Project: QR Code Phishing Attempt

Clay Jones

Objective:

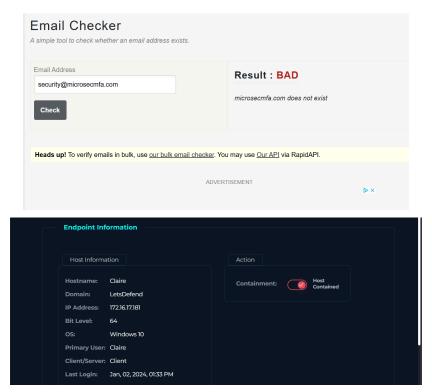
The SIEM alert recently went off and it detected a phishing attempt via QR code. Determine whether or not this was a phishing attempt or not.

The alert:

| EventID: | |
|-----------------------|--|
| Event Time : | Jan, 01, 2024, 12:37 PM |
| Rule: | SOC251 - Quishing Detected (QR Code Phishing) |
| Level: | |
| SMTP Address : | 158.69.201.47 |
| Source Address : | security@microsecmfa.com |
| Destination Address : | Claire@letsdefend.io |
| E-mail Subject : | New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA) |
| Device Action : | |

As you can see, the email was allowed through.

The Response:



I checked to see if the email was legitimate and it was not. I also would have deployed the email in a virtual machine and used a recognized phishing email scanner. Due to this, I contained the computer that was affected.

Threat Feed



Afterwards, the IP of the sender was added to the threat feed.

Lessons Learned

To prevent this from happening again, I would:

Stress User Education

Deploy email in a VM to check if domain matches QR code link

Enter the email into a domain checker

Look at threat feeds