Jason Lindsley
MIS 5211 – Introduction to Ethical Hacking
Analysis Report 1 – Reconnaissance Exercise

Beneficial Bank – Philadelphia, PA

Company Overview

Beneficial Bank is operated by Beneficial Mutual Bancorp, Inc., which is headquartered at 1818 Market St. Philadelphia, PA. The company has 57 retail branches located in Pennsylvania and New Jersey. They offer products and services in personal and business retail banking, lending, wealth management, insurance. The company was founded in 1853 and now employees approximately 950 people. The hold approximately $5 billion in total assets.

Leadership Profile

A profile of the leadership team was performed to understand what information was publically available about key members of the leadership team. This profiling exercise revealed that the company posted the name, photo, e-mail address, and direct phone number for 41 members of their leadership team on the corporate public website – www.thebenefical.com. Additional searches on social media platforms such as LinkedIn and Facebook revealed that other information about the Sr. Leadership team was publically available, including hobbies, education history, mutual contacts, and prior work history. This information, combined with the contact information posted on the company's website, significantly increases the risk and probability of successful spear phishing and social engineering campaigns.

Technical Profile

A technical profile was performed to identify key systems and 3rd party technology vendors used by Beneficial Bank. Job postings on the company's website assisted in identifying some of the systems that are in use. One job posting revealed that Beneficial Bank uses IBM's Bankway – "an integrated core banking solution with multiple delivery channels and integration points," per IBM's website. Job postings also revealed the names of suspected homegrown or custom applications that are in use at Bankway (e.g. BRM / CLX). Information about these core systems could be useful in identifying a company's "crown jewels" when conducting a network scan.

A "whois" query on thebeneficial.com revealed the employee name and contact information for the site administrator that registered the domain. Additional LinkedIn searches confirmed this individual was the SVP of IT at Beneficial Bank and provided links to other key contacts within Beneficial Bank's IT Department – including the VP of Operations and the VP of Information Security.

DNS lookups on thebeneficial.com returned an IP address that ultimately resolved to an IP range owned by Fidelity National Information Services (also referred to as FIS). A Google search returned several News Releases announcing that Beneficial Bank entered into an IT Managed Services agreement with FIS in December 2013 to reduce costs through outsourcing its servers, network, desktop support, and telecom.

Jason Lindsley
MIS 5211 – Introduction to Ethical Hacking
Analysis Report 1 – Reconnaissance Exercise

Conclusion

The most significant risk identified during this reconnaissance exercise is the company's exposure to spear phishing and social engineering threats. This decision to post team leader contact information could have been made to appeal to customers and business partners, however it significantly increases the risk of these attack vectors. Management should consider removing team leader contact information from the Company website immediately and increase employee training and awareness of phishing threats.

The technical information obtained would also be valuable in further reconnaissance activities such as wireless network scanning and social engineering. The company should consider implementing corporate policies that prohibit employees from listing the specific IT systems and services used by Beneficial Bank in public forums, such as job postings and press releases.