# EDITO

Bonjour à toutes et à tous, Alors que nous avançons dans l'ère du numérique et de l'intelligence artificielle, la cybersécurité demeure une préoccupation centrale, affectant tout un chacun à l'échelle mondiale. Notre édition de ce mois se concentre à nouveau sur des événements récents et inquiétants qui soulignent l'importance de rester vigilants et informés. À noter dans cette édition : deux articles consacrés au « quishing » (arnaque par QR Code), phénomène qui est en train de prendre de l'ampleur dans le paysage de la cybercriminalité. Notre objectif est de vous fournir des informations pertinentes et actualisées qui vous aideront à mieux comprendre et à naviguer dans le paysage complexe de la cybersécurité. Nous espérons que cette édition vous apportera à nouveau des connaissances précieuses par le biais de situations concrètes afin de renforcer votre sécurité numérique. Restez sécurisés et informés, Bonne lecture,

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

# BON A SAVOIR

## LE QUISHING OU L'ARNAQUE AU QR CODE

Le quishing, ou "QR phishing", est une nouvelle tactique de cybercriminalité utilisant les QR codes pour tromper les utilisateurs dans le but de permettre aux pirates de s'enrichir grâce à des paiements frauduleux. Ces attaques surfent sur la présence omniprésente des QR codes dans notre environnement. C'est en combinant des tactiques trompeuses à ce vecteur de communication que les pirates incitent les utilisateurs à révéler des informations personnelles ou financières. Ces QR codes frauduleux sont généralement placés dans le domaines public (gare, rue,

borne de stationnement...) pour remplacer ou se superposer sur des QR codes authentiques, redirigeant les victimes vers des sites Web frauduleux qui vont récolter les données de paiement.

**Fonctionnement :** Le ressort principal des attaques de quishing est la confiance qu'ont les utilisateurs sur les éléments où sont placés ces codes malveillants. Le postulat de base d'un utilisateur est que la borne de paiement qui se présente devant lui ne présente à priori pas de danger d'escroquerie et que par conséquent le QR code présenté hérite de la confiance donnée à priori par la future victime à ce processus de paiement. Un autre vecteur largement utilisé dans les phishings (et c'est un motif récurrent dans ce type d'attaque), c'est l'urgence. Les notions d'urgence ou les opportunités de bonnes affaires avec une date proche sont des moyens d'incitation efficace pour pousser une victime à scanner un QR code sans l'examiner attentivement.

**Risques du Quishing** Comme toutes les techniques de l'éventail de la cybercriminalité, le quishing présente un risque à ne pas négliger, pouvant entraîner comme nous l'avons vu, des pertes financières mais également de la récupération de données personnelles pour les consommateurs. Les attaques de quishing peuvent conduire à des violations de données significatives. Un individu peut par exemple scanner un code QR, croyant qu'il s'agit d'une enquête ou d'un sondage, le code ainsi utilisé se charge ensuite de collecter les informations de connexion saisis par l'internaute imprudent.

**Notre Conseil** Soyez Vigilant : Faites preuve de prudence lorsque vous utilisez des QR codes, en particulier ceux émanant de sources inconnues. C'est un conseil d'hygiène numérique incontournable : Changez fréquemment vos mots de passe et n'utilisez jamais le même mot de passe pour plusieurs comptes.

***Aller plus loin*** Le quishing représente, comme nous l'avons vu, une menace cyber en pleine évolution. Nous avons décidé de consacrer un article de notre rubrique « Ça n'arrive pas qu'aux autres » de cette édition de février à un cas particulièrement concret d'une fraude réalisée grâce à cette technique sur des bornes de recharge électrique.

# INDICATEURS SECURITE

**411 000 fichiers malveillants libérés par jour** par les cybercriminels *(Source Kapersky)* **30% des malwares** proviennent de campagnes de phishing *(source Deloitte)* **+173 % d'augmentation du nombre de mails de phishing** recensée au 3e trimestre 2023 *(source SoSafe)* **30 000 sites** sont piratés quotidiennement dans le monde *(source leBigData)*

# C'EST ARRIVE AILLEURS

## UN ÉDITEUR DE JEUX VIDÉOS PIRATÉ

**La cyberattaque et Ses Conséquences**

L'attaque de décembre 2023 sur la société de production de jeux vidéo Insomniac Games a eu l'effet d'un coup de massue sur la production de cette maison d'édition. Cette entreprise est notamment connue pour ses titres à succès tels que Ratchet & Clank ainsi que pour son accord de licence avec Marvel lui permettant de produire des jeux inspirés de la célèbre franchise de Super-Héros.

