PROMON

App Threat Report

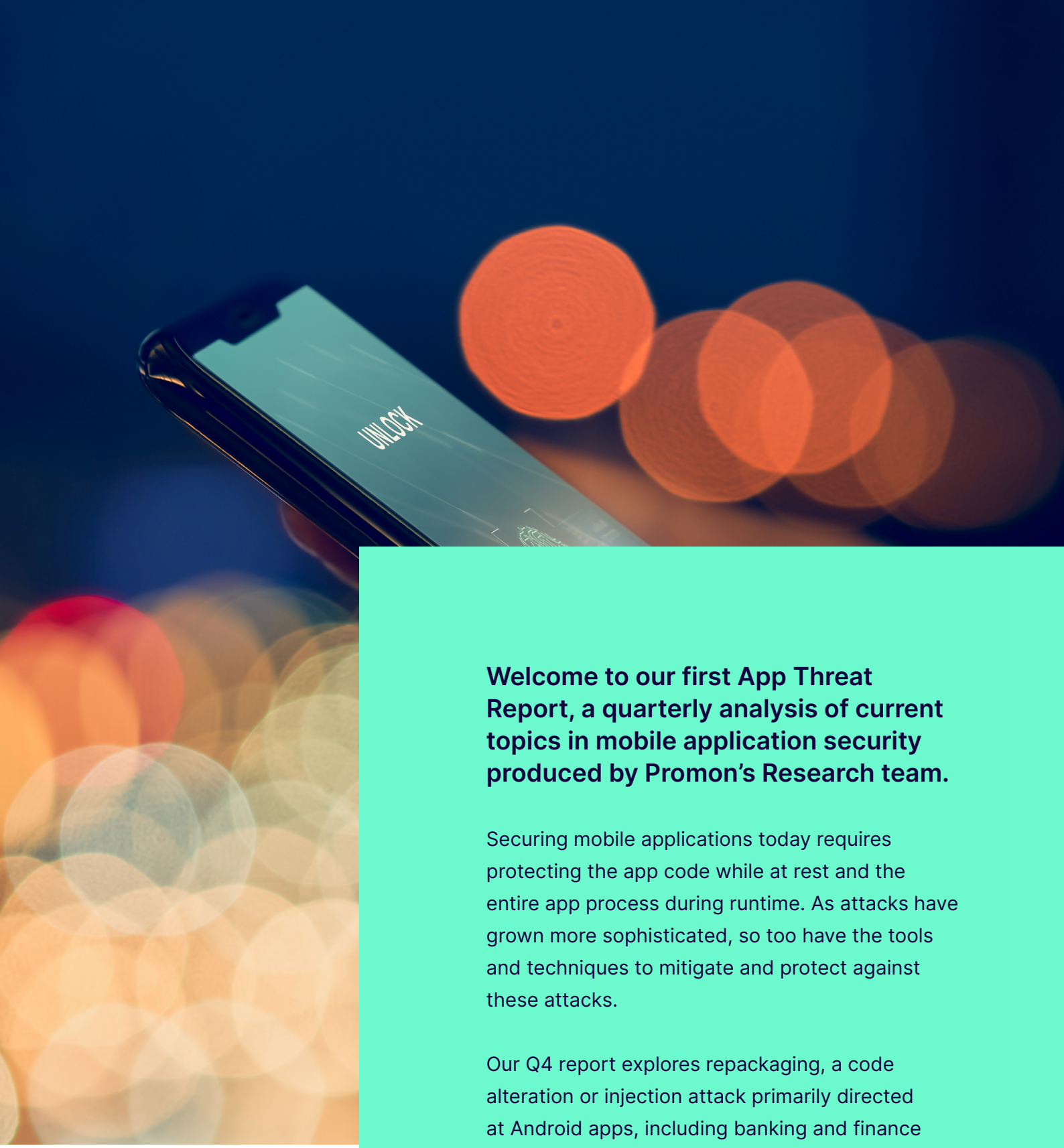
The State of App Repackaging

Q4 - 2022

Index

For more information visit us at

www.promon.co



Welcome to our first App Threat Report, a quarterly analysis of current topics in mobile application security produced by Promon's Research team.

Securing mobile applications today requires protecting the app code while at rest and the entire app process during runtime. As attacks have grown more sophisticated, so too have the tools and techniques to mitigate and protect against these attacks.

