Major Energy Company Targeted in Large QR Code Phishing Campaign

Archived: 2026-04-05 22:53:30 UTC

By: Nathaniel Raymond

Beginning in May 2023, Cofense has observed a large amount of QR code phishing campaigns targeting the Microsoft credentials of users from a wide array of industries. The most notable target, a major Energy company based in the US, saw about 29% of the over 1000 emails containing malicious QR codes.

Other top 4 targeted industries include Manufacturing, Insurance, Technology, and Financial Services seeing 15%, 9%, 7%, and 6% of the campaign traffic respectively. Most of the phishing links were comprised of Bing redirect URLs, but other notable domains include krxd[.]com (associated with the Salesforce application), and cf-ipfs[.]com (Cloudflare's Web3 services). Learn more about Web3 abuse. Historically, QR codes are not a popular choice due to the limiting nature of how QR codes are interacted with.

However, they have several advantages over a phishing link embedded directly in an email. QR code delivery methods have a much better chance of reaching an inbox as the phishing link is hiding inside the QR image, while the QR image is embedded inside a PNG image or PDF attachment.

Key Points

- A campaign has been observed delivering emails that spoof Microsoft security notifications that contain a PNG or PDF attachments in emails that ask a user to scan a QR code. The most notable target of the campaign is a major US Energy company.
- The average month-to-month growth percentage of the campaign is more than 270%. The overall campaign has increased by more than 2,400% since May 2023
- QR Codes are not historically popular as they are limited in the way a user can interact with them. Scanning a QR code is limited to the mobile device used, which provides a user with a sneak peak of the link embedded in the QR code and verifies if the user wishes to go to the link.
- Scanning a QR code on a mobile device puts the user outside the protections of the enterprise environment.
- Cofense has not historically seen large malicious campaign(s) utilizing QR codes. This may indicate that malicious actors are testing the efficacy of QR codes as a viable attack vector.

The Energy Company Campaign

While the QR code phishing campaign affected multiple industries, a major US-based Energy company was the focus. Most of the phishing emails contain PNG image attachments delivering Microsoft credential phishing links or phishing redirects via an embedded QR code, with the majority of them being Bing redirect URLs.

Email lures came in the form of updating account security surrounding 2FA, MFA, and general account security. The Energy company saw 29% of the overall volume, however the company saw 81% of the campaign in which Bing redirect URLs were being used.

The Bing Redirect URL

A major contribution to the campaign is the Bing redirect as shown in Figure 2. While Bing is a legitimate domain owned by Microsoft, Bing redirect URLs that were originally meant for marketing purposes, can also be used for malicious purposes.

Figure 2 highlights portions of the Bing URL to include the marketing section, and the malicious section, and where the phishing link is encoded into base64. However, the link showcased below is a sample structure of most URLs seen in QR code phishing campaigns.

This tactic of encoding phishing links in redirects and sending the victim's email with it is not new. What is important to note is that aside from hiding in QR codes, threats are abusing a trusted domain to carry attacks. Abusing trusted domains, using obfuscation tactics, coupled with hiding the URLs inside QR codes embedded into a PNG or PDF attachment, helps ensure that emails bypass security and make it into inboxes.

Figure 2: Bing Redirect URL

Over 2,400% Increase in Malicious QR Code Phishing Volume

Although the overall campaign was comprised of many domains, Bing redirect URLs shared the largest portion of the campaign, comprising 26% of the overall campaign phishing links used in the QR Codes, followed by the Salesforce application URL taking 15%. Figure 3 shows the top 5 domains used in the campaign to distribute credential phishing.

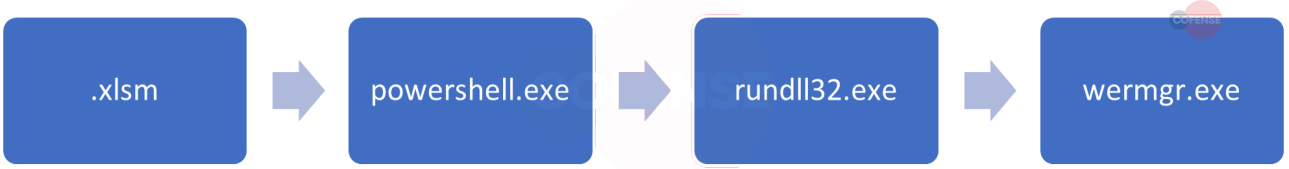

Figure 3: Top 5 Domains Used in QR Code Campaign

Even though the Energy company itself was observed to be the focus of the threats, the Energy sector was a major focus for the campaign overall as demonstrated by Figure 4 followed by manufacturing. The increase in volume in the Energy sector was due to a large 2-day campaign in late June as shown in Figure 6.

Figure 4: Volume by Industry

From the beginning of the campaign in May, we have seen an average month-to-month increase of roughly 270% with May to June being the biggest jump of around 500% and around 155% from June to July as shown in Figure 5. Since May, there has been an increase by more than 2,400% in QR code phishing in emails.

