- June 18, 2024

Rising Wave of QR Code Phishing Attacks: Chinese Citizens Targeted Using Fake Official Documents

CRIL Has Analyzed The Increase In QR Code Phishing Campaigns Using Microsoft Word Documents As A Lure To Target Chinese Citizens.

Key Takeaways

- There has been a significant increase in QR code phishing attacks in 2024, with cybercriminals exploiting the technology to steal personal and financial information.
- Threat Actors (TAs) are using office documents embedded with QR codes, redirecting users to fraudulent websites designed to harvest sensitive data.
- A recent phishing campaign targets Chinese citizens by impersonating the Ministry of Human Resources and Social Security, using QR codes in fake official documents
- The MS Word document is disguised as an application notice for receiving labor subsidies above 1000 RMB.
- The TA employs a Domain Generation Algorithm (DGA) to create phishing URLs, making detection and blocking more challenging.
- Users are tricked into providing bank card details and passwords under the guise of identity verification and authentication processes.

Overview

In the evolving landscape of cyber threats, a new vector has emerged, exploiting the ubiquitous QR codes to lure unsuspecting users into phishing traps. Recently, there has been a significant uptick in

malicious documents embedded with QR codes, which, when scanned, redirect users to fraudulent websites designed to steal personal information.

In 2024, QR code phishing attacks have increased, highlighting a growing trend among cybercriminals to exploit this seemingly benign technology to direct users to malicious websites or initiate malware downloads. Notably, the Hoxhunt Challenge revealed a 22% increase in QR code phishing during the latter part of 2023, and research by Abnormal Security shows that 89.3% of such attacks are aimed at stealing credentials.

The increase in QR code phishing can be attributed to several factors. First, the widespread adoption of QR codes, especially during the COVID-19 pandemic, has made them a convenient target. QR codes became popular for contactless transactions, menus, and information sharing, making users more accustomed to scanning them without hesitation. This familiarity creates a false sense of security, making it easier for cybercriminals to exploit.

Second, QR codes can easily mask the destination URL, making it difficult for users to verify the legitimacy of the site they are being redirected to. Unlike traditional hyperlinks that display the URL, QR codes provide no immediate indication of their destination, increasing the likelihood of successful phishing attempts.

Furthermore, the integration of QR code scanners into smartphones and the rise of mobile payment systems have expanded the attack surface. Threat actors can embed malicious QR codes in physical locations, emails, or online documents, broadening their reach and making it harder to track and mitigate these attacks.

Recently, Cyble Research and Intelligence Labs (CRIL) came across a campaign utilizing Microsoft Word documents for QR code-based phishing attacks targeting individuals in China. These files, which are suspected to be distributed via spam email attachments, masquerade as official documents from the Ministry of Human Resources and Social Security of China.

Figure 1 – MS Word file containing QR code

The document presents itself as a notice for applying for labor subsidies, claiming to offer subsidies above 1000 RMB for registered bank cards. It directs users to use their mobile phones to scan a QR code for authentication and to receive the subsidy.

We identified several additional Word files linked to QR code phishing attacks impersonating a Chinese government agency, with most of these files having zero detection rates. The goal of these QR code phishing attacks is to collect financial information, including credit card details and passwords.

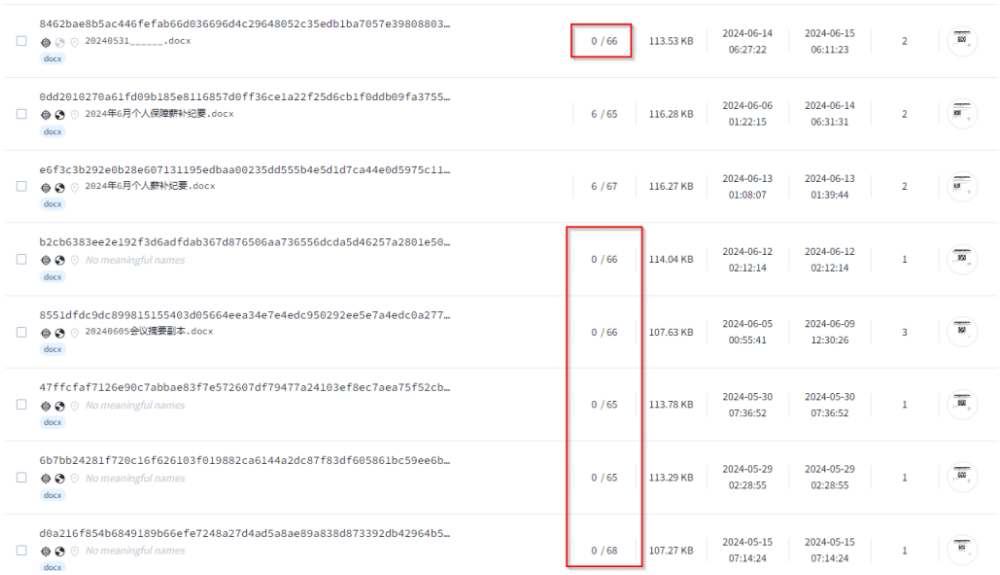

Figure 2 – Similar MS Word file with zero detection

A similar campaign was identified in January 2023 and documented by Fortinet, where QR code phishing attacks impersonated a different Chinese government agency to target users. This campaign has resurfaced, once again targeting users in China to collect financial information.