Our Q4 report explores repackaging, a code alteration or injection attack primarily directed at Android apps, including banking and finance apps. Read on for a short primer on repackaging, followed by a review of the hundreds of financial services apps across various sectors, install bases, and regions to assess the overall level of security against this routine attack.

About

Repackaging

What is a repackaging attack?

Repackaging attacks either inject code into an app or modify an application's existing code and then repackage it into an application that can execute. While this report focuses on Android, iOS apps can also be repackaged. Apple cites the risks of repackaging in its decision not to allow sideloading iOS apps. However, app developers may still find their apps on jailbroken iPhones, and sideloading is possible using, for example, enterprise distribution solutions.

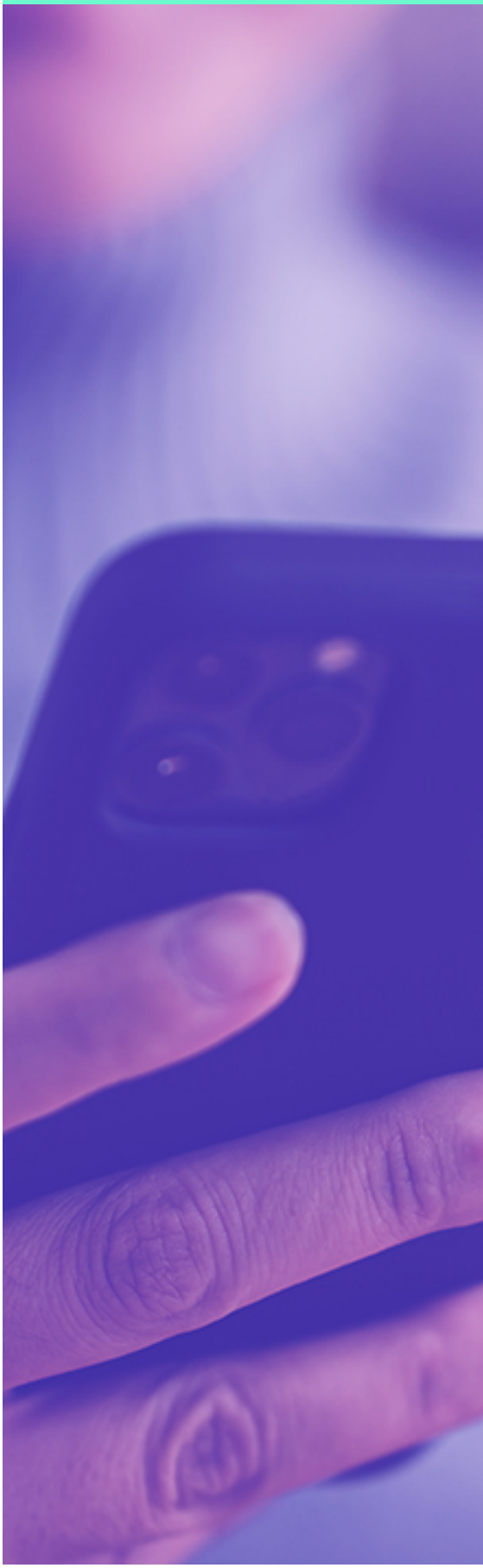
What are the risks of repackaging?

Malicious code injection carries significant risks for both app owners and users. Yet the dangers of repackaging go well beyond code injection.

Repackaging attacks are also a fundamental starting point to removing existing in-app security, providing easy access to reverse engineering of any proprietary code and I.P. Additionally, malicious app activity also carries a risk of brand reputational damage.

Do the app stores protect against repackaged apps?

While a legitimate app may be distributed in the major app stores, third-party app stores may not have such stringent policies. Also, attackers can use various methods, from ads to spam, to trick users into downloading a repackaged app. A recent example occurred when a malicious WhatsApp clone stole thousands of user accounts and P.I. data.



How can I protect my mobile app against repackaging?

Code encryption and obfuscation can help protect against code modification and reverse engineering and is thus a recommended strategy. However, strong runtime protection is required to mitigate against code injection.

Android and iOS developers can add these features to their apps:
1. Independent verification of the app's signature. O.S. verification will not work if it has been disabled (e.g., on a Jailbroken phone) or re-signed with a different but valid distributor key.
2. Verification of app resources before use.
3. Code integrity checks to detect tampering.

