Phishing campaign used QR codes to target large energy company

By Jonathan Greig

Published: 2023-08-16 · Archived: 2026-04-06 01:15:37 UTC

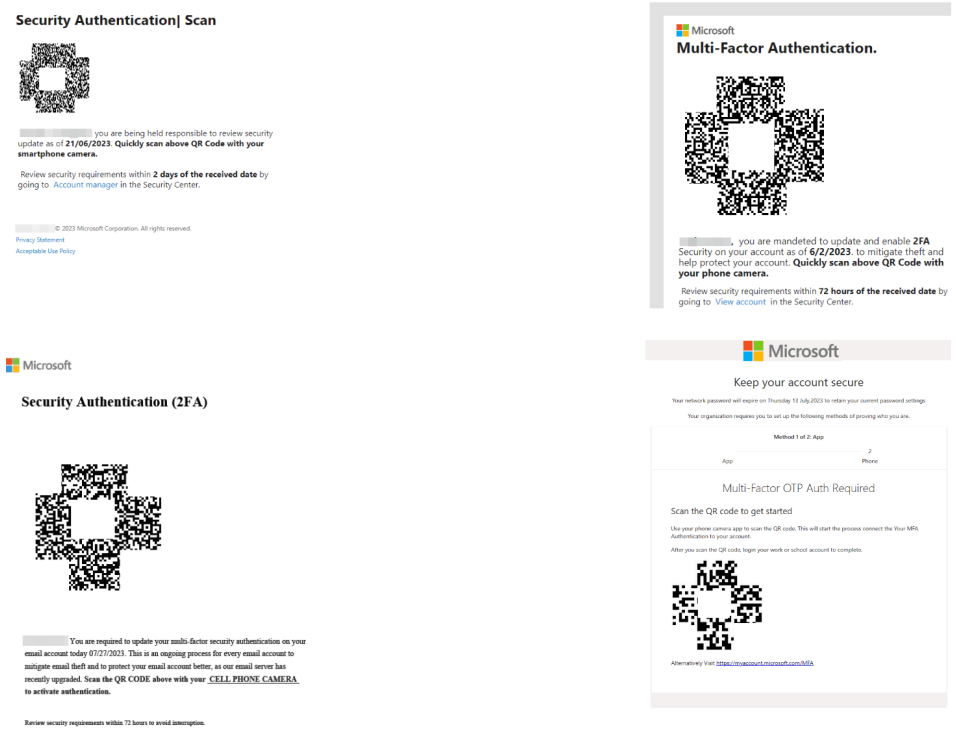
Cybersecurity researchers uncovered a large phishing campaign using malicious QR codes with the hopes of acquiring Microsoft credentials at several targets, including a major U.S. energy company.

QR codes have become widely adopted since the onset of the COVID-19 pandemic, with thousands of restaurants and businesses replacing physical menus and guides with the machine-readable images that pull up webpages containing the same information.

But hackers have been quick to exploit the trend, launching campaigns that spread fake QR codes to steal user information.

Cybersecurity firm Cofense released a new report on Wednesday identifying a campaign that began in May targeting a wide array of industries. The hackers sent thousands of emails containing malicious QR codes to companies, which took users to a Microsoft credential phishing page.

The report's author, Cofense cyber threat intelligence analyst Nathaniel Raymond, told Recorded Future News that they were unable to attribute the campaign to a specific threat actor but found similarities to a previous campaign that used tools from companies in Russia.



Examples of QR codes used in the campaign. Image: Cofense

“This campaign initially appeared in small numbers but eventually grew to a volume far beyond what is normally seen in campaigns of a similar level, making it stand out,” Raymond said, adding that the number of emails sent out has grown by about 270% each month.

Raymond declined to name the energy company that was attacked but said that about 29% of the emails they tracked as part of the campaign were sent to the energy company.

The researchers said the manufacturing industry saw another 15% of the emails while insurance, tech and financial services firms also saw sizable portions of the campaign’s traffic.

Raymond noted that it is likely other organizations are being attacked by the threat actors with the same campaign but their percentages are based on the emails Cofense observed. The emails lured victims by appearing to relate to account security updates. The QR code took victims to a fake Microsoft page asking for credentials.

The researchers noted that QR codes have not typically been used by hackers at this scale, but threat actors may be testing out the method because of its effectiveness in comparison to more traditional links embedded in most phishing emails.

They noted that QR codes 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.”

Most mobile devices are not regulated by employers, putting them outside of the protection of the enterprise environment, the researchers explained.

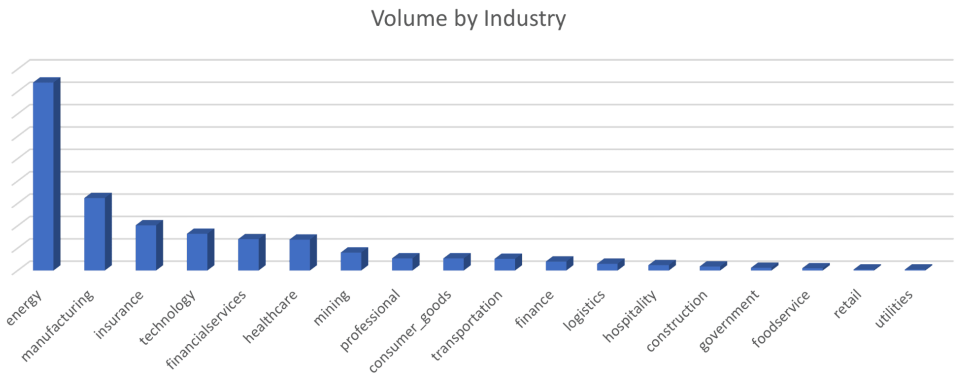


Figure 4: Volume by Industry

Image: Cofense

The hackers also encoded the phishing links in redirects so that when victims flash their camera over the QR code, the link that appears looks legitimate.

SafeBreach CISO Avishai Avivi said the report represented an interesting development in how malicious actors operate, noting that the pandemic has made QR codes ubiquitous.

“Users, by now, are used to responding to these codes by simply pulling their smartphones and scanning the code. This action is done with little concern about whether these codes are malicious,” Avivi said.

“This tendency to scan any QR code presented to the user raises concerns as some applications, including security controls, also use QR codes to accomplish different tasks. These tasks include confirming identity, enrolling an

authenticator application, and more. A malicious code can bypass or divert the user to perform an action they did not intend to execute."

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
