Voatz App Security Flaws

Overview

Recently, news broke of multiple vulnerabilities in the Voatz mobile voting app, which was going to be used by both Oregon and West Virginia to allow voting by people who are physically unable to make it to the polls. The vulnerabilities, discovered by researchers at MIT, could allow hackers to see someone's vote or even change their vote. Specifically, the researchers noted that malware with root access to a voter's mobile device could bypass the host protection provided by Zimperium's zIAP SDK. According to the researchers, the SDK can be disabled via the xPosed Framework and four lines of code by using a hooking utility to alter the application's control flow. After that, an attacker with root access can commandeer the app to alter the interface and do things such as divert votes and leak ballots and personal data to an external server.

Lookout Analysis

Lookout Application Defense SDK and Lookout Mobile Endpoint Security (MES) will detect xPosed Framework. In order to provide full anti-tampering coverage, Lookout has partnered with Promon to provide an anti-tampering solution that protects apps against runtime hooking scenario as described by the MIT researchers. For an attack like this to be successful, xPosed framework requires the device to be rooted. Lookout SDK's advanced device compromise module would uncover rooting techniques such as Magisk and Magisk Hide.

How Lookout Detects and Protects

For application developers, especially those developing apps that collect highly sensitive data tied to industries like finance, healthcare, and government, security must be baked in. Protection against threats like runtime hooking with frameworks like xPosed is a key component of ensuring their app is secure. They can do so by embedding the Lookout App Defense SDK for threat detection and wrapping the application with Lookout Anti-tampering solution, which is created in partnership with Promon. Promon Shield ensures that the code cannot be reverse engineered and prevents other processes from hooking into the application code at runtime.

Lookout Threat Advisory Service

Lookout App Defense detects various types of cyber threats that can lead to account takeovers such as credential theft, data leakage, and fraud on the mobile app. The Lookout Security Cloud has analyzed over 100M mobile apps globally, delivering mobile app protection to counter various threat vectors including malicious apps, network and compromised devices.

Click here to learn more about Lookout App Defense