A comprehensive Application Shielding solution can help eliminate the risk of both code injection and code modification repackaging attacks. Promon's App Shielding combines advanced obfuscation and robust runtime protection to help protect apps and end-users from harm.

Get in touch at promon.co to learn more.

Analysis

Summary

Promon Research wanted to explore the risk of repackaging attacks on the world's most-used finance apps. Out of the 384 apps tested, we could repackage 61% or 236 apps. Our analysis also indicated that these apps could not mitigate or defend against such attacks and likely could not detect code injection and repackaging attacks. For more information on what constituted a successful repackaging, please consult our Methodology.

It is encouraging that some countries are leading the charge regarding application security. In Australia (38%), Norway (40%), and Japan (42%), less than half of the apps tested were successfully repackaged, which compares favorably to the Report Benchmark of 61%. As a category, trading apps were the weakest (we successfully repackaged 75%), while Banking and Payment both came out marginally better than average (both at 58%).

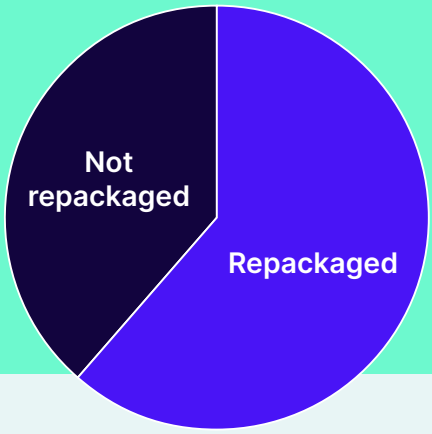
This report highlights the ever-present need to harden mobile applications against common attacks. Once successfully repackaged, an altered app needs only a distribution method to get into the hands of unsuspecting users. Fortunately, there are concrete steps highlighted above that developers can take to protect against the repackaging threat and reduce risk.

Read on for a detailed breakdown of the repackaging rates by country/region and app category.

ANALYSIS RESULTS

Report Benchmark

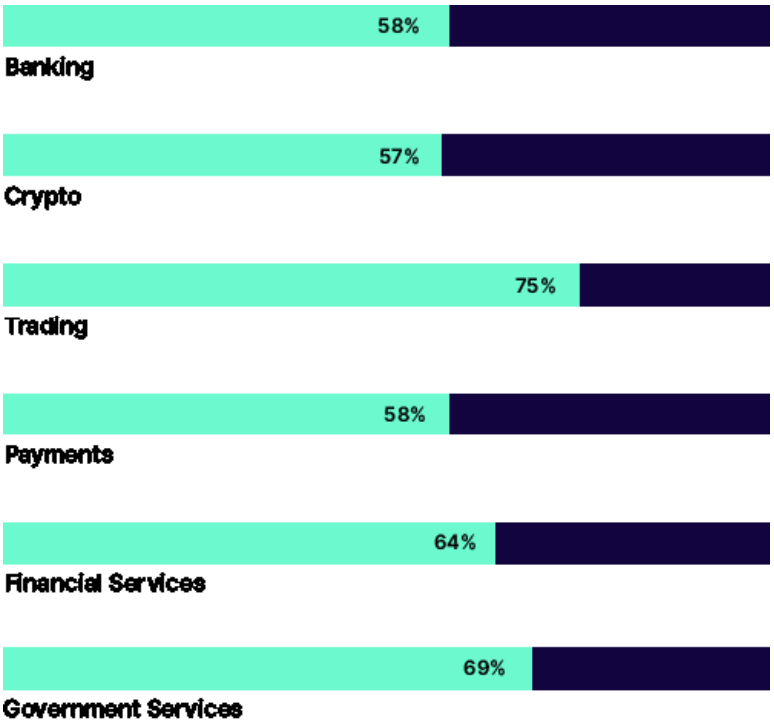
To produce this report, Promon Research downloaded 434 unique applications, of which 384 were able to complete the test (see “Methodology” for more information). Of those, 236 apps could be repackaged (61%).



Overall, trading apps were most susceptible to our repackaging test, as 33 of 44 tested (75%) had code injected, and the app ran successfully.

