour bénéficier dès aujourd'hui des solutions de sécurisation. Enregistrer par exemple votre smartphone dans le service SecuriPass proposé par le Crédit Agricole Pyrénées Gascogne, permettra d'éviter que quelqu'un d'autre le fasse à votre place ;)

INDICATEURS SECURITE

21,9 milliards de dollars par jour, c'est le préjudice attendu réalisé par le cybercrime en 2023 *(Source ATOS)* **53% des entreprises** ont signalé une cyber-attaque en 2023 *(à octobre, source Hiscox)* **Plus d'un milliard d'emails** : 25,7 % des emails reçus dans nos messageries électroniques sont des spams *(source mailinblack)* **+143%** c'est l'augmentation du nombre de victimes de ransomware au cours du deuxième trimestre 2023 *(source Le Monde Informatique)*

C'EST ARRIVE AILLEURS ANONYMOUS CONTRE-ATTAQUE CONTRE LA RUSSIE

Article paru dans l'édition #24 d'avril 2022 :

La guerre se joue aussi sur le terrain de l'information. Depuis le début de l'invasion russe en Ukraine, la Russie a pris soin de contrôler la moindre information qui circule dans son pays. Interdiction des VPN, loi sur la diffusion de « fausses informations » punissant toute diffusion de contenu visant à critiquer les forces armées du Kremlin… Le pays se refermant sur lui-même, bloquant toute forme d'information autre que celle autoproclamée dictée par Vladimir Poutine. Le collectif Anonymous est un mouvement hacktiviste (entendez pirate informatique qui agit par activisme) qui utilise ses compétences informatiques en fomentant des attaques visant à obtenir une justice politique, sociale ou religieuse conforme aux idéaux qu'ils se sont attribués. Ceux-ci, en révolte contre l'invasion Ukrainienne par la Russie, ont décidé de passer à l'action.

Acte 1 – Paralyser les médias

Dès le 7 mars 2022, plusieurs chaînes russes, connues pour être contrôlées par le Kremlin, ont été attaquées par le collectif qui en a pris le contrôle. Les chaînes de télévision R24 (Russia 24), Moscow 24, Channel One ainsi que les plateformes de streaming Wink et Ivi ont, bien malgré elles, diffusé des images de la guerre en Ukraine dévoilant une autre réalité que celle dictée par le gouvernement Russe. L'objectif pour le collectif était de montrer au peuple Russe la réalité d'un

conflit dont on lui cache presque jusqu'à l'existence. Dès le début du conflit, Vladimir Poutine maintenait en effet que la Russie menait une "simple" opération de désarmement pour libérer les Ukrainiens de l'oppression... bien loin de la réalité de cette guerre. En raison de la propagande d'État et de la censure, la majorité des images de cette invasion sont interdites et sont, pour le peu qu'il en reste, édulcorées ... Le message d'Anonymous diffusé en lieu et place des programmes des chaînes piratées est on ne peut plus clair : "Cette guerre a été menée par le régime criminel et autoritaire de Poutine au nom des citoyens russes ordinaires. Russes, opposez-vous au génocide en Ukraine".

Acte 2 – Lever le masque

La deuxième offensive du collectif date du 11 mars et concerne le piratage de Roskomnadzor, l'agence fédérale russe chargée de surveiller et de censurer les médias. Anonymous a pu se procurer, grâce à cette attaque, des documents montrant que la Russie censure l'information, notamment concernant son rôle dans cette guerre. Ce sont près de 360 000 fichiers qui ont été ensuite publiés par le groupe de hackers. Pour la plupart, ceux-ci démontrent comment le Kremlin a censuré toutes les informations qui pourraient mettre en évidence la réalité de l'invasion de l'Ukraine par la Russie. Intoxication ou pas, le Kremlin s'est ensuite félicité d'avoir riposté en faisant tomber le site officiel du collectif... Anonymous a démenti l'information selon laquelle son site Web aurait été piraté par des pirates pro-russes... pour la simple et bonne raison que ce site n'existait pas !

CA N'ARRIVE PAS QU'AUX AUTRES « JE COMPTE SUR VOUS... »

Article paru dans l'édition #23 de février 2022 :

La société Sefri-Cime est dans la tourmente en ce début d'année. Ce groupe spécialisé dans la construction et la promotion de programmes immobiliers, vient de se faire détourner plusieurs millions d'euros au nez et à la barbe de ses dirigeants. L'affaire a débuté le 2 décembre 2021, lorsque la responsable de la comptabilité de la société Sefri-Cime a été contactée par e-mail par un escroc se faisant passer pour le Directeur Général de l'entreprise. Ce message « confidentiel » prétextait que se préparait l'entrée en Bourse de l'entreprise. Le « faux directeur » a ordonné à la comptable de réaliser plusieurs virements vers des comptes bancaires à l'étranger, lui demandant de faire cela dans la plus grande discrétion. La collaboratrice, a donc procédé à près de quarante virements à la demande des escrocs. Les fonds ont tous été envoyés vers des comptes bancaires à l'étranger (principalement vers la Hongrie, la Croatie et la Grèce). Bien entendu les sommes ont ensuite été redirigées vers des paradis fiscaux. L'arnaque aurait pu durer plus longtemps si l'alerte n'avait pas été donnée par un autre comptable qui venait de tomber sur un mail des arnaqueurs le 29 décembre. Le préjudice total s'élèverait à plus de 33 millions au profit des malfrats. Dès le 30 décembre, les enquêteurs de la brigade des fraudes ont été saisis de l'affaire.

