Vishing, Smishing

This lesson will cover two different phone-based phishing attacks, vishing and smishing. These attacks move away from the conventional delivery method of electronic mail and utilize mobile phones and social engineering tactics to target users by voice or text messages. These events are typically uncommon, and the security team probably doesn't have visibility over company-owned phone text messages, and will not have access to employee-owned mobile phone text messages.

SMISHING

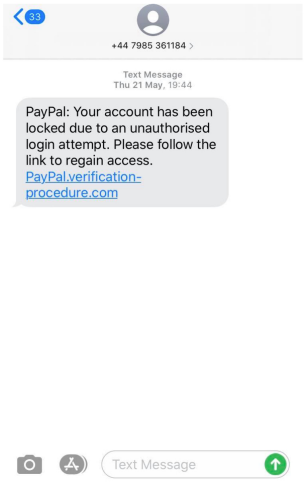
Smishing is a kind of phishing attack, where the attack vector is through a text message or SMS. Below would be a profile that a smishing attack could follow:

Victim: This type of phishing can often be sent in bulk to multiple cell phones/message services at one time, resulting in a generic victim profile.

Target: Most often these attacks are after Personal Identifiable Information (PII) or banking or financial information such as credit card details, known as Payment Card Information (PCI), therefore there is no specific target group.

Ways to Defend: The best way to defend is user security awareness training and education, as well as being diligent in clicking links or completing actions sent from unknown phone numbers or impossible phone numbers (such as 4291). Many services provide "do not text/anti-bot" lists which can help mitigate some of these threats as well.

Below is an example of a fake PayPal-themed attack via text message, which may seem legitimate at a glance, but the URL is actually: `PayPal.verification-procedure[.]com` (the domain is "verification-procedure[.]com", instead of "PayPal.com")



VISHING

Similar to smishing, vishing is a kind of phishing attack, where the attack vector is through a phone call. This method relies heavily on the social engineering aspect of phishing by having direct voice-to-voice contact with their victim. Below would be a profile that a vishing attack could follow:

Victim: The victim of vishing attack often are people in the organization that would have access to sensitive information, often being one or two levels below the "C" level executive

Target: Most often these attacks go after financial information or corporate accounts that could give them access to the network.

Ways to Defend: As with smishing one of the best ways to defend is user security awareness training and education, especially when it comes to sharing passwords with someone without verification, but blocking auto callers helps decrease vishing attempts as well. Having internal authorization codes would also trip up an external malicious actor, as they wouldn't know the private codes. Separation of duties can also work to reduce the number of people that have the appropriate access to complete actions such as processing payments.

SOCIAL ENGINEERING CTF

DEFCON 2017 hosted a "Social Engineering Capture The Flag" where participants had to perform open-source intelligence collection and then use phone calls to try and gain information from the willing target organization. You can watch a great 15 minute video on how this SECTF went, including a real example of Vishing that worked to retrieve lots of information. Social Engineering call starting at 03:11, with on-screen captions that explain the different social engineering tactics that were used.

Previous Topic
Back to Lesson
Next Topic