Nine of 13 (69%) Government Services apps tested failed to mitigate against repackaging. Financial Services had a similar rate (64%), although we tested a much larger number of apps – 74.

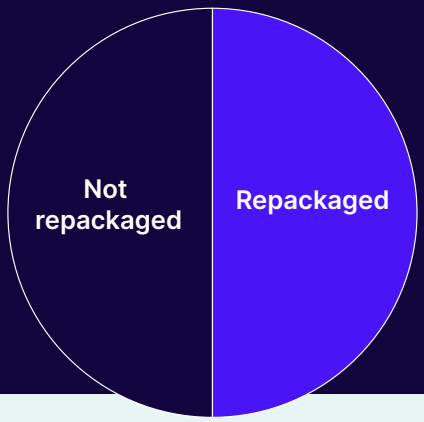
The category with the most apps tested, Banking, had 89 of 154 (58%) repackaged in our test. Payment (19 of 33) and Crypto (34 of 60) apps fared similarly, at 58% and 57%, respectively.



ANALYSIS RESULTS

Top 100 Global Finance Apps

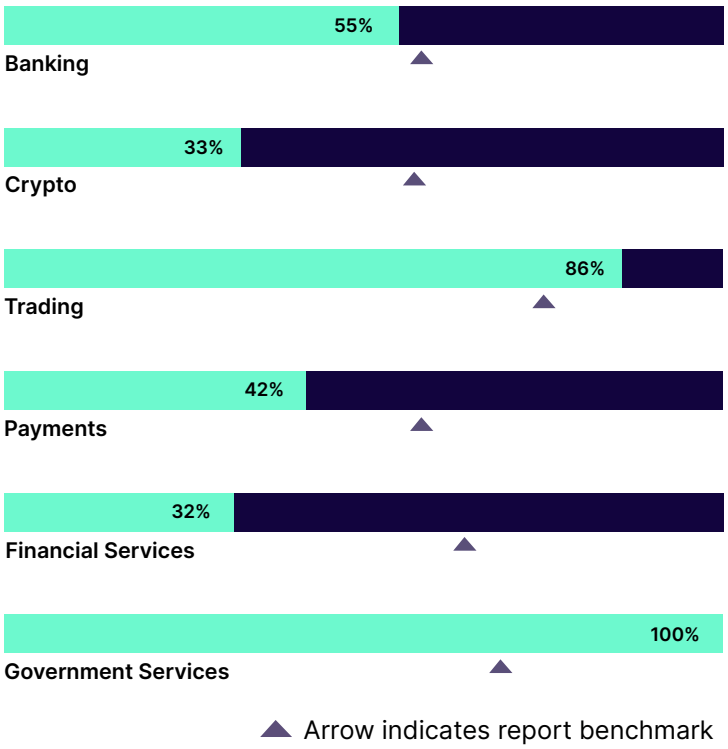
Promon Research analyzed the 100 most-used finance apps in the Google Play Store globally, of which 93 were able to complete the test (see “Methodology” for more information). Of those, 46 apps could be repackaged (50%).



Crypto and Financial Services apps had the fewest number of apps that were repackable. Six of 19 Financial Services apps (32%) could be repackaged. Similarly, just two of six crypto apps tested were repackaged (33%).

Of the apps tested, 26 out of 47 banking apps were susceptible to repackaging (55%), slightly below the Report Benchmark. Although comprising a smaller overall number of apps tested, 86% of trading apps were repackable*, well above the Report Benchmark.

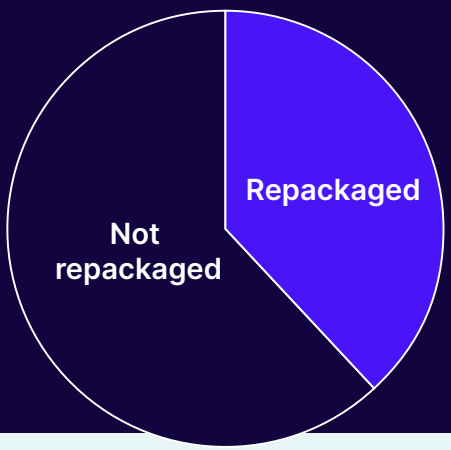
*Governmental Services had one app tested, which was also repackable.



