Observed Increase in QR Code Phishing Attacks

Threat Bulletins ○ TLP:WHITE Alert ID : 9cb5e075 Sep 19, 2023, 03:12 PM

A recent uptick in threat actors delivering phishing emails laced with malicious QR codes has been observed. Quishing, also known as QR code phishing, involves sending a seemingly time sensitive email containing lures to trick the recipient into taking action and scanning an innocuous QR code. Once the recipient scans the unsolicited QR code, they are taken to a malicious website used to either download malware to the user's device or steal sensitive information.

The use of QR codes to augment malicious operations has increasingly become a common tool abused in phishing campaigns. According to security researchers, targeted attacks against firms in energy, manufacturing, insurance, technology, and financial services have been observed. These observations represent the first time that QR codes have been used in this magnitude, indicating threat actors are likely testing their effectiveness as an attack vector.

The identified malicious behavior further substantiates recent Health-ISAC member observations of similar attacks targeting their organization's personnel. Health-ISAC is distributing this communication to help raise awareness of the ongoing use of malicious QR codes leveraged in phishing campaigns and encourage organizations to assess their level of risk against this threat.

Additional Information

A QR code, or quick response code, consists of information specific to the labeled item. As the QR code is scanned, it will enable users to access the desired information embedded in the code. QR code phishing attacks attempt to trick users into scanning what seems to be a normal QR code, but in reality is a malicious code designed to compromise systems or steal sensitive data.

Threat actors use QR codes embedded in images to bypass email security tools that can scan a message for known malicious links, allowing the phishing messages to reach the target's inbox. The bulk of QR phishing campaigns contain PNG image attachments delivering Microsoft credential phishing links or phishing redirects via an embedded code using redirect URLs related to trusted infrastructure, such as Bing, Salesforce, and Cloudflare's Web3 service. Hiding the redirection URL in the QR code, abusing legitimate services, and using base64 encoding for the phishing link all help evade detection and circumvent email protection solutions.

Evidence suggests that quishing attacks have increased since the beginning of the COVID-19 pandemic as organizations transitioned into contactless transactions. Moreover, senior executives have become the primary target for quishing attacks. Quishing is specific in nature as the attack vector is limited, requiring threat actors to execute the malicious operation in a manner that targets assets with scanning capabilities, such as mobile devices. Other factors, including the likelihood that recipients scan the QR code and advance passed destination URL verification notices displayed on modern smartphones, affect the success of these attacks. As a result, to overcome these obstacles, threat actors use effective communication relative to the recipients they are targeting to increase the chances of a successful attack.

Sources

Quishing on the Rise: How to Prevent QR Code Phishing
Microsoft: Five Common QR Code Scams
Cofense: Major Energy Company Targeted in Large QR Code Phishing Campagin
Major US Energy Organization Targeted in QR Code Phishing Attack
QR Code Phishing Campaign Targets Top US Energy Company
QR Code Phishing Attacks Spread

Recommendations

As with any type of phishing, the best defense against quishing attacks is an educated user base. Enterprises should provide security awareness training that includes the following best practices:

- Never scan a QR code from an unfamiliar source.
- If you receive a QR code from a trusted source via email, confirm via a separate medium -- e.g., text message, voice call, etc. -- that the message is legitimate.
- Stay alert for hallmarks of phishing campaigns, such as a sense of urgency and appeals to your emotions -- e.g., sympathy, fear, etc.
- Review the preview of the QR code's URL before opening it to see if it appears legitimate:
    - Make sure the website uses HTTPS rather than HTTP
    - Does not have obvious misspellings and has a trusted domain; do not click on unfamiliar or shortened links.
- Be extremely wary if a QR code takes you to a site that asks for personal information, login credentials or payment.
- Observe good password hygiene by changing your email password frequently and never using the same password for more than one account.

Tactic-Techniques

● Tactic ○ Techniques

Initial Access › Phishing

Reference | References

Tech Target

Microsoft
Cofense
Bleeping Computer
Dark Reading
shrm

Tags

Quishing, QR Codes, Phishing

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

HICP:

The Health Industry Cybersecurity Practices (HICP) refer to a set of guidelines and recommendations developed by the U.S. Department of Health and Human Services (HHS) to help healthcare organizations improve their cybersecurity posture. The HICP was created in response to the increasing threat of cyberattacks and data breaches in the healthcare sector, which has been a target for cybercriminals due to the sensitive and valuable nature of healthcare data.

The HICP resources are aimed at helping healthcare organizations of all sizes, including small, medium, and large entities. It provides practical and actionable guidance for managing and mitigating cybersecurity risks in healthcare environments, with a focus on five key cybersecurity threats: ransomware, phishing, loss or theft of equipment or data, insider threats, and attacks against connected medical devices.

For Questions or Comments:

Please email us at toc@h-isac.org