Jackson Warren

Jeremy Bergen

CSCI 370

9/10

Week 2 Assignment: Attacks

1. Attack Scenario – Phishing Attacks
   1. Goals
      1. Gain personal information about people, usually credit card info, logins, or confidential information.
      2. Gained via misleading entities asking for information through text, email, or call.
      3. Users click on said misleading links, and gain unwanted malware or give up information unknowingly.
   2. Resources Required:
      1. Skills/Training: In general, most phishing attacks don’t require a large amount of skill unless the target has very adept security or knowledge. If the hacker has decent malware they can install upon the attack, skill level doesn’t need to be major. Research on the target, creating a believable phishing scam, and determination to output the scam to the target is the hard part. Once the target has fallen into the trap, the installed malware takes over or the believable false website lures people to give up their information.
      2. Personnel: Can range from one to many.
      3. Equipment: Beyond normal technology needed, the hacker will need decent to advanced malware and coding skills to create believable links, as well as some ability to cover their tracks and remain hidden.
      4. Preparation Time: Varies. Most likely, not long at all. Unless the attack is for a specific target, no time would be required except to set up a believable attack with malware. If target is specific, studying the target could take a few days/weeks.
      5. Timing constraints: Only constraints would be the use of the personal info gathered. If this info is used, the unauthorized use of a credit card or any other personal info could get flagged therefore blocking access to use this info.
   3. How it Happens:
      1. Targets see an add they believe could be useful or intriguing, they click on the scam advertisement, and maybe follow a link within the text/email. This link may bring them to a false website, where they give up personal information thinking they are giving it to a trusted source.
   4. Collateral Results:
      1. Phishing attacks in general are isolated to the user giving up their info. The hacker can obviously get caught creating issues for them, but collateral results would usually be somewhat isolated.
   5. Mitigation Steps:
      1. Avoid any emails/texts/calls that are from a company you are not involved in, offer you things for free, or seem scam-like.
   6. References:
      1. Ewing, S. (2020, August 20). *4 cyber Incident scenarios you should exercise and test*. Delta Risk. https://deltarisk.com/blog/4-cyber-incident-scenarios-exercise-test/.
      2. *What is phishing: Attack techniques & scam examples: Imperva*. Learning Center. (2020, June 17). https://www.imperva.com/learn/application-security/phishing-attack-scam/.
2. Attack Case Study – COVID-19 Relief Payment Scam
   1. Overview:
      1. In November 2020, an SMS message was sent out to US citizens asking them to go to a website to receive their relief-funds. They then went to an IRS.gov impersonating website, where they were asked for personal information, and bank information.
   2. Perpetrator:
      1. There were many parties that utilized this pandemic as a chance to phish information from people. No specific group was responsible and many are still at large and unknown.
   3. Attack Scenario:
      1. Multiple parties, all utilizing the pandemic, used phishing attacks on people looking for their relief payments as a chance to make them a victim by impersonating the IRS.gov websites.
   4. Risk Management:
      1. Categorize the Information System:
         1. The main information systems targeted is personal devices. Any weaknesses on these personal devices to detecting phishing scams will prove to be a weakness. Having firewalls stopping fraudulent websites, or knowing to avoid phishing scams is the only real solution.
      2. Security controls:
         1. Security will depend on the user. Some will have little to no protection from phishing attacks, while other systems may be capable of detecting this. Downloadable software can always be added as well. Once attacks have happened and been flagged, it is up to the company being impersonated to notify people of the scam, such as the IRS and COVID relief funds phishing attack. Otherwise, detecting these scams can be hard to do. Sending out emails and SMS messages is not illegal, and therefore, detecting it before it has been reported can be somewhat complex. Most detection/software is dependent on the user to do themselves, rather than a protection from another source. However, corrective security controls could be very advantageous to help victims recover.
   5. References:
      1. *IRS warns about COVID-19 economic Impact payment fraud*. Internal Revenue Service. (n.d.). https://www.irs.gov/compliance/criminal-investigation/irs-warns-about-covid-19-economic-impact-payment-fraud.
      2. Daughney, T. (2021, January 21). *2020'S top 5 phishing Scams exposing Hackers' questionable MORALS – and how to hold strong against them*. Security Magazine RSS. https://www.securitymagazine.com/articles/94408-s-top-5-phishing-scams-exposing-hackers-questionable-morals-and-how-to-hold-strong-against-them.