Phishing Activity Details

When the user scans the QR code in the Word document, they are directed to the link "hxxp://wj[.]zhvsp[.]com". Upon visiting this link, they are redirected to a URL with the subdomain "tiozl[.]cn", which has been generated using a Domain Generation Algorithm (DGA). This URL hosts a phishing site that impersonates the Ministry of Human Resources and Social Security of the People's Republic of China.

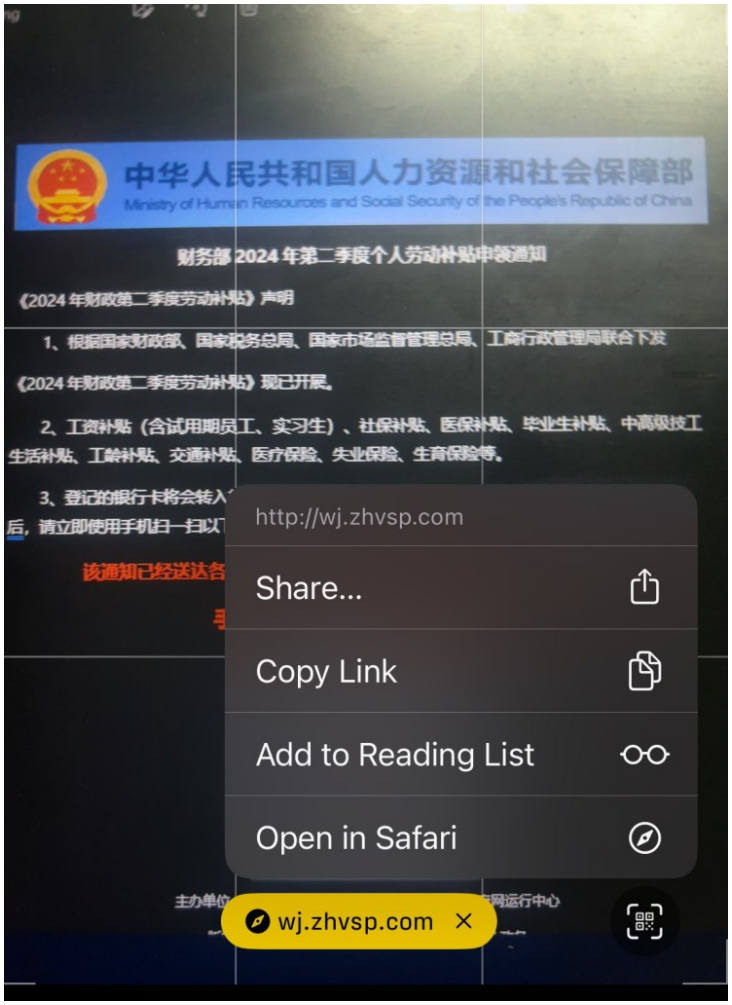

Figure 3 – QR code displays phishing link upon scanning

The domain “tiozl[.]cn” is hosted on IP address “20.2.161[.]134”, which is also associated with five additional domains. Among these, four are subdomains of “tiozl[.]cn” and one is a subdomain of “zcyyl[.]com”. All these domains are linked to the same campaign, hosting similar phishing sites, suggesting a massive distribution effort. The domains are listed below:

- 2wxlrl.tiozl[.]cn
- op18bw[.]tiozl.cn
- gzha31.tiozl[.]cn
- i5xydb[.]tiozl.cn
- hzrz7c.zcyyl[.]com

Upon further investigation of phishing sites, we observed that the SHA-256 fingerprint of an SSH server host key (bc5d98c0bfaaf36f9a264feefa572e97607eadff6ab70251ddaf59df486d7787) associated with the IP address “20.2.161[.]134” has been utilized by 18 other IPs. These IPs share the same ASN, AS8075, and are located in Hong Kong. Below is a list of IPs hosting URLs with a similar pattern linked to this phishing campaign.

- 52.229.166.225
- 20.2.16.132
- 52.184.66.142
- 52.175.13.206
- 20.2.200.161
- 20.255.100.54
- 52.229.190.40
- 20.255.73.44

The landing page entices the user by displaying a dialogue box on a phishing website, offering a labor subsidy. When the user proceeds to claim the subsidy, they are redirected to another page that prompts them to enter personal information, including their name and national ID, as shown in the figure below.

After the user provides their name in Chinese and their national ID, the website presents a page with information about card binding, which is required for further payment processing following a successful application.

As the next step, the user is prompted to enter their card details, including the bank card number, phone number, and bank card balance. This information is requested under the guise of identity verification, but the threat actor will collect it to perform unauthorized transactions.

After collecting the entered card details, the phishing site displays a dialogue box indicating that the information is being verified and requests the user to wait for 2-3 minutes before proceeding to the next step.

