Rayzone Group

CASE STUDY

A Comprehensive Security Overview of Banking Operations

OBJECTIVES

One of the largest banks in the United States turned to RayzSecurity, Rayzone Group's cybersecurity division, for a unique and comprehensive security overview of the bank's operations.

CHALLENGES

The bank encountered a multitude of challenges, with confidential information stored on most devices categorized into well-defined areas such as intellectual property (IP), personally identifiable information (PII), and adherence to payment card industry data security standards (PCI DSS).

Numerous functions within this institution execute sensitive operations using this data, exposing them to potential vulnerabilities. These vulnerabilities span a spectrum of threats, ranging from identity theft to industrial espionage and from the illicit brokerage of sensitive information to the manipulation of fiscal transactions.

Attackers have a myriad of methods to exploit these vulnerabilities for personal gain. Weaknesses extend from the absence of physical defense on computing systems to vulnerable web applications whose databases may be at risk. With numerous attack surfaces available, the extensive scope of banking organizations makes them an attractive target for attackers seeking compromise and a formidable challenge for security experts striving to defend them.

AT A GLACE

OBJECTIVES

A comprehensive security overview for one of the largest banks in the United States.

SOLUTION

Full Red Team exercise that covered both the physical and digital aspects of the bank's operations, providing a distinctive and all-encompassing security overview.

KEY TAKEAWAYS

- Achieved physical penetration, enabling the deployment of custom malware on internal devices.
- Exploited a deficiency in security training to successfully execute phishing attacks, resulting in the acquisition of data from executives and the installation of malicious files on their computers.

SOLUTION & WORK PROCESS

Our specialists conducted a **comprehensive Red Team exercise for the bank**, aiming to evaluate both its digital and physical assets. As part of this exercise, we were tasked with conducting physical security assessments for various facilities identified as sensitive by the bank, along with numerous branches and residences of personnel.

The physical assessment encompassed efforts to infiltrate facilities, gain access to internal devices and networks, and breach wireless networks within these facilities or the homes of senior executives. Following successful access, we proceeded to attempt the delivery of custom malware onto employees' physical devices.

Furthermore, the exercise involved an assessment of overall physical security countermeasures. This evaluation included scrutinizing guard behavior and adherence to protocols, assessing security camera coverage, and examining approach vectors to mission-critical assets.

RESULTS

The exercise revealed a recurring pattern of poor practices within the tested environments. While not all of these practices constituted exploitable vulnerabilities, the persistent use of inadequate security measures was identified as a fundamental factor contributing to the diverse results observed in the penetration testing. It was determined in the assessment that the cost for a hacker to breach the system was $200,000. Following the implementation of our recommendations, the cost for an attacker would more than triple, serving as a significant deterrent.

The independent vulnerabilities identified in this security assessment raised concerns and pointed to a common root cause – a lack of adherence to security policies. From vulnerabilities related to human factors to substantial flaws found in proprietary technology and assets, these weaknesses rendered the audited institution susceptible to attacks across the various vectors outlined at the beginning of the exercise.

To address these issues, we provided recommendations for immediate remediation and ongoing prevention through the adoption of best practice security policies. We are committed to offering continued support in maintaining and enhancing the security posture of the institution.