ISSN: 2278-4632
Vol-14, Issue-9, No.03,September: 2024

QR CODE PHISHING: A REVIEW OF THE CURRENT ATTACKS AND COUNTERMEASURES

Sefiya Aramide Galadima, Department of Computer Science & Engineering
Vivekananda Global University Jaipur, India: e-mail: galadimasefiya@gmail.com
Dr. Manish Shrivastava, Department of Computer Science & Engineering
Vivekananda Global University Jaipur, India : e-mail: manish.shrivastava@vgu.ac.in
Dr. Gunikhan Sonowal, Department of Computer Science[3]
Galgotias University Greater Noida, India : gunikhan.sonowal@gmail.com

ABSTRACT:

QR code phishing, commonly known as "quishing," which exploits the inherent ambiguity of QR codes to conduct phishing attacks. Initially developed by Denso Wave in 1994 for manufacturing purposes, QR codes have seen a surge in usage, particularly during the COVID-19 pandemic, as businesses sought to reduce physical contact. However, this increased adoption has also led to a rise in cybercriminal activities targeting both individuals and organizations. This paper outlines various tools used in QR code phishing, including QR code generators that facilitate the creation of malicious codes, and techniques such as QRL jacking, where attackers create fake login pages to capture user credentials. Additionally, it discusses the risks associated with infected QR code readers, which can compromise mobile devices through deceptive applications.To address these threats, this paper explores several countermeasures, including machine learning models designed to detect phishing URLs and secure QR code frameworks that utilize encryption to protect sensitive data. The study highlights the importance of user awareness and education in mitigating risks associated with QR code usage. Furthermore, it identifies limitations in current detection methods and emphasizes the need for continuous updates to combat evolving threats. By providing a comprehensive overview of QR code phishing and its countermeasures, this paper aims to enhance understanding and promote safer practices in the utilization of QR code technology in an increasingly digital world.

Keywords-QR Codes, Phishing, Quishing, Cybersecurity, QRL jacking, Malicious QR codes, Countermeasures, Machine Learning, Encryption, User Awareness.

INTRODUCTION:

Quick Response codes, known as QR codes, a data encoding technique developed by Denso Wave in Japan. These two-dimensional barcodes, capable of storing vast amounts of data vertically and horizontally, have found widespread application in diverse sectors, revolutionizing various industries. From retail and marketing, where QR codes streamline product tracking and customer engagement, to logistics and supply chain management, where they facilitate efficient item identification and inventory control, QR codes have become indispensable tools. Moreover, their versatility extends to personal identification, travel documents, and digital payments, enhancing convenience and security in daily life. Industries like healthcare, education, and entertainment have also embraced QR codes for tasks such as patient records, event ticketing, and interactive content delivery. By allowing for brandspecific customization, QR codes serve as valuable marketing assets, enabling businesses to create a strong visual identity and connect with their target audience in innovative ways[1].

Contains Data
Contains Data

Figure 1: Quick Response (QR) Code [2]

As illustrated in Figure 2, each component of a QR code contributes to its scannability. The most prominent features are the three identical finder patterns, located at the top-left, top-right, and bottom-left corners. These red squares, composed of a 3x3 matrix of black modules surrounded by white modules, assist the scanner's software in identifying the QR code and its orientation, allowing for scanning from any angle.

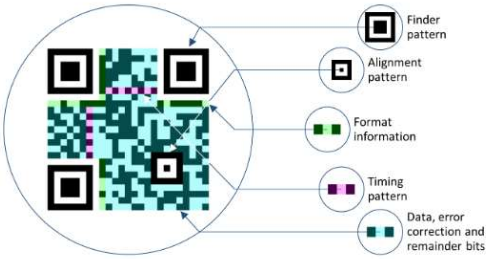

Figure 2: Structure of a version 2 QR Code [3]

Separating the finder patterns from the rest of the code are the white separators, each one pixel wide. These separators enhance the scanner's readability. The timing pattern, consisting of alternating black and white modules, enables the software to determine the width of a single module.Alignment patterns, included from version 2 onwards, aid in decoding distorted images. The format information, adjacent to the separators, stores data about the selected masking pattern and error correction level.The data is encoded as a bit stream and stored in 8-bit segments known as codewords. Error correction codewords, also 8-bit long, are included to protect against data corruption. Finally, the remainder bits, used when data and error correction bits cannot be divided into 8-bit codewords without a remainder, fill any empty spaces.

QR codes are categorized into 40 versions, each with a unique configuration of black and white dots, or modules. Version 1 consists of a 21x21 module grid, while version 40 has a 177x177 module grid. As the version number increases, the size of the grid expands by four modules on each side[4].