ANALYSIS RESULTS

Australia

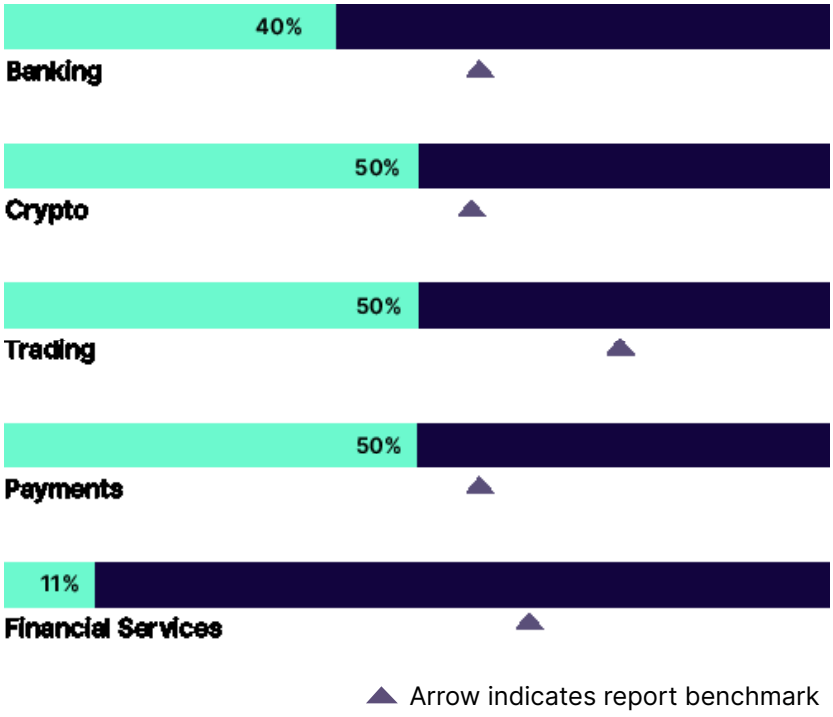
Promon Research analyzed 50 of the most-used finance apps in Australia's Google Play Store, of which 47 were able to complete the test (see "Methodology" for more information). Of those, 18 apps could be repackaged (38%), making Australia the best-performing country in our set and well below the Report Benchmark of 61%.



Financial Services apps had the fewest number of apps susceptible to repackaging. Only one out of nine apps (11%) was successfully repackaged, compared to 64% in the Report Benchmark.

The story was different for all the other app types tested. 8 of 20 Banking apps (40%) were repackable. 50% of all Crypto (5/10), Trading (3/6), and Payment (1/2) apps were repackable.

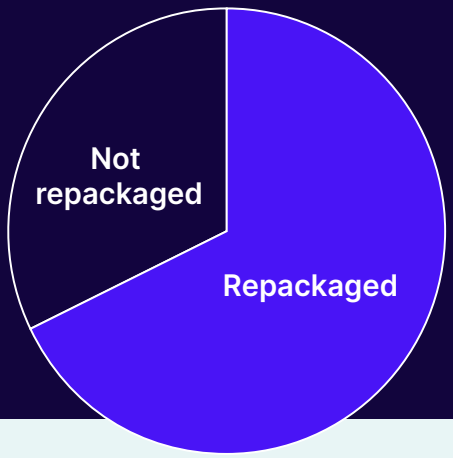
No Government Services apps were in the test set.