L'arnaque au président (FOVI ou Faux Ordres de Virement à l'International)

L'arnaque au président utilise invariablement la même mécanique : elle consiste pour le fraudeur à entrer en contact avec un opérateur d'une entreprise cible (comptable, secrétaire, adjoint) ayant des pouvoirs de validation d'ordres financiers en se faisant passer pour le président de la société mère ou du groupe. Le **contact** se fait par **mail** ou par **téléphone** (jamais en personne). Les premiers échanges sont destinés à instaurer **la confiance**, puis le fraudeur demande que soit réalisé un **virement international non planifié**, au **caractère urgent** et **confidentiel**. L'attaque réussit si l'entreprise ciblée s'exécute... L'un des pionniers à l'origine de cette arnaque est le Franco-Israélien Gilbert Chikli. Alors qu'il était en fuite en Israël, il a été condamné en 2015 à sept ans de prison pour avoir utilisé ce procédé et escroqué plusieurs grandes entreprises. Plus récemment, en 2020, il a de nouveau été condamné à sept ans de prison pour s'être fait passer pour Jean-Yves Le Drian, notre ministre français des Affaires Etrangères, auprès de riches personnalités dans le but de les soulager de dizaines de milliers d'euros. Un film sorti en 2015 a même été réalisé sur les aventures de ce roi de l'arnaque : « Je compte sur vous » de Pascal Elbé ;)

C'EST ARRIVE PRES DE CHEZ VOUS UNE COMMANDE BLOQUÉE

Article paru dans l'édition #20 d'août 2021 :

L'arnaque est toujours très bien montée, les clients ciblés reçoivent en effet un mail indiquant que la validation de leur commande nécessite une action de leur part... Or, comme ils n'ont rien commandé, les victimes potentielles sont tentées de répondre à ce message qui semble légitime... C'est là que le piège se referme sur eux :

De : Merci pour votre commande ! <support@3op.devpv.pl>
Envoyé : vendredi 12 mars 2021 à 05:32
À : [redacted]@hotmail.fr
Objet : Confirmation de votre commande n°0613

Détails de la transaction originale

Description	Prix unitaire	Quantité	Montant
Apple iPhone 12 Noir Numéro #: 73800	909.00 EUR	1	909.00 EUR

Total: Total EUR : 926.59
Frais de port et de manutention: 7.50€
Assurance: 10.09€
Total: 909.00€

Numéro de Facture: 34516103

Informations utiles
- Dès la réception de votre commande, merci de confirmer la réception de celle-ci dans votre espace client.

Pensant qu'il s'agit d'un mail légitime du site de paiement mais que la transaction elle, est malhonnête, le client paniqué peut être amené à cliquer sur le lien de contestation. C'est alors qu'il est dirigé vers un faux site où il saisira ses coordonnées confidentielles réutilisées ensuite par les fraudeurs pour réaliser de vraies opérations frauduleuses... **Notre conseil :**
Si vous avez un doute sur une transaction, ne cliquez jamais sur le lien présent dans le mail, mais connectez-vous plutôt à votre compte client en ouvrant une nouvelle page web sur votre navigateur pour en vérifier les informations.

LE SUJET DU MOIS
UN PEU D'HISTOIRE LE PRINCE NIGERIAN

Article paru dans l'édition #23 de février 2022

L'escroquerie par e-mail du « prince nigérian » est peut-être l'une des fraudes Internet les plus anciennes.

Le principe :

Également appelées escroqueries par « lettre nigériane » ou « arnaque aux frais d'avance », elles commencent généralement par un e-mail d'une personne à l'étranger qui prétend être issue de la royauté ou disposer d'une grande fortune. Les fraudeurs vous attirent en vous offrant une part d'une énorme opportunité d'investissement ou d'une somme mirobolante qu'ils ne peuvent pas sortir du pays sans votre aide. Ensuite, ils vous demandent soit votre numéro de compte bancaire afin qu'ils puissent vous transférer l'argent en lieu sûr, soit un petit acompte pour aider à couvrir les frais de transfert de l'argent, moyennant toujours un pourcentage pour votre précieuse aide… C'est alors qu'ils prennent votre paiement et disparaissent, ou, pire, vident votre compte bancaire.
Quelques variantes :