The phishing site presents a dialogue box with instructions that, as part of the verification process, the user will need to provide their bank card password for authentication. It then loads a phishing page prompting the user to enter their withdrawal password, as shown in Figure 9 and Figure 10.

We suspect this withdrawal password is the same as the payment password used by banking users for domestic credit card transactions. By using the harvested bank card details along with the collected withdrawal password, the threat actor can conduct unauthorized transactions, leading to financial loss for the user.

Conclusion

The rise in QR code phishing attacks highlights cybercriminals' growing sophistication and adaptability. By exploiting the widespread use of QR codes, especially post-pandemic, these attacks

effectively lure users into divulging sensitive financial information. The recent campaign targeting Chinese citizens underscores the threat's severity, as malicious actors use seemingly official documents to gather card details and passwords, leading to significant financial losses. This trend underscores the importance of heightened vigilance and robust security measures to protect against such evolving threats.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Only scan QR codes from trusted sources. Avoid scanning codes from unsolicited emails, messages, or documents, especially those claiming to offer financial incentives or urgent actions.
- After scanning a QR code, check the URL carefully before proceeding. Look for signs of legitimacy, such as official domains and secure connections (https://).
- Install reputable antivirus and anti-phishing software on your devices. These tools can help detect and block malicious websites and downloads.
- Stay informed about phishing techniques and educate others about the risks associated with QR codes. Awareness is a crucial step in preventing successful phishing attacks.
- Use 2FA for your online accounts whenever possible. This adds an extra layer of security, making it harder for attackers to gain unauthorized access.
- Keep your operating systems, browsers, and applications up to date with the latest security patches. This helps protect against known vulnerabilities.
- Consider using QR code scanner apps that include security features, such as checking the URL against a database of known malicious sites before opening it.
- Review your bank and credit card statements regularly for unauthorized transactions. Report any suspicious activity to your bank immediately.

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
8462bae8b5ac446fefab66d036696d4c29648052c35edb1ba7057e39808803fa 71f4eaebbd9cccaa2a9ca2575dbf12a420482394 c31837a9c1ed6a540782f63d4f196b11	SHA256 SHA1 MD5	MS word file

hxxp://wj[.]zhvsp[.]com hxxp://ks.ozzlds[.com hxxp://rc[.]nggznm.cn hxxp://ry[.]ngghznm.cn hxxp://web[.]ioomk-1.sbs	URL	URL after scanning QR codes
2wxlrl.tiozl[.]cn op18bw[.]tiozl.cn gzha31.tiozl[.]cn i5xydb[.]tiozl.cn hzrz7c.zcyyl[.]com web.innki-1[.]sbs web[.]oiiunm-4.sbs web.liooik-2[.]sbs web[.]jneuz-4.sbs web[.]yoopk-4.sbs web[.]ioomil-4.cfd web.miiokn-4[.]sbs wweb[.]muuikj-6.sbs web.ikubzn9-1[.]sbs inb[.]yhuiz-5.sbs admin.yhuiz-4[.]sbs web[.]otuz1-2.sbs fmqe9s[.]ikknzjd.cn wqegi8.skqkkdm[.]cn nhfvhi.skqkkdm[.]cn k7pnec.skqkkdm[.]cn qerxjj[.]uehsht.cn vjym48.uehsht[.]cn y1hc3j.rygwnr[.]cn ofwdfq[.]qttsgzhcn.cn g97hwf[.]okdmzjcm.cn thrrai.okdmzjcm[.]cn f8lhst[.]okdmzjcm.cn xzlky6.uhhsjzn[.]cn rcgali.uhhsjzn[.]cn azure.5atrade[.]cf ahgfus[.]pixqd.cn sfdncx.lppdzna[.]cn cjpb1j[.]lppdzna.cn cqy8ek.poozpd[.]cn fyo63q[.]wiiaks.cn l9qxrr.wiiaks[.]cn yzfpmj[.]wiiaks.cn zcqgtm[.]wiiaks.cn inwp8n.ekksjcm[.]cn xicfpx[.]ekksjcm.cn	Domain	Redirected Phishing domain
8462bae8b5ac446fefab66d036696d4c29648052c35edb1ba7057e39808803fa 0dd2010270a61fd09b185e8116857d0ff36ce1a22f25d6cb1f0ddb09fa375511 e6f3c3b292e0b28e607131195edbaa00235dd555b4e5d1d7ca44e0d5975c111e	SHA256	MS Word file

b2cb6383ee2e192f3d6adfdab367d876506aa736556dcda5d46257a2801e508c 8551dfdc9dc899815155403d05664eea34e7e4edc950292ee5e7a4edc0a277e9 47ffcfaf7126e90c7abbae83f7e572607df79477a24103ef8ec7aea75f52cb25 6b7bb24281f720c16f626103f019882ca6144a2dc87f83df605861bc59ee6b14 d0a216f854b6849189b66efe7248a27d4ad5a8ae89a838d873392db42964b595		

Source: Cyble