Les attaques de phishing utilisant des codes QR capturent les informations d'identification de l'utilisateur

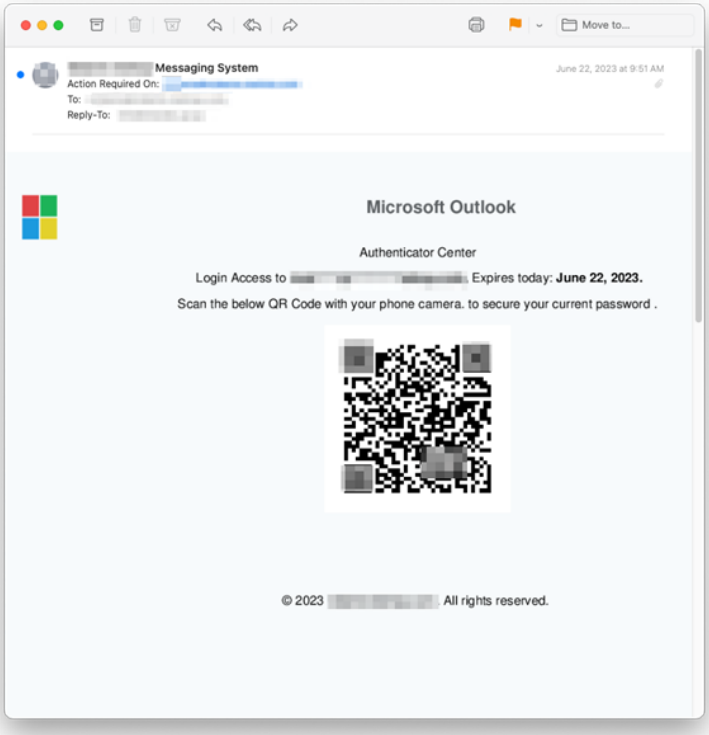
Stu Sjouwerman ⁝

Utilisant une nouvelle tournure pour contourner la détection des solutions de sécurité, les cyberattaques utilisent maintenant des codes QR que vos utilisateurs ne reconnaîtront pas comme quelque chose de suspect.

Les auteurs de menaces ont besoin de moyens d'amener un utilisateur à interagir avec un contenu malveillant – qu'il s'agisse d'une pièce jointe, d'un lien ou d'un appel téléphonique, il doit y avoir du contenu dans un e-mail qui fournit à l'utilisateur victime sa prochaine étape.

Juste derrière cela se trouvent les solutions de sécurité qui ont utilisé l'analyse de ces pièces jointes, le suivi des liens jusqu'à leur fin, etc. dans le but de fournir à l'utilisateur et à son organisation une première couche de défense pour arrêter ces attaques avant qu'elles ne commencent.

Une nouvelle méthode d'attaque de phishing repérée par les chercheurs en sécurité d'Inky comprend l'utilisation d'un code QR, incitant un utilisateur victime à prendre une photo de l'image et à accéder à la page de connexion usurpée qui en résulte.



Source: Inky

C’est insidieux pour un certain nombre de raisons, dont deux sont évidentes immédiatement:

- Je ne connais aucune solution de sécurité capable de suivre une URL basée sur un code QR pour déterminer si l’URL résultante est malveillante ou non.
- Il déplace l’action réelle de menace vers un autre appareil, en particulier un appareil qui dispose de beaucoup moins de protections que le point de terminaison d’un utilisateur.

Mais c’est aussi gênant, car *qui prend une photo d’un code QR pour se connecter à son courriel, etc. au lieu de simplement cliquer sur un lien.*
Malgré ce manque de raisonnement quant à la raison pour laquelle cela devrait fonctionner, nous voyons que ce type d’ingénierie sociale fonctionne de toute façon, sinon les cybercriminels n’utiliseraient pas cette méthode.

Ce type d’attaque met en évidence le fait que vos utilisateurs doivent être continuellement informés par le biais d’une formation de sensibilisation à la sécurité que tout ce qui sort de l’ordinaire – en particulier quelque chose d’aussi farfelu juste pour se connecter à un site Web – doit être évité.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230718
"C'est ensemble qu'on avance"