Top Characteristics of a QR Code Phishing Email

DECEMBER 6, 2023

SHARE THIS ARTICLE

Facebook Twitter LinkedIn

By Max Gannon

QR codes in the phishing threat landscape are a major topic of interest and worth paying particularly close attention to, despite how insignificant they were earlier this year. QR codes change the attack vector and enable threat actors to trick victims into using their personal phones which are typically not protected by enterprise controls and are therefore more vulnerable. As campaigns using QR codes grow in size and complexity it is important to track not just the QR codes themselves, but also the context of the emails delivering the QR codes. Some of the emails bearing QR codes deliver them in attached files like HTM, PDFs, or Word documents. Others use images embedded in the email or QR codes rendered from external sources. The more recent QR code campaigns utilize a wide range of email themes rather than the earlier campaigns that primarily used multi-factor authentication as a lure for victims. When it comes to the URLs from the actual QR codes, there are many different characteristics such as their purpose as a legitimate redirect, a link shortener, etc. or the fact that one of the redirect pages makes use of a cloud flare captcha. This report discusses each of these pieces of context in more detail.

Key Points

- The most common characteristics associated with the credential phishing chains from URLs embedded in QR codes were, in order of popularity, captcha, multi-factor authentication (MFA), and URLs that had an open redirect to a credential phishing page.
- The most common sources for QR codes were, in order of popularity, embedded in the email, attached PDF, attached HTM, and attached DOC.
- The subjects of QR code bearing emails were more likely to be MFA themed, contain a date, and contain personally identifiable information that was redacted, than regular credential phishing emails. In particular, the emails were 28% more likely to contain MFA themes than regular credential phishing emails.
- The types of domains of URLs embedded in QR codes were, in order of popularity, malicious or compromised, legitimate, QR code related, and a standard link shortener service.
- Of the legitimate domains of URLs embedded in QR codes the most popular were, in order of popularity, Bing, Google, Baidu, and 5 other minor sources.

Accompanying Characteristics

Cofense Intelligence tags Active Threat Reports (ATRs) with certain tags. These tags indicate when a campaign has certain characteristics, like a QR code or captcha. By looking at the tags on reports with QR codes we are able to see the information in Figure 1. Of note is that while campaigns with captcha were the most popular for both QR Code based reports and all credential phishing reports, the MFA tag was the least popular among all credential phishing reports but a close second among QR Code reports. This reinforces MFA as a primary theme for QR codes as expected, however, the fact that only 29% of QR code reports had the multi-factor authentication tag indicates that in fact, QR code emails may be more diverse than they would first appear. The large portion of QR code emails that utilize a captcha code at some point in their delivery chain is an indicator that even when automated systems start scanning QR codes and following links they will still likely be stymied before recording the entire chain.

Reports with the open redirect tag showed up in only 13% of QR code based emails. Although this is significantly higher than the 0.78% of all credential phishing emails, it is still unusually low given how many QR codes seem to have some form of redirection. This is because the open redirect tag is not focused on any open redirect but rather specifically on open redirects abusing known services such as Baidu or Google.

