Threat Actors Experimenting with QR Codes

The Federal Bureau of Investigation (FBI) released an advisory on cyber criminals tampering and switching legitimate QR codes. Since October 2022, the use of QR codes within phishing scams has risen. Threat actors are relying on this new tactic to reduce suspicion of victims. Operators of Emotet have used QR codes in phishing attacks to get around Microsoft's stricter macro policies. A known phishing campaign utilizing this tactic was identified as malicious actors masquerading as a parcel delivery company seeking payment. The QR code redirected victims to a site that looked identical to the legitimate business and prompted the individual to enter login credentials and financial information.

Recommendations to protect your business and employees against this new tactic:

- When scanning a QR code, verify the URL before clicking the link to be redirected. It is likely there will be typos or misplaced letters in a malicious domain name.
- Always practice caution when personnel information such as login credentials or financial information is required from scanning a QR code.
- Ensure the QR code has not been physically tampered with when scanning.
- Utilize your phone's app store to download apps rather than a QR code.
- If you are requested to make a payment through a QR code, validate with the company that the information you received is correct, or pay through the company's trusted online portal or by phone number.
- Use your phone's built in QR code scanner; do not download a QR code scanner as this increases the risk of malware being downloaded.
- If receiving a QR code from someone you know, validate the QR code with them through known contact information.

Organizations should look out for emails and websites targeting their employees utilizing QR codes. This can result in sensitive corporate data being leaked through stolen credentials. We recommend organizations provide education and training to their employees on new vulnerabilities and how to mitigate them.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.helpnetsecurity.com/2023/03/21/qr-scan-scams/?web_view=true
2. https://www.bleepingcomputer.com/news/security/fbi-warns-of-malicious-qr-codes-used-to-steal-your-money/
3. https://www.govtech.com/security/fbi-warns-that-cyber-criminals-now-using-qr-codes-for-theft#:~:text=The%20FBI%20listed%20the%20following,typos%20or%20a%20misplaced%20letter