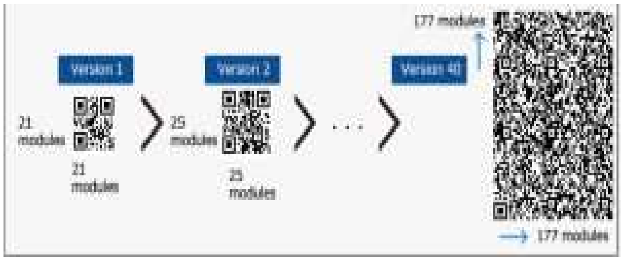

Figure 3: Image of QR Code Versions 1,2 and 40 [4]

This review will shed light on the severity of the QR code phishing attacks and the limited research done on combatting this phishing attack vector that has gained prominence. Section II discusses the current vulnerabilities of the QR Code which threat actors continue to exploit currently. Section III looks at the tools employed by the phishers to deceive unsuspecting QR users. Section IV looks at the current countermeasures and proposed methodologies. Section V concludes the paper.

QR CODE PHISHING :

QR code phishing, also known as ‘quishing’ exploits the lack of immediate clarity of QR codes to launch phishing attacks. This QR code technology facilitates seamless interaction between mobile devices and websites or printed materials. QR code generation is primarily accomplished through web-based software applications. These platforms offer intuitive interfaces and extensive customization capabilities. To create a QR code, users simply input desired data, such as URLs, contact information, or images, into a QR code generator. Additional customization options, like adding company logos or specific colors, are often available. Once generated, the QR code can be easily downloaded for subsequent use[5]Notably, QR codes eliminate the need for manual URL or contact information entry, streamlining user experience [6]. QR codes, requiring a scanner app or built-in camera functionality on most mobile devices, offer a convenient way to access information. The simplicity of QR code creation and dissemination has made them a target for criminal activities.Attackers employ various methods to distribute malicious QR codes. These deceptive codes can be surreptitiously applied as stickers overlaying legitimate ones on billboard advertisements. Phishing emails may also embed QR codes, tricking recipients into scanning them [7]. Alternatively, attackers might strategically place these codes in public spaces, exploiting people's natural curiosity to prompt scanning. When a victim scans a malicious QR code, it can trigger various harmful consequences. The code might embed malware that automatically downloads upon scanning, compromising the victim's device [8]. Alternatively, it can redirect the user to a phishing website designed to steal credentials, sensitive information or malware downloads.As highlighted by [9],attackers can also employ verifier impersonation, creating fraudulent QR codes that mimic legitimate login interfaces. When scanned, these deceptive codes can trick users into unknowingly providing their credentials to attackers, leading to unauthorized access. The ease of generating and distributing QR codes makes this a potent phishing tactic. Additionally, attackers could intercept the communication between the user and the Identity Provider (IdP) when a QR code is scanned. If compromised, the QR code can redirect the user to a phishing site or capture sensitive authentication data. Replay attacks can occur when an attacker captures a valid QR code and attempts to reuse it, posing a significant risk if the QR code lacks built-in expiration or validation features.

TOOLS UED IN QR CODE PHISHING:

A. ***QR Code Generators***

QR code generators offer a versatile functionality, allowing users to create these matrix barcodes for diverse applications, from directing users to websites and displaying text to initiating actions like sending emails or connecting to Wi-Fi, QR codes have become an important communication tool. QR codes inherently direct users to the embedded webpages, bypassing the traditional address bar displayed in web browsers. This can pose a security risk as users might not critically examine the actual URL upon landing on the webpage. Phishing websitescan exploit this behavior by meticulously mimicking legitimate sites. Notably, the generation of such malicious QR codes is facilitated by various QR code generating programs, highlighting the ease with which cybercriminals can exploit this technology for phishing attacks. Notably, the generation of such malicious QR codes is facilitated by various software programs, highlighting the ease with which cybercriminals can exploit this technology for phishing attacks.

B. ***QRL Jacking***

In a qrljacking attack [10], a malicious actor creates a fake login page disguised as a legitimate one through a QR code. Unsuspecting users who scan the code unknowingly enter their login credentials on this fraudulent page, compromising their accounts to the attacker.

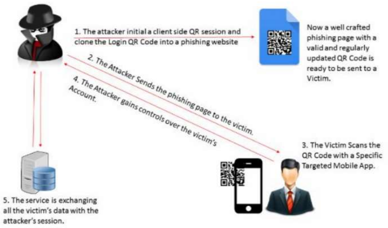
1. The attacker initial a client side QR session and clone the Login QR Code into a phishing website
Now a well crafted phishing page with a valid and regularly updated QR Code is ready to be sent to a Victim.
2. The Attacker Sends the phishing page to the victim.
4. The Attacker gains controls over the victim's Account.
3. The Victim Scans the QR Code with a Specific Targeted Mobile App.
5. The service is exchanging all the victim's data with the attacker's session.

