Threat Advisory

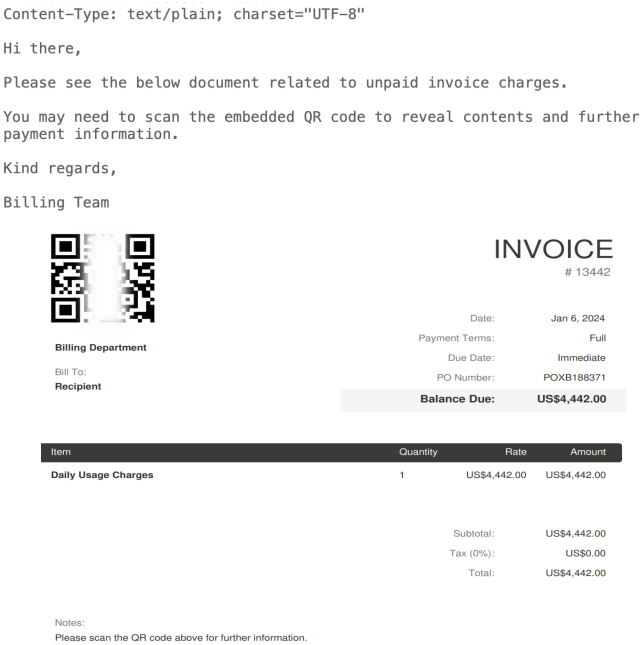
Microsoft Login - QR Code Phishing Scam

Origin

Corrata recently detected a Microsoft-based Phishing Threat. The phishing link originated in a document related to an unpaid invoice.
The document contained redacted information and the user was prompted to scan a QR code to reveal the redacted content.

The reliance on a QR code, rather than a conventional URL, represents a significant evasion technique. QR codes are frequently not subjected to the same level of scrutiny by existing phishing protection systems. In addition, use of a QR code makes it less likely that the user will be alerted to the phish by reading the domain name. And finally, because the user uses their smartphone to open the URL, any desktop best web-filtering system is bypassed.

A preview of the document is below. Note the QR code has been masked to prevent accidental engagement with the phishing site.



Content-Type: text/plain; charset="UTF-8"

Hi there,

Please see the below document related to unpaid invoice charges.

You may need to scan the embedded QR code to reveal contents and further payment information.

Kind regards,

Billing Team

INVOICE
13442

Billing Department

Bill To:
Recipient

Date:	Jan 6, 2024
Payment Terms:	Full
Due Date:	Immediate
PO Number:	POXB188371
Balance Due:	**US$4,442.00**

Item	Quantity	Rate	Amount
Daily Usage Charges	1	US$4,442.00	US$4,442.00

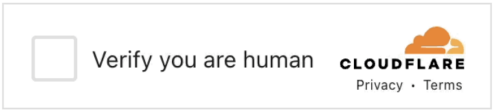
Subtotal:	US$4,442.00
Tax (0%):	US$0.00
Total:	US$4,442.00

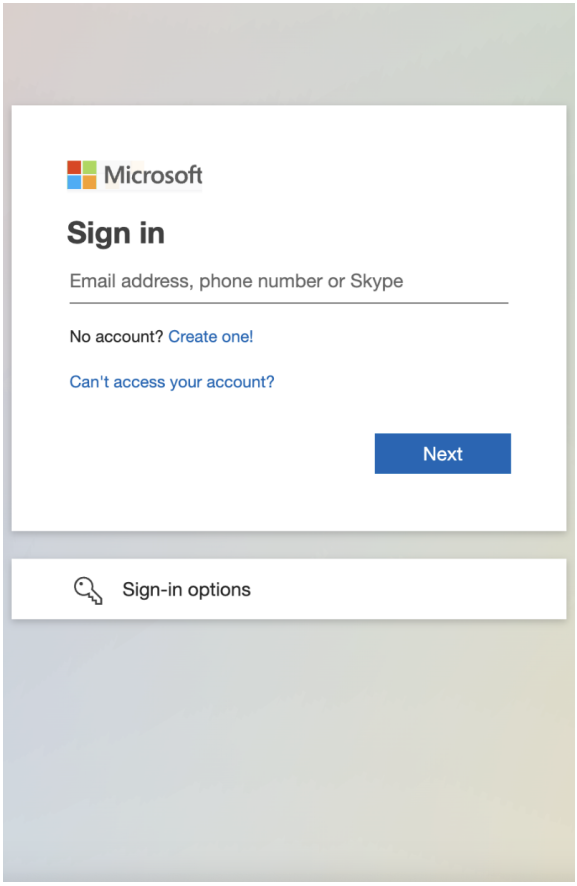
Notes:
Please scan the QR code above for further information.

Document Received via Email

Contents

The phishing campaign in question begins with an initial redirection of the user to a CloudFlare verification page. Attackers commonly employ this strategy to impede both dynamic and static analysis techniques. By mandating a human interaction checkpoint, the attackers increase the likelihood that their phishing site remains undetected by automated security systems designed to identify and assess potential threats.





Detection

As it was a newly registered domain which was not yet analysed, Corrata classified it as Zero Day Protection and blocked the threat.
After analysis, Corrata re-classified the domain as Phishing.

LAST ↓	EVENTS	ACCOUNTS	DEVICES	THREAT	NAME	ACTIONS
12/01/2024, 21:34:06	6	1	1	ZERO DAY PROTECTION	REDACTED	

Conclusion

Attackers are increasingly utilising a gap in phishing protection - mobile devices. This is apparent with their usage of QR codes which force the user to use a mobile device to scan, evading usual methods for detecting malicious websites.

With Corrata running on the device such threats are detected and blocked as a matter of course.

Corrata Team.