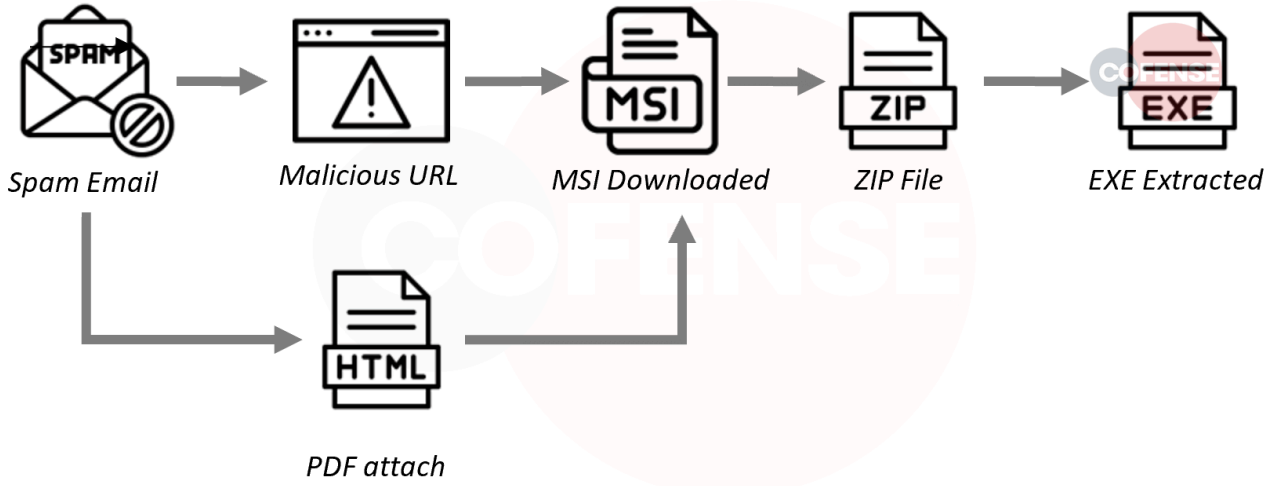

Figure 5: Month-To-Month Volume

Trend Analysis

While it is impossible to predict the future of a phishing campaign, we can look at the historical trend beset by the campaign itself. Figure 6 shows an upwards trend starting from May to August with a major outlier in late June where this can indicate testing and deployment phases.

Cofense observed that the outlier in question was the bulk of the emails with QR codes targeting the major Energy company. Around the middle of July begins a multi-weeklong campaign that has targeted a multitude of industries including the continuance of targeting the Energy sector.

Figure 6: Volume Trends by Date

The Problem with QR Codes

Although QR code phishing is advantageous for getting malicious emails into user's inbox, they may fall short of being efficient in getting the user to the phish. This shortcoming is due to the nature of QR codes as they need to be scanned by an image capturing device. While online scanners exist and will show you where the QR code is going, the user is prompted to scan the code with their mobile device's camera as seen in Figure 1.

However, modern mobile devices also show the embedded artifact and ask the user to verify the URL before launching a browser to the link which allows the user to see where the link is going before accepting. This is showcased in Figure 7 where a mobile device shows that the QR code in question leads to cofense.com.

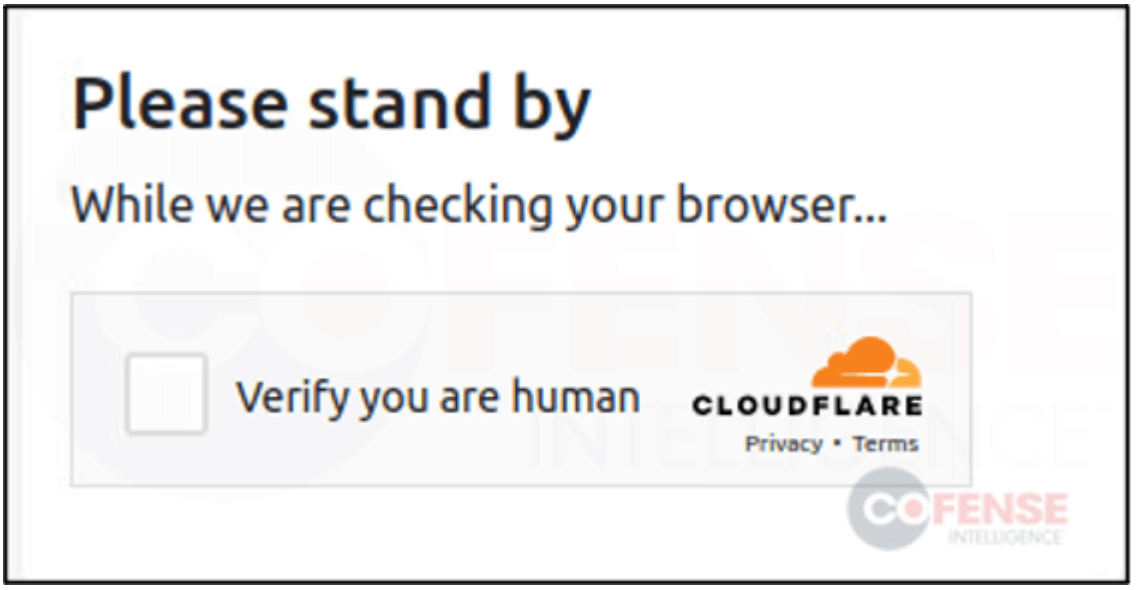

Figure 7: QR Code Verification

The QR Code Phishing Solution

While QR codes do have legitimate reasons to be used, malicious actors also have reasons to use them as well. The first is that QR codes with malicious artifacts can reach inboxes and the malicious link is hidden in the QR code. Secondly, they can be embedded into other images to disguise the QR code as an image attachment, or embedded image in a PDF file.

While automation such as QR scanners and image recognition can be the first line of defense, it is not always guaranteed that the QR code phishing will be picked up. Especially if it's embedded into a PNG or PDF file.

Therefore, it is also imperative that employees are trained not to scan QR codes in emails they receive. This will help ensure that accounts and businesses security remain safe.