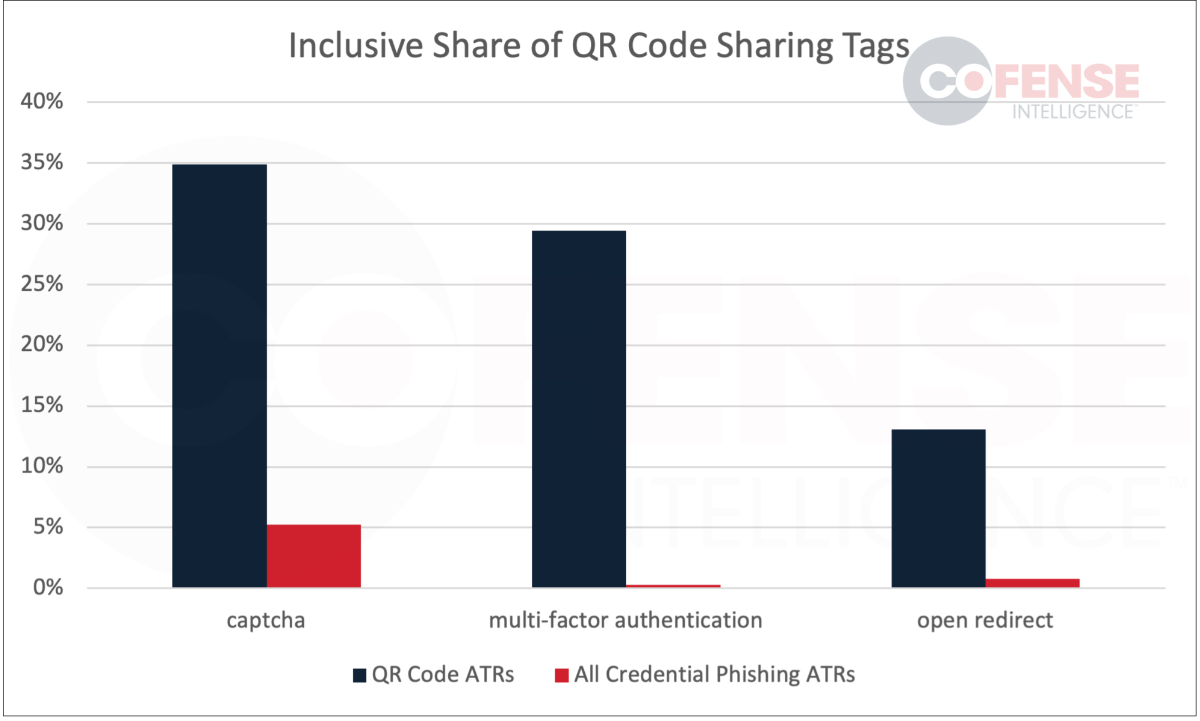

Figure 1: Inclusive share of QR code sharing tags.

QR Code Image Sources

QR codes are primarily delivered via images embedded in emails. However, as automated systems have become better at spotting and scanning embedded QR codes, threat actors have already sought out alternatives. One of the more clever alternatives currently only appears in less than 3% of campaigns but if it continues to be effective, it will likely appear in more. Threat actors abuse a little-known Google API to generate a QR code that is referenced as an external image in the email or HTML attachment. The URL is:

hxxps://chart[.]googleapis[.]com/chart?chs=300×300&cht=qr&chl=<URL>

This URL generates a QR code with a link to whatever the threat actors include in the <URL> portion of the path. For example, hxxps://chart[.]googleapis[.]com/chart?chs=300×300&cht=qr&chl=hxxps://cofense[.]com/knowledge-center-hub/real-phishing-email-examples/ gives the QR code in Figure 2.

Figure 2: QR code generated from hxxps://chart[.]googleapis[.]com/chart?chs=300×300&cht=qr&chl=hxxps://cofense[.]com/knowledge-center-hub/real-phishing-email-examples/

Given that most external images are ignored by SEGs when scanning emails, it is likely that automated systems will ignore it when scanning for QR codes. Additionally, by generating a QR code dynamically rather than using one that is attached or embedded threat actors further increase their chances of bypassing SEGs.

The more commonly adopted responses to automated scanning of embedded QR code images is to use an attached file with a QR code embedded in it. As can be seen in Figure 3, out of all of our QR code-based campaigns only 17% make use of attachments but this number is likely to grow. Currently, at 12%, PDFs make up the most common attachment containing an embedded QR code. This is likely because it is easier to disguise a QR code embedded in a PDF than in a Word document or HTM file when it comes to systems that automatically extract an attachment’s content. PDFs peaked in July but continued to be popular in August and are expected to make a comeback when high volume campaigns resume in the new year.

