Analyzing and Preventing Quick Response Code-based Malware and Phishing Attacks for Smartphones

Saxena, Alisha (School: Cherokee High School)

More than 11.6 million mobile devices around the world are infected with malware, and this number is increasing as smartphones gain popularity and become prime targets for hackers. Quick Response (QR) codes can pose a threat to unassuming scanners, as the URLs embedded in the codes can lead to malware or phishing sites. QR codes are especially vulnerable because a scan can automatically trigger the download of malware from an infected site, unbeknownst to the user. This paper investigates the prevalence of malware in QR codes and implements a solution to make QR codes secure. As part of my research, I gathered over 5 million records of barcode and QR code scans from a popular smartphone application and developed a tool to exhaustively parse through the big dataset. My tool extracts URLs from the data and checks each of them for malware and phishing vulnerabilities. My results indicated there are roughly 200 sites per million unique URLs that lead to malicious sites. Although this percentage is small today, my research conclusively proves that QR code exploits are increasing, legitimate threats. The simple yet opaque process of infecting smartphones through QR codes will become a serious concern as QR codes and smartphones become ubiquitous. Unfortunately, most QR code scanning applications in the market today do not check websites for security threats. Thus as a defense, I developed a secure Android QR code scanning application that protects users from QR code exploits.