ANALYSIS RESULTS

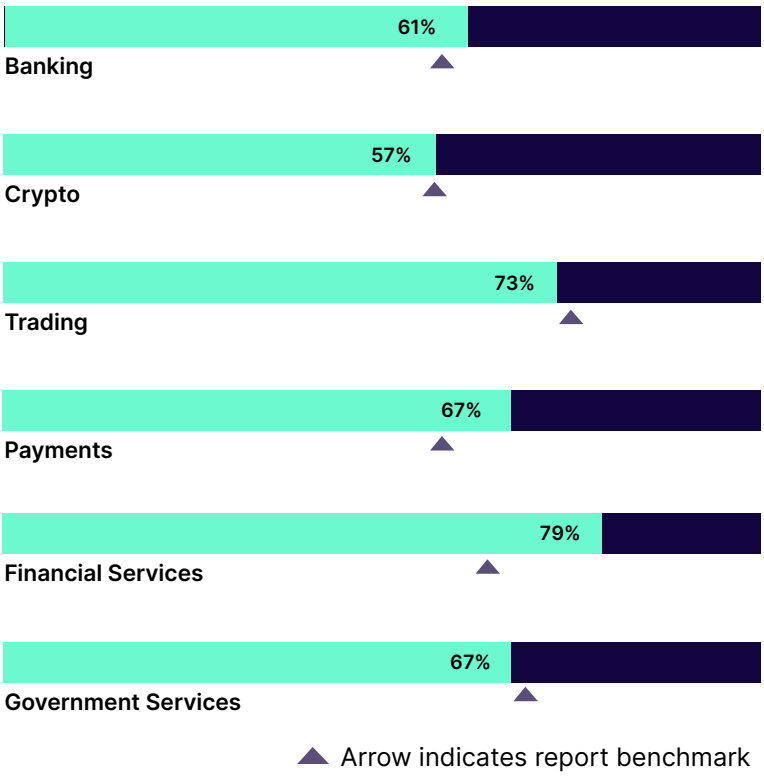
Brazil

Promon Research analyzed 65 of the most-used finance apps in Brazil's Google Play Store, of which 59 were able to complete the test (see "Methodology" for more information). Of those, 40 apps could be repackaged (68%).



Crypto apps were the least susceptible, yet four of seven were successfully repackaged (57%). This percentage is in line with the Report Benchmark.

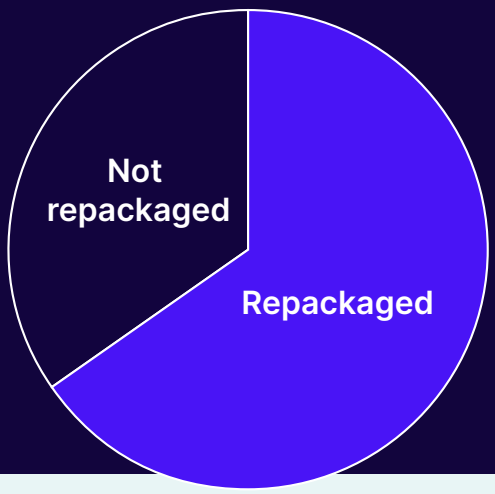
11 of 14 Financial Services apps (79%), 8 of 11 Trading apps (73%), 4 of 6 Government Services apps (67%), 2 of 3 Payment (67%), and 11 of 18 Banking apps (61%) were repackable. Banking, Payment, and Financial Services repackaging rates exceeded the Report Benchmark.



ANALYSIS RESULTS

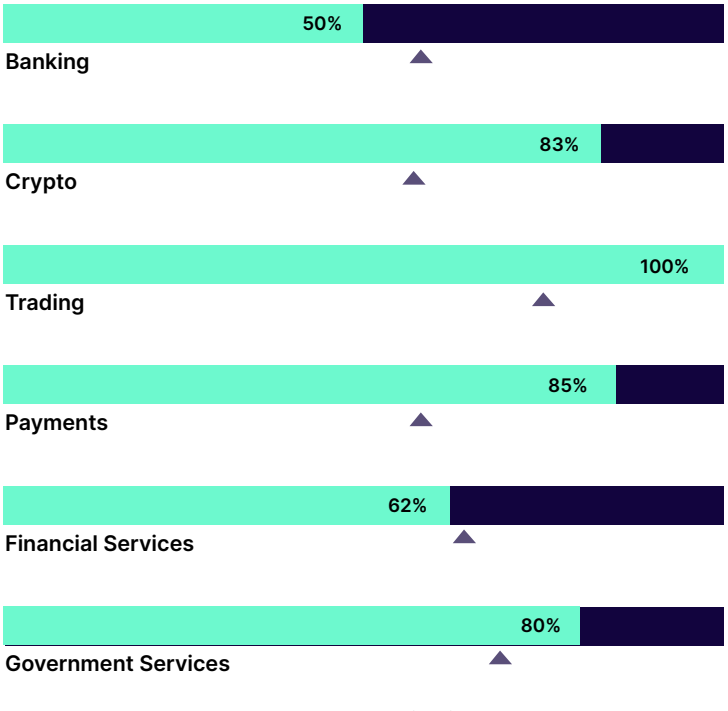
The European Union

Promon Research analyzed 102 of the most-used E.U. finance apps as ranked by SensorTower, of which 81 were able to complete the test (see “Methodology” for more information). Of those, 53 apps could be repackaged (65%).