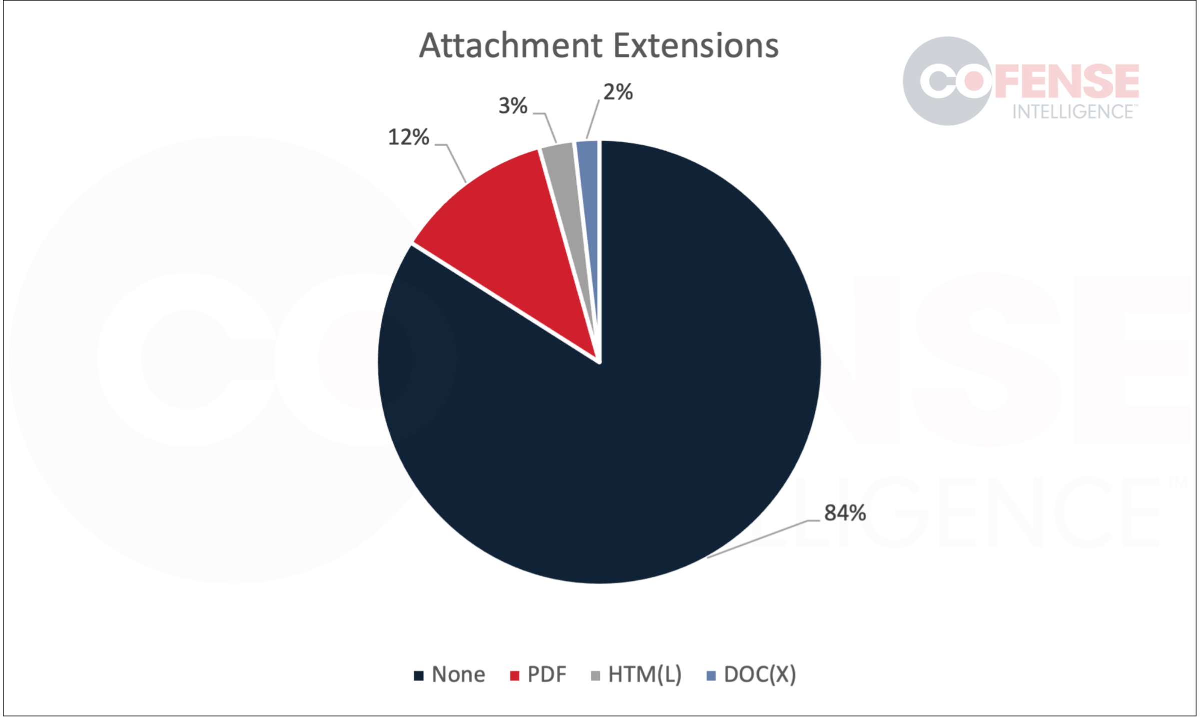

Figure 3: File extensions on attachments containing QR codes.

When looking at the actual names of the attachments there were some interesting trends. For attached HTM files, over 70% of the attachments had the name ePrints.htm or some variation thereof. For the attached PDF files 50% of them had some variation of a finance theme and only 40% of them were MFA themed. Additionally, 53% of them had to have some portion of their file name redacted within ThreatHQ due to personally identifying information being present. This is in keeping with the higher-than-normal number of QR code-based campaigns that had to have their subjects redacted.

Subjects Of QR Code Campaigns

The subjects of emails delivering QR codes, seen in Figure 4, were mostly in line with expectations. Unsurprisingly, emails with MFA themes in their subjects were much more common than the same themes in the subjects of general credential phishing emails. MFA themes making up 29% of QR code emails makes sense as that matches up with the data from the tagged reports. What is surprising is that only 29% of emails themed around QR codes, which are typically associated with MFA setups, had MFA related subjects or bodies. As mentioned earlier, this indicates that QR code emails are more varied than they would first appear, but it also indicates that threat actors may believe employees are likely to see QR codes in correspondences not related to MFA setups.

Seeing more personally identifiable content requiring redaction in subjects also makes sense as QR code emails are more likely to be delivering information that appears to be specifically relevant to the recipient's company. The only surprising result is that there is an 11% difference in subjects that have a date in them. QR code emails with subjects with dates in them have themes ranging from MFA to salary reports to overdue documents. The biggest differences were that QR code subjects did not have dated voicemail or any kind of audio recording themes but had an abundance of salary related notifications with deadlines.