**1.67 To de données** Les pirates, se réclamant du groupe de ransomware Rhysida, ont ainsi divulgué une quantité énorme de données, évaluée à plus de 1,2 million de fichiers soit environ 1,67 To de données. Ces données qui incluaient des détails sur les jeux à venir, contenaient de surcroit des informations personnelles des collaborateurs, d'anciens employés ainsi que développeurs indépendants travaillant en tant que consultants.

**Impact sur les Sorties de Jeux à Venir** Dans les données divulguées, figuraient de nombreuses informations top secrètes sur les futurs projets d'Insomniac Games. Ces secrets de sortie sont généralement bien gardés mais la fuite révélait les périodes de sortie de ses premiers titres inspirés des X-Men. Ces productions d'un budget total de 360 millions de dollars (120 millions par titre) représentaient un investissement colossal pour la société qui avait prévu de soigner tous les aspects du lancement. Parmi les titres qui ont fuité, on peut compter par exemple le jeu consacré au célèbre X-Man, Wolverine (prévu au plus tard le 1er septembre 2025), un deuxième jeu X-Men (avant le 31 décembre 2029) et un troisième (avant le 31 décembre 2033). En plus de ces informations, des séquences, des concepts arts, ainsi que des versions jouables limitées de certains

autres jeux faisaient partie des données divulguées. Dans les données ainsi rendues publique, il a été trouvé des mentions à un nouveau jeu Spider-Man comme suite du Spider-Man 2 de 2023, ainsi que le prochain jeu Ratchet & Clank, prévu pour 2029. Après avoir subi les conséquences de cette violation et encaissé le coup, Insomniac Games a affirmé son dévouement à poursuivre le développement des jeux sans changer son calendrier. Le studio a, de surcroît, exprimé sa détermination à surmonter les défis posés par cette cyberattaque et a affirmé son souhait de maintenir la qualité et l'intégrité de ses sorties pour les années venir. Ce piratage d'Insomniac Games sert de rappel frappant des vulnérabilités de la sécurité numérique et des conséquences étendues que de telles violations peuvent avoir sur la vie privée et les stratégies d'entreprises. L'industrie du jeu vidéo, ainsi que son public, sont désormais confrontés à la tâche complexe de naviguer dans ces défis de sécurité, tout en se réjouissant des développements passionnants dans le domaine du jeu vidéo, qui se profilent à l'horizon.

# CA N'ARRIVE PAS QU'AUX AUTRES

## UNE BORNE DE RECHARGE COURCIRCUITÉE ?

C'est en décembre 2023, qu'une arnaque de type « Quishing » (arnaque par QR Code) a ciblé des propriétaires de véhicules électriques (VE). Pour recharger les véhicules, l'hexagone est doté de milliers de bornes de recharges publiques, comme dans le petit village de Lorris dans le Loiret. Pour fonctionner et délivrer l'énergie nécessaire à la recharge du véhicule, un système de badge permet de s'identifier afin de valider l'opération sur la borne. Si l'utilisateur ne possède pas ce précieux sésame, les points de charges permettent en outre aux clients de scanner un QR code qui les redirige vers un site de paiement pour la recharge de leur véhicule. C'est ce dernier mode de fonctionnement qui a été utilisé dans cette arnaque : les criminels ont utilisé de faux QR codes superposés sur le code légitime, redirigeant les utilisateurs vers un site web frauduleux conçu pour les inciter à fournir leurs informations de carte bancaire, occasionnant des paiements illicites au

