PROMON

App Threat Report

The State of Financial Services' Malware Defense

Q2 - 2023

Index

Introduction

Welcome to our Q2 App Threat Report, Promon's quarterly analysis of current topics in mobile application security produced by our Security Research Team.

Malware continues to target financial services apps. According to SecureList, more than 57,000 banking trojans were observed in Q1 2023, up 19% over Q4 2022. These trojans can steal customer credentials, observe, and record personal data and sometimes conduct transactions.

In our Q2 report, our team created a screen reader that could exfiltrate data in a manner similar to real-world malware. We used this tool to see if we could extract sensitive information from 100 of the top financial services apps in order to assess the security level of financial services applications and understand how they tackle a common malware-style exfiltration attack.

Screen readers and malware

Screen readers are essential accessibility tools. Screen readers will often convert digital text into synthesized speech or, alternatively, a braille output. They are primarily designed to assist visually impaired individuals in navigating and interacting with digital content.

The access that screen readers and other accessibility services ask for is extensive and gives broad access to the screen and its contents, making it ripe for abuse.

Malware that can successfully access the screen and its contents without root privileges can:

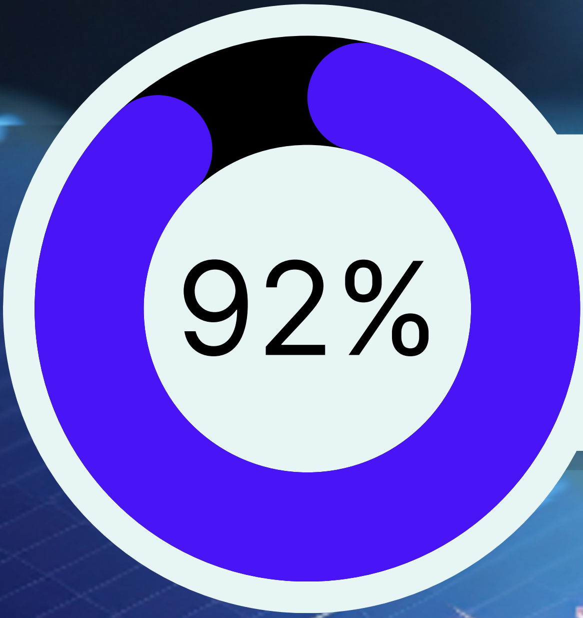
1. **Steal sensitive information.** Malware can use screen reader capability and accessibility services to read text from apps, websites, and other sources. This information could include passwords, credit card numbers, and other sensitive data.

2. **Intercept two-factor authentication codes.** Malware can use accessibility services to intercept two-factor authentication codes that are sent to users' phones. This could allow the malware to gain unauthorized access to accounts.

3. **Control the device.** Malware can use accessibility services to control the device's UI (User Interface), such as opening and closing apps, clicking on buttons, and entering text. This could allow malware to carry out a variety of malicious activities, such as making unauthorized purchases or sending spam messages.

4. **Bypass security features.** Malware can use accessibility services to bypass security features, such as those that prevent apps from being installed from unknown sources. This could allow the malware to install itself on the device without the user's knowledge or consent.

Results



of the apps tested did not have sufficient protection in place.

Promon tested 100 of the world's top banking and financial services apps for Android to see how these apps would handle a malicious screen reader attack. Hundreds of millions of people use these apps, every day, to conduct sensitive financial transactions.

To simulate a real-world screen reader attack, our team authored a simple screen reader that would exfiltrate data entered in the app. For more details on the software and test process, please see our “Methodology” section.

Our research team successfully tested 92 of the 100 apps. The screen reader could read and exfiltrate data from 85 of the 92 apps (92.4%). Only seven apps showed clear defense against the screen reader’s attempts to read the data (7.6%).

Recommendations

While robust App Shielding technology can help mitigate the threat of malicious screen readers, there are steps developers can implement right away.

Developers can implement code in their apps to detect if a screen reader is active. If the app detects that a screen reader is active the app will need to take a decision: display a warning to the user, shut down, or simply do nothing.

However, all those solutions have some drawbacks. A warning message can be removed by malware with accessibility features, defeating the point. Ignoring the screen reader may be harmful to the user as malware would be able to trivially retrieve their information. Finally, shutting down the app will prevent even legitimate accessibility features to be used, which will impede the user experience and potentially infringe on local regulations.

Developers can verify which application is using the accessibility features in an attempt to mitigate the issues with shutting down the application. Well-known accessibility applications would not trigger the application to shut down limiting the risk of legal issues and bad user experience. However, lesser known ones would still cause the app to shut down, despite being legitimate. This would ultimately necessitate some maintenance to be sure that new legitimate accessibility applications will be recognized as safe by the application. In such cases, solutions like Promon SHIELD™ take away the maintenance part from the application developers, making shutting down the application a more attractive solution, while also providing extensive security features.

Finally and most helpfully, Android 14 has promised new security features aimed at preventing accessibility service abuse. Mishaal Rahman of Esper commented: "Starting in Android 14, though, developers can prevent non-accessibility tools from interacting with their app. By setting the new ACCESSIBILITY_DATA_PRIVATE_YES attribute on a View, only accessibility tools can interact with that View. This can be used by an app like Google Authenticator to ensure that only declared accessibility tools (like TalkBack) can read 2FA codes."

While this is a welcome development, it's important to remember that Android 14 will take some time to roll out and that OS features should always be used in concert with strong defensive measures at the app level to protect end-users.

Methodology

Selection

Overall, Promon downloaded 100 of the most-used finance Android apps. Apps tested were determined by finding the finance apps with the most downloads over the past year on the Google Play Store, according to SensorTower.

Testing environment and process

All testing was done manually by Promon's dedicated quality assurance and control team.

For each app to test, we first uninstalled our screen reader, installed the app and ran it to see if it would work correctly. This was done to ensure it would not malfunction for some reason unrelated to the attack. Six of the apps we tested did not run correctly on our test device even without a screen reader installed.

We then installed and activated the screen reader and re-launched the app. After that, we navigated to a login or registration screen and entered some recognizable text. We then checked if that text was logged by our screen reader or not.

PROMON

About Promon SHEILD™

A comprehensive Application Shielding solution can help you achieve compliance, eliminate in-app fraud, and defend against malware attacks, such as the one described in this report. Promon SHIELD™ combines advanced obfuscation and robust runtime protection to help protect apps and end-users from harm.

Read more >

About Promon

Promon is the leader in proactive mobile app security. We exist to make the world a little bit safer, one app at a time.

Since 2006, some of the world's most impactful companies have trusted Promon to secure their mobile apps. Today, more than 1 billion people use a Promon-protected app.

Promon is headquartered in Oslo, Norway with offices throughout the globe.

Learn more >