Figure 4:Qrljacking[11]

ISSN: 2278-4632
Vol-14, Issue-9, No.03,September: 2024

Qrljacker [11] automates the hijacking of login sessions by exploiting weaknesses inherent in QR based mechanisms.

Qrljacker generates malicious QR codes that, when scanned by an unsuspecting user, grant the attacker unauthorized access to the victim's account. A typical attack scenario involves social engineering or strategically placed codes to trick the victim into scanning a malicious QR code generated by Qrljacker. This scan triggers session hijacking, granting the attacker full access to the compromised account. This tool is primarily an open-source framework designed for educational and penetration testing purposes, exposing vulnerabilities in QR based authentication systems employed by web services, but threat actors have adopted it and been able to use it for their malicious intents. It allows attackers to hijack QR code-based login sessions to gain unauthorized access to user accounts.

C. *Infected QR Code Readers*

The rise of QR codes across physical environments e.g., printed advertisements and digital platforms e.g., social media, email has raised a corresponding rise in user demand for QR code reader applications on mobile devices. While some devices come equipped with built-in camera functionalities for QR code scanning, others lack this capability, necessitating the download of third-party software. This scenario presents a vulnerability exploited by malicious actors who distribute fake QR reader apps [12][13]. These deceptive applications often masquerade as legitimate QR code readers [14] on app stores like the Play Store. To further enhance their legitimacy, some fake apps might request seemingly reasonable permissions. However, the true malevolent intent lies in their ability to request and exploit unnecessary permissions, potentially granting them control over unsuspecting victims' mobile devices. This can lead to a range of criminal activities, including data theft and the propagation of further malware. Another tactic employed by malicious actors involves the monetization of free apps through in-app advertising, by adding an ad-SDK (software development kit) at the end of the app's development, which installs new apps onto the victim's device upon installation[15].

COUNTERMEASURES:

Amoah and Hayfron-Acquah [16] propose a machine learning model to combat QR code phishing ('quishing'). Their framework ingests a collection of both phishing and legitimate URLs for pre-processing and analysis. Features specific to phishing URLs are identified and leveraged to differentiate malicious from benign ones. Tokenization is performed through count vectorization, essentially extracting words from URLs and converting them into tokens. These features and tokens are then fed into machine learning algorithms for phishing URL classification. The study concludes that logistic regression provided the strongest baseline accuracy, serving as a benchmark for future comparisons and highlighting the potential benefits of employing larger datasets in further research.The paper identifies several limitations, including the reliance on machine learning techniques like Naive Bayes and logistic regression, which may not effectively counter zero-day phishing attacks due to the transient nature of phishing URLs.

The paper[17] proposed a proactive, secure, real-time computational intelligence barcode scanner implementation called BarCI. This model utilizes a multilayer perceptron artificial neural network (MLP-ANN) as the best classifier for detecting malicious URLs embedded in QR codes. BarCI is designed to efficiently and effectively detect malicious links in real-time, providing users with notifications regarding the safety of the URLs before they visit them. The model BarCI, while effective in detecting malicious URLs, has limitations including its dependency on the quality of the dataset used for training, which may not encompass all potential malicious patterns. Additionally, it focuses solely on URL lexical properties without analyzing the actual web page content, potentially missing threats embedded within the site itself. The model's performance may also be influenced by the evolving nature of web attacks, requiring continuous updates and retraining to maintain accuracy against new types of threats.

The paper[18] proposes a model called Secured QR (SQR) to enhance the security of QR codes. This model utilizes the Advanced Encryption Standard (AES) algorithm to encrypt the data stored in the QR code. The process involves generating a 128-bit key from a password, which is used to encrypt the data before embedding it in the QR code. When the QR code is scanned, the user must enter the correct password to generate the same key, allowing the encrypted data to be decrypted and accessed. This approach aims to protect sensitive information from various security threats such as phishing and manipulation, ensuring that only authorized users can retrieve the original data. The proposed Secured QR (SQR) model has some limitations, primarily related to time complexity, as it requires additional processing time for both generating and scanning QR codes compared to traditional methods. This extra time may be a drawback for users who prioritize quick responses during scanning. Additionally, the model relies on the correct entry of a password to decrypt the data, which could pose a challenge if users forget or enter the wrong password. Despite these limitations, the model effectively enhances security against various threats.