profit des pirates. Comble de l'ironie, pour éviter de se faire repérer, les criminels, qui n'ont toujours pas été identifiés, ont eu la finesse de limiter à souvent quelques euros le montant des prélèvements, afin qu'ils restent proches du prix d'une recharge. On appelle ce type de piratage « attaque man-in-the-middle » (attaque de l'homme du milieu) car les cybercriminels viennent intercepter les informations de la victime entre ce dernier et l'action légitime qu'il est en train de réaliser. Il s'agit en effet d'une tactique simple et efficace. Très facile à réaliser, elle n'a pas nécessité de s'attaquer à la borne de recharge elle-même ni à l'application de paiement associée légitimement au système de recharge. Avec la pandémie de Covid-19, l'utilisation des QR codes s'est généralisée dans de nombreux domaines, rendant les tentatives d'hameçonnage d'autant plus faciles. Il y a fort à parier que ce type d'escroquerie risque de faire tache d'huile.

**Quelles précautions prendre ?** La première est d'utiliser les applications officielles : privilégiez les applications mobiles du fournisseur d'Energie de la borne pour payer votre session de recharge. Ces applications permettent de sécuriser la transaction mais également de suivre en direct le déroulement de la charge. L'autre solution, pour éviter de scanner un QR Code, est de passer par des services qui prennent en charge plusieurs réseaux de charge grâce leur carte NFC comme Chargemap freshmile ou encore Chargepoint pour les plus connus. Dans tous les autres cas, il convient de bien vérifier que le QR code renvoie sur le site auquel il est censé accéder. Comme toujours, la vérification de l'adresse du site (l'URL) est primordiale (si elle vous paraît incohérente : passez votre chemin). Vérifiez toujours que l'adresse commence par "https://" – gage d'une connexion sécurisée.

# C'EST ARRIVE PRES DE CHEZ VOUS

## VOTRE COLIS EST EN ATTENTE

La période des fêtes de fin d'année et la traditionnelle époque de soldes qui s'ensuit sont des

moments où l'activité des achats en ligne explose. Des millions de colis sont commandés par les consommateurs et des délais plus longs liés à cette affluence temporaire sont souvent constatés. C'est sur ce phénomène saisonnier que surfent les cybercriminels qui ont multiplié de façon industrielle les faux mails ou SMS relatifs à des problèmes de livraisons de colis. En voici un exemple, parmi tant d'autres reçus d'un client par nos services avec quelques clés pour identifier la supercherie :


# LE SUJET DU MOIS

## LE PORTEFEUILLE NUMÉRIQUE EUROPÉEN :

## VERS L'INTÉGRATION NUMÉRIQUE

La genèse du portefeuille numérique européen trouve ses racines dans le processus progressif de l'intégration numérique européenne. Depuis les années 2000, l'UE a adopté plusieurs politiques et directives pour favoriser le développement du marché unique numérique. Ces initiatives comprennent la Directive sur les services de paiement (DSP2), le Règlement Général sur la Protection des Données (RGPD), et le Code des communications électroniques européen. La Commission Européenne, le Parlement Européen et le Conseil de l'Europe viennent de trouver un accord sur l'identité numérique. Ce projet, qui a muri au fil des années, a pour but de mettre à disposition de chaque citoyen européen une sorte de plateforme destinée à conserver ses différents documents d'identité (passeport, carte d'identité, permis de conduire...). Cet espace pourra également servir de plateforme sécurisée pour effectuer des transactions.
**L'ambition d'un marché unique numérique et la stratégie de l'UE** Le marché unique numérique est un pilier central de la stratégie de l'UE. Il vise à supprimer les barrières liées à l'usage d'Internet et à permettre aux personnes et aux entreprises de profiter pleinement du potentiel numérique de