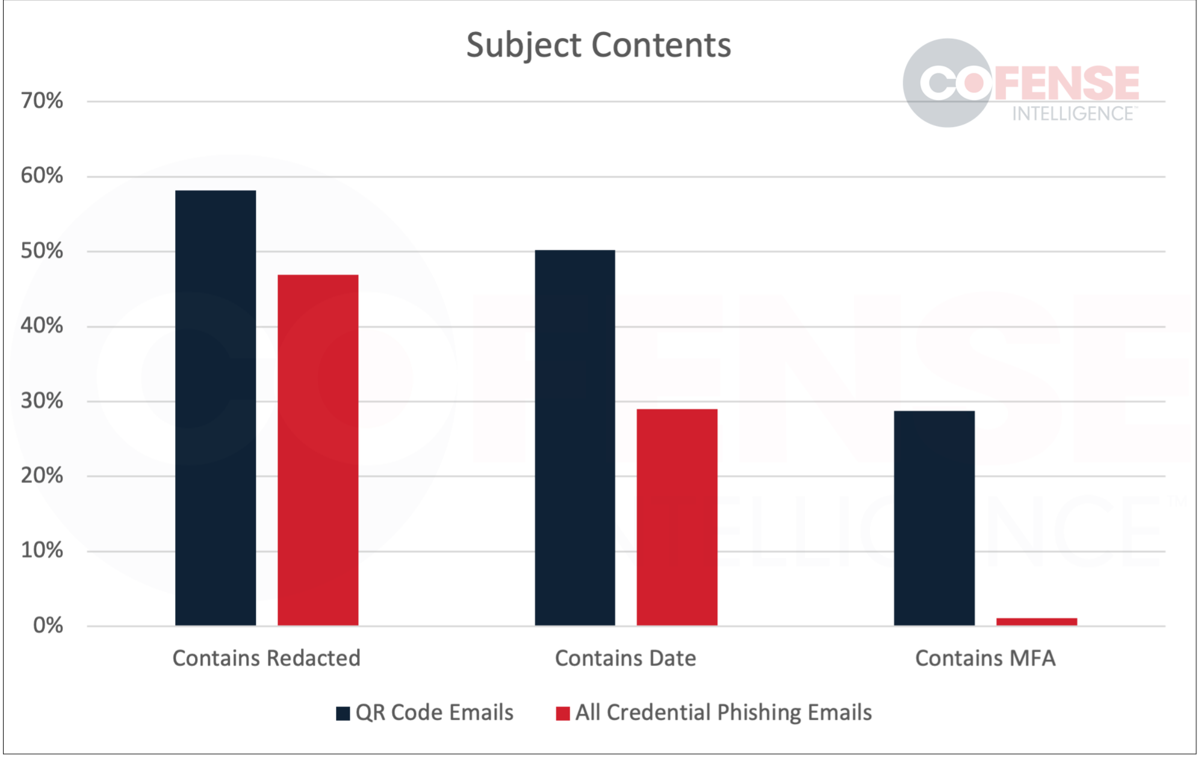

Figure 4: Contents of subjects of QR code bearing emails versus all credential phishing emails.

URLs Embedded in QR Codes

One of the most interesting, and information rich, aspects of QR codes are the URLs that are embedded in the QR codes. An important characteristic of a URL embedded in a QR code is its purpose. This covers whether the embedded URL is legitimate, a link shortener, is part of a QR code generation platform, or is directly malicious or compromised. Breaking down the legitimate URLs used for redirection a bit more we will see that Bing is actually the most abused.

Domain Type

The domain of a URL embedded in a QR code can be one of several different types which can be seen in Figure 5. The first is a legitimate domain which is used for redirection such as Bing. The second is a link shortener like Bitly which, although technically legitimate, is often viewed less favorably by automated defenses. The third is that the domain can be QR code related. Specifically, this means that the domain belongs to one of the QR code domain shorteners services like qrco[.]de which purports to track statistics about the scanning camera and device. The final is the general category of malicious or compromised domains.

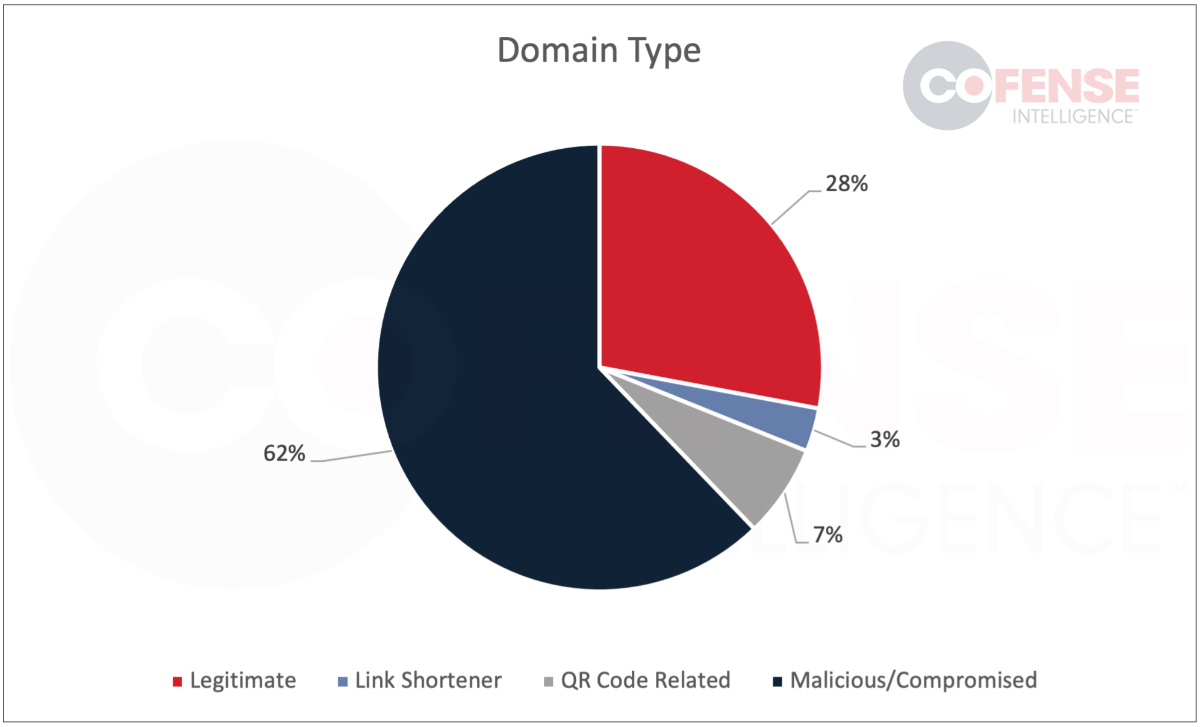

Figure 5: Type of domain in URLs embedded in QR codes.