La loterie : un e-mail vous informe que vous avez gagné à la loterie, même si vous n'avez pas acheté de billet. Pour vous aider à récupérer la somme, l'escroc se faisant passer, par exemple, pour la Française de Jeux, vous demande une modeste somme d'argent en avance de paiement. Les sites de rencontre : appelées arnaques ou fraudes sentimentales, les escroqueries sur les sites de rencontres surviennent lorsqu'une personne pense échanger avec une autre sur un site ou une application. En réalité son interlocuteur est un escroc utilisant un faux profil qui va ensuite profiter de sa victime en lui soutirant de l'argent. Ce type d'arnaque est réalisé par des malfrats appelés « catfisher ». L'héritage : une personne que vous ne connaissez même pas vous nomme comme héritier d'une grosse fortune mais vous devez d'abord faire un petit dépôt pour obtenir votre héritage…

Appelée également « Arnaque 419 », du nom de l'article de la section du code pénal nigérian qui définit cette fraude, l'escroquerie nigériane peut sembler être un fléau de l'ère d'Internet, mais elle est en réalité antérieure au courrier électronique. Bien avant que nous ne commencions à recevoir des emails inattendus dans nos boîtes de réception, des escrocs en Afrique de l'Ouest exerçaient leur métier par fax, télégrammes et lettres papier. Les premières escroqueries de ce type à apparaître en Europe sont arrivées par télex en 1989 par le biais des transactions sur le pétrole. Des hommes d'affaires britanniques ont effectivement eu vent qu'un pétrolier de brut nigérian en difficulté, pouvait céder sa cargaison de pétrole à des prix anormalement bas – à condition, bien sûr, de payer certains frais à l'avance pour profiter de cette aubaine financière. Mais même si cette arnaque, qui remonte aux années 1980, peut nous sembler très ancienne, ce type d'escroquerie trouve ses origines bien plus tôt dans l'histoire, comme le témoignent les exemples suivants qui en définissent ses contours modernes.

La lettre de Jérusalem :

En 1836, le célèbre Eugène-François de Vidocq, ancien délinquant et bagnard devenu chef de la sûreté nationale pendant la Restauration, rédige un ouvrage intitulé **Les Voleurs** dans lequel il raconte la façon dont des prisonniers envoient chaque jour des lettres d'escroquerie, nommées en argot des voleurs "lettres de Jérusalem". Dans ces courriers, les malfrats ciblent des personnes riches de préférence, habitant en province. Dans ces lettres, ils assurent à leurs potentielles

victimes qu'ils ont connaissance de l'existence d'un trésor caché. Prétextant qu'ils sont évidemment dans l'incapacité d'y d'accéder, ils réclament de l'aide, contre la garantie de récupérer une fraction de la fortune cachée. Bien entendu, les victimes, une fois les premiers frais avancés, n'entendaient plus parler de ces arnaqueurs. Une autre version, plus proche de nous, jouait sur les mêmes ressorts, en ajoutant une touche de romantisme à l'histoire...

Le prisonnier/La prisonnière espagnole :

Cette arnaque est apparue pour la première fois au XIXe siècle et a évolué au fil des ans pour revêtir diverses formes, mais là aussi toujours en utilisant la même dynamique. Cette escroquerie était exploitée par des criminels basés en Espagne. Ils ont envoyé des centaines de lettres à travers l'Angleterre, racontant l'histoire émouvante d'une personne détenue dans une prison espagnole. En règle générale, l'histoire racontait qu'un ancien militaire était retenu prisonnier dans une geôle espagnole. Pour mettre en confiance les victimes britanniques, le fraudeur écrivait que son père ou son grand-père était anglais et qu'il était entré dans l'armée Espagnole avant d'être accusé, à tort, d'avoir volé de l'argent. Désormais gravement malade, il craignait pour sa vie. Le nœud de l'escroquerie résidait dans la révélation, par le condamné, qu'il avait une fille ayant besoin de soins. Le fraudeur proposait alors de nommer dans son testament le destinataire de la lettre comme tuteur de sa fille en promettant de révéler où il avait caché une grosse somme d'argent qui devait être récupérée dans un endroit secret... Bien entendu, là encore, après que la victime a répondu à ce qu'elle pensait être une histoire sincère et véridique, de l'argent était demandé pour payer les frais de voyage de la fille...

Des scénarios infinis

Comme nous l'avons vu, ces détournements ont existé tout au long de l'histoire sous différentes formes mais tous avec la même logique : un mystérieux donateur richissime ou une promesse de richesse inattendue... Il est évident, par conséquent, que de nouveaux scénarios s'évertuent à user des mêmes ficelles de nos jours et il y a fort à parier que ce type d'arnaques continuera à pulluler sous d'autres formes, dans les années à venir. **Pour aller plus loin** Une version « moderne » ce cette arnaque est mise en images dans l'excellent film « La prisonnière espagnole » de David Mamet, sorti en 1997.

RETROUVEZ LES ANCIENNES EDITIONS