Banking apps performed best, with 19 of 38 (50%) able to be successfully repackaged.

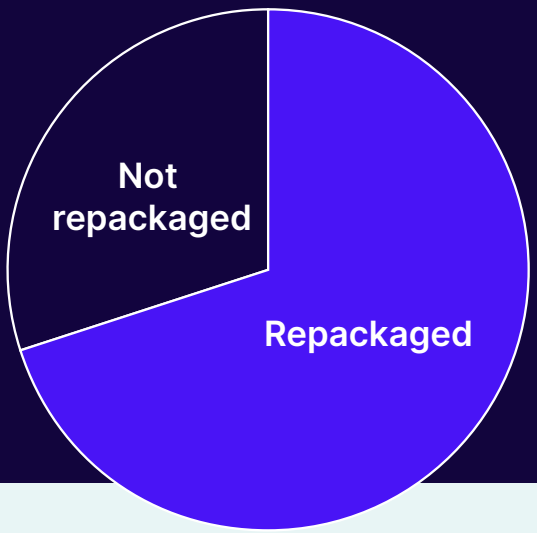
Six of six Trading apps (100%), 11 of 13 Payment apps (85%), 5 of 6 Crypto apps (83%), 4 of 5 Government Services apps (80%) and 8 of 13 Financial Services apps (62%) were repackable.



ANALYSIS RESULTS

India

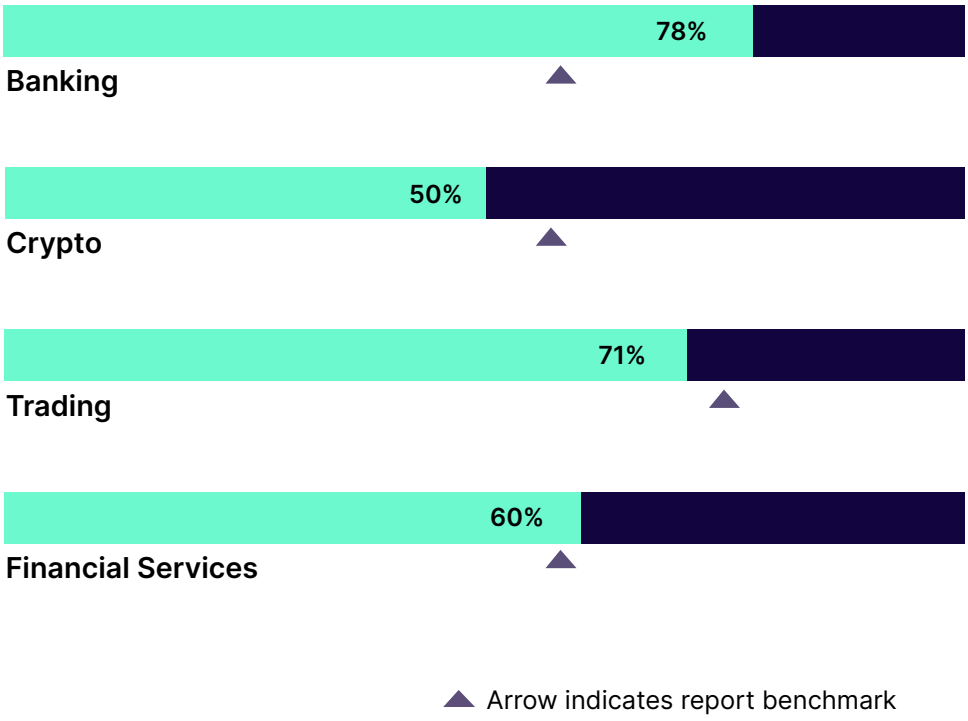
Promon Research analyzed 78 of the most-used finance apps in India's Google Play Store, of which 67 were able to complete the test (see "Methodology" for more information). Of those, 47 apps could be repackaged (70%).



Like Brazil, Crypto apps were least susceptible, yet five of 10 were successfully repackaged (50%). Still, this is seven percentage points below the Report Benchmark.

21 of 27 Banking apps (78%), 12 of 17 Trading apps (71%), 2 of 3 Payment (67%) were repackable.