Legitimate Redirection

Legitimate domains used for redirection make up the second largest portion of domains seen in QR code phishing campaigns. This makes sense as, while they are not as necessary as when URLs are directly embedded in emails, they can still provide a false sense of legitimacy when users view the embedded URL when the QR code is scanned. As can be seen in Figure 6, the most common one was Bing followed by Google. Bing was often seen being used to redirect in a way that obfuscated the redirection URL so that users were only able to view “hxxps://bing[.]com/ck/a?!&&p=” followed by encoded content. Google was more likely to reveal the malicious URL victims were being redirected to, however, the displayed URL was likely so long that when victims scanned the QR code on their phone and looked at the URL preview they were not able to see the end of the path where the malicious URL is listed.

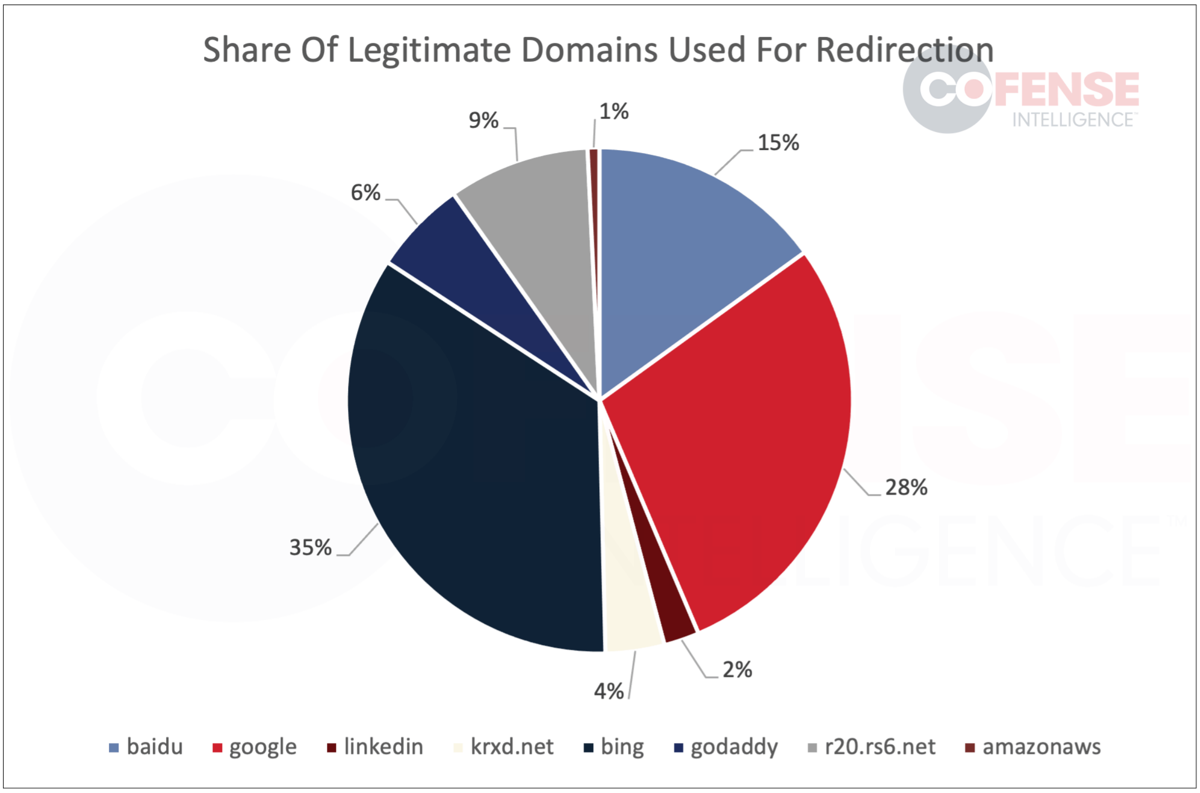

Figure 6: Legitimate domains used for redirection which are embedded in QR codes.