QRCodes : pièges à internaute ? – ZATAZ

	QRCodes : pièges à internaute ? – ZATAZ

Détection du premier cas d'email frauduleux utilisant des QRCodes. Le Flashcode, une porte d'entrée à pirate qu'il ne faut pas négliger.

On retrouve ces QRcodes, baptisés aussi Flashcode, dans les journaux, la publicité… Il est possible de naviguer vers un site internet ; mettre l'adresse d'un site en marque-page ; faire un paiement direct via son cellulaire (Europe et Asie principalement) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique ; déclencher un appel vers un numéro de téléphone ; envoyer un SMS ; montrer un point géographique sur Google Maps ou Bing Maps ; coder un texte libre. SnapChat, par exemple, propose un QR Code maison pour suivre un utilisateur. Bref, toutes les possibilités sont ouvertes avec un QRcode. Il suffit de présenter l'image à votre smartphone, et à l'application dédiée, pour lancer la commande proposée par le QR Code. A première vue, un pirate a eu l'idée de fusionner QR Code et hameçonnage.

Fusionner QR Code et hameçonnage

Le hameçonnage, baptisé aussi Phishing/Filoutage, est une technique qui ne devrait plus être étrangère aux internautes. Pour rappel, cette attaque informatique utilise le Social Engineering dont l'objectif est la collecte des identifiants de connexion (mail, login, mot de passe, adresse IP…). Dans l'attaque annoncée il y a quelques jours par la société Vade retro, le cybercriminel a présenté son mail comme une image usurpée à un opérateur national et proposant au destinataire un remboursement consécutif à une facture payée. Le QR Code conduisait à un site présentant une page falsifiée qui incitait la victime à renseigner son identifiant et mot de passe légitime chez l'opérateur usurpé, puis présentait un message d'erreur.

L'illustration flagrante des cyber-risques pour tous

Comme le rappel Maitre Antoine Chéron, avocat spécialisé en propriété intellectuelle et NTIC aujourd'hui, presque tout le monde a une adresse électronique personnelle ou du moins professionnelle. C'est en effet devenu un mode de communication indispensable non seulement pour travailler mais également pour consommer toutes sortes de biens et services. Destinées aux particuliers, les messageries électroniques ne sont pas toujours sécurisées. Avec l'usage en masse de l'internet, et la dématérialisation des richesses, ce sont de précieux biens tels que nos données personnelles, « l'or noir du 21ème siècle », qui sont aujourd'hui convoités par les personnes mal intentionnées.

QRCodes : carrés aux angles dangereux

Les QRcodes envahissent le web et nos vies. Déjà, dès 2012, je vous informais d'une attaque découverte dans le métro parisien. Preuve que les pirates se penchaient sur la manipulation des QRcode depuis longtemps. J'ai pu rencontrer un chercheur « underground » qui s'est penché sur le sujet. Nous l'appellerons DBTJ. Il se spécialise dans la recherche de procédés détournés pour QRcode. « ***Avec mes collègues,*** explique-t-il à ZATAZ.COM, ***nous avons testés plusieurs cas, qui, hélas, se sont avérés efficaces.*** » Dans les cas de Qrcodes malveillants que j'ai pu constater : naviguer vers un site internet et se retrouver face à un code raquetteur (Ransomware) : mettre l'adresse d'un site en marque-page (Shell) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique, lancer un DDoS… bilan, derrière cette possibilité se cachait un vol de données et une mise en place d'usurpation d'identité.
J'ai pu constater aussi des QR Code capable de déclencher un appel vers un numéro de téléphone ou envoyer un SMS. « Nous avons réfléchis aux méthodes d'infections les plus débiles aux plus élaborés, s'amuse mon interlocuteur. Envoyer le QRcode depuis votre téléphone ; la fonctionne SMS dans SET pourrait être intéressante et ne laissera pas de traces ; utiliser le QRcode sur de faux sites, ou encore des sites vulnérables XSS (via un iframe) ; fausses publicités ; remplacer les QRcode aperçus sur des affiches. »
Ce dernier cas a été remarqué par ZATAZ.COM. Il suffit de coller un autre Flashcode, malveillant cette fois, en lieu et place de l'original sur une affiche, dans un arrête de bus par exemple. Effet malheureusement garanti. « Dans le cadre de la démonstration, nous avons infecté exactement 1.341 personnes d'une banlieue de Saint-Denis, et cela en seulement 14 heures, souligne le témoin de ZATAZ.COM. Avec une technique de SE (Social Engineering) d'une simplicité redoutable, nous avons fait des publicités contenant notre QRcode pour un jeu mobile gratuit que nous avons ensuite imprimé en plusieurs exemplaires et diffuser dans les lieux publics (gare/train – centre-ville). » ZATAZ.COM peut confirmer qu'après le test, les « pentesteurs » du QRcode ont effacé l'intégralité des informations collectées.
Bref, voilà de quoi regarder ces petits carrés noirs et blancs d'un œil nouveau … et plus suspicieux. Pour se protéger, des logiciels comme GData QRCode permettent de palier ce type d'intrusion. A utiliser sans modération.

Article original de Damien BANCAL

Réagissez à cet article

Original de l'article mis en page : QRCodes : pièges à internaute ? – ZATAZ