***Campagnes de phishing par QR codes en accÃ©lÃ©ration.***
**Internet**
PostÃ© par : JerryG
PubliÃ©e le : 12/10/2023 13:00:00

Depuis fin 2022, le Centre de recherche avancÃ©e (ARC) de Trellix a constatÃ© une forte augmentation des attaques de phishing via QR codes. Beaucoup de pays sont Ã ce jour touchÃ©s, bien que ce ne soit pas encore le cas de la France. Voici ce que les chercheurs de lâ□□ARC ont constatÃ© :

**Campagne 1 : Attaque phishing de comptes Microsoft via QR code**

Depuis la mi-mai 2023, une nouvelle technique dâ□□attaque de phishing sÃ©vit et cible les comptes Microsoft. Son originalitÃ©, elle utilise un QR code, ce qui lui permet dâ□□Ã©chapper Ã la vigilance des systÃ¨mes de sÃ©curitÃ© qui se basent uniquement sur la dÃ©tection de texte et dâ□□URL.

***Plus en dÃ©tails :***

â□¢ Le mail suspect contient simplement du texte et un QR code, tous les deux sous forme dâ□□images, tandis que lâ□□objet du mail appelle les destinataires Ã procÃ©der dâ□□urgence Ã une authentification multifactorielle, par exemple, en annonÃ§ant une Â« Mise Ã jour de la sÃ©curitÃ© 2FA (Authentification Ã deux facteurs) Â». Les destinataires sont alors invitÃ©s Ã scanner le QR code avec leur tÃ©lÃ©phone portable.

â□¢ Cette campagne a touchÃ© plusieurs secteurs stratÃ©giques, dont l'Ã©nergie, la finance, les tÃ©lÃ©communications, l'informatique, les soins de santÃ©, les transports et lâ□□industrie.
â□¢ Les pays actuellement touchÃ©s sont : les Ã□tats-Unis, le Qatar, le Danemark, la SuÃ¨de, l'Australie, l'Afrique du Sud, Abu Dhabi, le Pakistan, l'Inde, Singapour et la Chine.

**Campagne 2 : Fausse campagne dâ□□aides gouvernementales en Chine Ã base de codes QR**

Cette campagne de phishing qui utilise Ã©galement des QR codes intÃ©grÃ©s Ã des mails redirige cette fois vers un site dâ□□hameÃ§onnage copie du rÃ©seau bancaire â□□China Union Payâ□□ afin de rÃ©cupÃ©rer une aide octroyÃ©e par le gouvernement chinois.

***Plus en dÃ©tails :***

â□¢ Les mails suspects promettent des aides du gouvernement chinois qui seraient octroyÃ©es par le ministÃ¨re des finances et incitent les destinataires Ã scanner un code QR pour en bÃ©nÃ©ficier.

â□¢ Si au dÃ©part les emails contenaient une piÃ¨ce jointe Word dans lequel se trouvait le QR code, plus rÃ©cemment le QR code a Ã©tÃ© intÃ©grÃ© directement au mail de phishing.

â□¢ Les pays actuellement touchÃ©s par cette campagne sont : la Chine continentale, la RÃ©publique de CorÃ©e, Hong Kong, le Japon, les Ã□tats-Unis, l'Allemagne, la Suisse, l'Australie, l'Italie, le Royaume-Uni et l'Arabie saoudite

Dans le cadre de lâ□□utilisation croissante des QR codes Ã des fins malveillantes, Trellix a

rÃ©cemment intÃ©grÃ© un module de dÃ©tection des tentatives de phishing par le biais de codes QR dans son produit ETP. Ce module a la capacitÃ© dâ□□analyser les images (et donc les QR codes intÃ©grÃ©s Ã un mail/une piÃ¨ce jointe) ainsi que les URL associÃ©es.

Vous trouverez ***plus de dÃ©tails*** sur ces recherches et les conclusions du Centre de recherche avancÃ©e de ***Trellix*** (ARC).

Pour ***en savoir plus*** sur le dÃ©cryptage rÃ©alisÃ© par lâ□□ARC de la distribution de logiciels malveillants via Microsoft Teams orchestrÃ© par lâ□□acteur malveillant Storm-0324.