CONCLUSION :

QR codes have emerged as a transformative technology across various industries, enhancing efficiency and user engagement. However, their increasing prevalence has also given rise to significant security concerns, particularly in the form of QR code phishing attacks. These attacks exploit the inherent ambiguity of QR codes, allowing cybercriminals to deceive users into revealing sensitive information or downloading malicious software. This paper has highlighted the various methods employed in QR code phishing, including the creation of fraudulent codes, strategic placement in public spaces, and the use of malicious applications. It has also discussed the importance of user awareness and education as a primary defense against such threats. To combat QR code phishing effectively, a multi-faceted approach is necessary. This includes the implementation of advanced security measures, such as machine learning models for URL classification, the use of secure QR code readers, and the promotion of best practices for verifying the legitimacy of QR codes. As QR codes continue to play a vital role in modern communication and transactions, it is imperative for users, businesses, and developers to remain vigilant and proactive in safeguarding against potential threats. By fostering a culture of security awareness and employing robust countermeasures, we can harness the benefits of QR codes while minimizing the risks associated with their misuse.

REFERENCES:

[1] A. Singh, V. Verma, and G. Raj, “A novel approach for encoding and decoding of high storage capacity color QR code,” in *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, IEEE, 2017, pp. 425–430.

[2] P. Kieseberg*et al.*, “QR code security,” in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010, pp. 430–435.

[3] K. S. C. Yong, K. L. Chiew, and C. L. Tan, “A survey of the QR code phishing: the current attacks and countermeasures,” in *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, IEEE, 2019, pp. 1–5.

[4] denso wave incorporated, “Information capacity and versions of the QR code,” qrcode.com. Accessed: Sep. 16, 2021. [Online]. Available: https://www.qrcode.com/en/about/version.html

[5] D. Lau and Beardscript, “How to Create a QR Code Reader for Your Mobile Website,” sitepoint. Accessed: Jan. 02, 2022. [Online]. Available: https://www.sitepoint.com/create-qr-code-reader-mobile-website/

[6] A. Y. Alnajjar, S. Manickam, M. Anbar, S. Al-saleem, and O. Elejla, “TrustQR: A New Technique for the Detection of Phishing Attacks on QR Code,” *Adv Sci Lett*, vol. 22, no. 10, pp. 2905–2909, Oct. 2016, doi: 10.1166/asl.2016.7102.

[7] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, “QR code security: A survey of attacks and challenges for usable security,” in *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2*, Springer, 2014, pp. 79–90.

[8] P. Rastogi, “5 Ways to Identify A Fake QR Code to Avoid Scams and Frauds,” Gadgetstouse. Accessed: Feb. 02, 2022. [Online]. Available: https://gadgetstouse.com/blog/2022/01/28/spot-fake-qr-code-to-avoid-frauds/

[9] S. Mukhopadhyay and D. Argles, “An Anti-Phishing mechanism for single sign-on based on QR-code,” in *International Conference on Information Society (i-Society 2011)*, IEEE, 2011, pp. 505–508.

[10] Sayaala, “QRL Jacking,” Infosec. Accessed: Mar. 26, 2022. [Online]. Available: https://www.infosecinstitute.com/resources/hacking/qrl-jacking/

[11] owasp, “Qrljacking,” owasp.org. Accessed: Jun. 26, 2022. [Online]. Available: https://owasp.org/www-community/attacks/Qrljacking

[12] G. Dixon, “Popular QR code scanner app infected with malware,” reviews.org. Accessed: Jan. 27, 2022. [Online]. Available: https://www.reviews.org/au/mobile/qr-code-scanner-app-malware/

[13] P. Lall, “Millions Affected by Malware Attributed to Android Barcode-Scanning App,” mcafee.com. Accessed: Jun. 27, 2022. [Online]. Available: https://www.mcafee.com/blogs/mobile-security/millions-affected-by-malware-attributed-to-android-barcode-scanning-app/

[14] K. Komando, “QR code app caught hiding malware – Check your phone! ,” komando.com. Accessed: Jun. 27, 2022. [Online]. Available: https://www.komando.com/tips/software-and-apps/qr-code-app-hiding-malware/

[15] J. Xiung, “This QR code scanner was infected by malware after an update, over 10 million Android devices are affected,” soyacincau. Accessed: Jun. 27, 2022. [Online]. Available: https://soyacincau.com/2021/02/10/this-qr-code-scanner-was-infected-by-malware-after-an-update-over-10-million-android-devices-are-affected/

[16] G. Awuah Amoah and H.-A. J.B., “QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing),” *Int J Comput Appl*, vol. 184, pp. 34–39, Mar. 2022, doi: 10.5120/ijca2022922425.

[17] H. Wahsheh and M. Al-Zahrani, “Secure Real-Time Computational Intelligence System Against Malicious QR Code Links,” *International Journal of Computers, Communications and Control*, vol. 16, no. 3, pp. 1–9, Jun. 2021, doi: 10.15837/ijccc.2021.3.4186.

[18] N. Goel, A. Sharma, and S. Goswami, “A way to secure a QR code: SQR,” in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, IEEE, 2017, pp. 494–497.