l'Europe. Dans ce cadre, le portefeuille numérique est conçu comme un outil permettant de naviguer plus aisément dans cet espace unifié. C'est une pierre fondamentale de la construction de l'autonomie digitale européenne La priorité principale au cœur de la construction de ce portefeuille est la confiance. En effet, la sécurité (security by design) sera au centre des préoccupations de développement de cette application. Les données seront protégées et chiffrées à chaque étape. Fin 2023, les trois institutions du vieux continent se sont accordées sur le texte (le Conseil Européen, la Commission Européenne et le Parlement Européen), Il faudra maintenant environ deux ans pour voir fonctionner, sur l'ensemble de l'union, ce fameux « Digital ID Wallet » (portefeuille d'identité numérique). Pour ce faire, quatre consortiums dont Potential, porté par l'Agence Nationale des Titres Sécurisés (ANTS) et le ministère de l'Intérieur, ont pour objectif de tester le déploiement. L'identité numérique est ainsi expérimentée à l'échelle européenne. C'est également dans ce cadre que la France a lancé très récemment l'application « France identité. » Voyons en détails les fonctionnalités attendues : Les grandes fonctionnalités déjà présentées ne sont que le socle d'innovations à venir, mais on peut d'ores déjà dévoiler que ce passeport bénéficiera d'une authentification sécurisée avec authentification forte, très certainement associée avec un appareil pour renforcer la robustesse (PassKey). Ce sésame universel sera la porte d'entrée unique à privilégier pour accéder à des services en ligne officiels ou affiliés au processus. Le stockage des documents officiels sera également au rendez-vous. Une des fonctionnalités attendues sera la possibilité de stocker et de gérer ses documents numériques officiels, sorte de coffre-fort numérique personnel. Une autre des promesses est l'interopérabilité transfrontalière. Tous les états membres étant sur la même plateforme, cela permettra de faciliter l'accès aux services administratifs et affiliés dans les différents États de l'UE. **Les ambitions de ce projet :** La démarche de l'Union est audacieuse et ambitieuse mais s'inscrit dans une démarche cohérente et innovante ; le but principal étant de ne pas rater le virage de la révolution digitale. À ce titre, ce projet aura de sérieux avantages : Tout d'abord, le renforcement du marché intérieur européen : ce portefeuille numérique va contribuer à renforcer le marché intérieur en facilitant le commerce et les services en ligne. Ensuite, une dimension pédagogique essentielle sous-tend la démarche. Il s'agit de favoriser l'inclusion numérique afin de familiariser le plus possible de citoyens de l'UE au digital, en leur donnant plus de simplicité et de facilité d'accès aux services numériques associés. La lutte contre la fraude et l'usurpation d'identité : de par sa construction même, le portefeuille digital va offrir un mécanisme robuste pour contrer les activités frauduleuses et protéger l'identité des utilisateurs. Grâce aux fonctionnalités de sa plateforme, il sera également possible de signaler des violations de données qui seront centralisées entre tous les acteurs. Et bien sûr, fil rouge de l'ensemble de la démarche entreprise par l'UE : la Protection des Données. le passeport accentue encore la protection des données personnelles en ligne, encadré par les dispositions héritées du RGPD.

**Le chemin est encore long :** Bien que prometteur, le portefeuille numérique européen doit surmonter plusieurs défis. C'est, pour l'essentiel, la raison qui explique que son déploiement progressif s'étalera jusqu'en 2026. Il s'agit, comme nous l'avons évoqué, d'un projet ambitieux qui nécessite pour réussir de fédérer tous les Etats, mais également d'être largement adopté par les Utilisateurs. Un des enjeux majeurs sera donc de promouvoir et d'encourager l'adoption massive par les citoyens européens. La sécurité des données également, est une des préoccupations essentielles du lancement de ce portefeuille. Au cœur de ce thème, la confiance que veut insuffler ce portefeuille numérique se devra d'être à l'épreuve de toute cyberattaque et hermétiques aux

fuites de données. C'est l'essence même de son existence. Véritable casse-tête administratif et numérique, les responsables du projet devront également surmonter la difficile harmonisation des systèmes nationaux afin de garantir l'interopérabilité entre les différents systèmes d'identité numérique et services co-existants entre les différents États membres de l'UE.

**Une avancée majeure** Le portefeuille numérique européen est un jalon important dans la quête de l'UE pour une intégration numérique complète. En offrant une solution harmonisée pour l'identification et l'accès aux services en ligne, il représente un pas de géant vers un avenir numérique plus intégré et sécurisé pour tous les citoyens de l'UE. C'est également un moyen d'affirmer la puissance et l'indépendance de l'Europe face aux géants américains des GAFA.

RETROUVEZ LES ANCIENNES EDITIONS