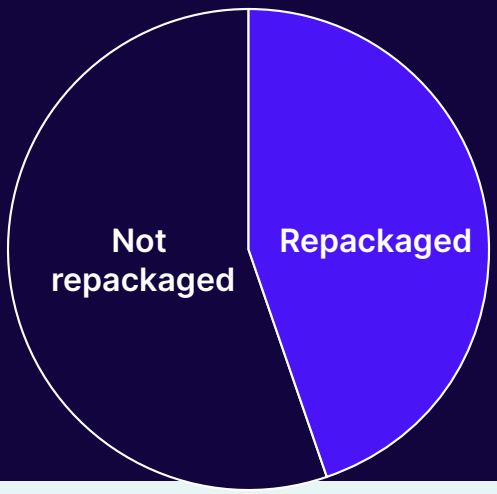
No Payment, Financial Services or Government Services apps were in the test set.



ANALYSIS RESULTS

Japan

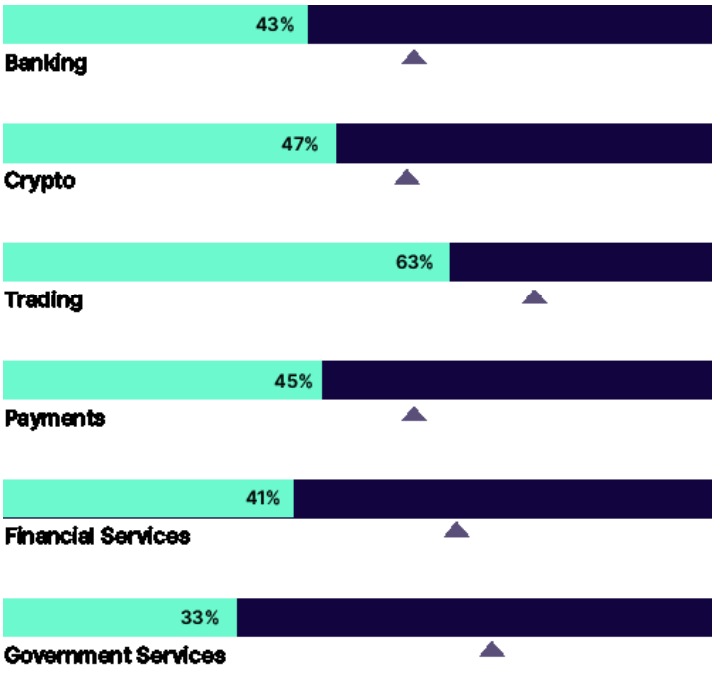
Promon Research analyzed 118 of the most-used finance apps in Japan's Google Play Store, of which 109 were able to complete the test (see "Methodology" for more information). Of those, 49 apps could be repackaged (42%).



All app categories performed better than their respective report benchmarks. 12 of 29 (41%) Financial Services apps were repackaged. While just 33% of Government Services apps were repackaged, only three were in the category.

Like the global benchmark, Trading apps were the most susceptible, with 5 of 8 (63%) able to be repackaged. This category was the only one with more than 50% of apps successfully repackaged.

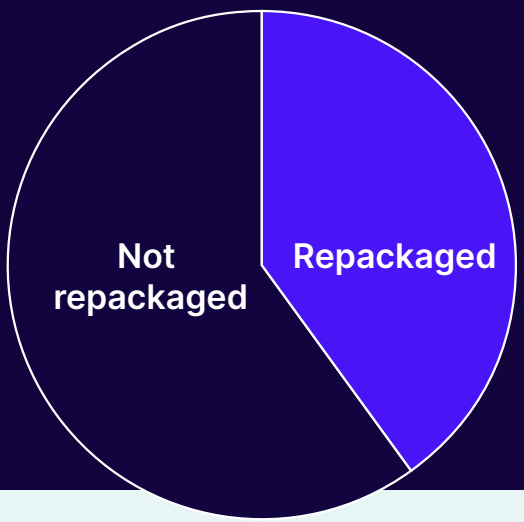
12 of 28 (43%) Banking apps, 5 of 11 (45%) Payment apps, and 14 of 30 (47%) Crypto apps were successfully repackaged.



ANALYSIS RESULTS

Norway

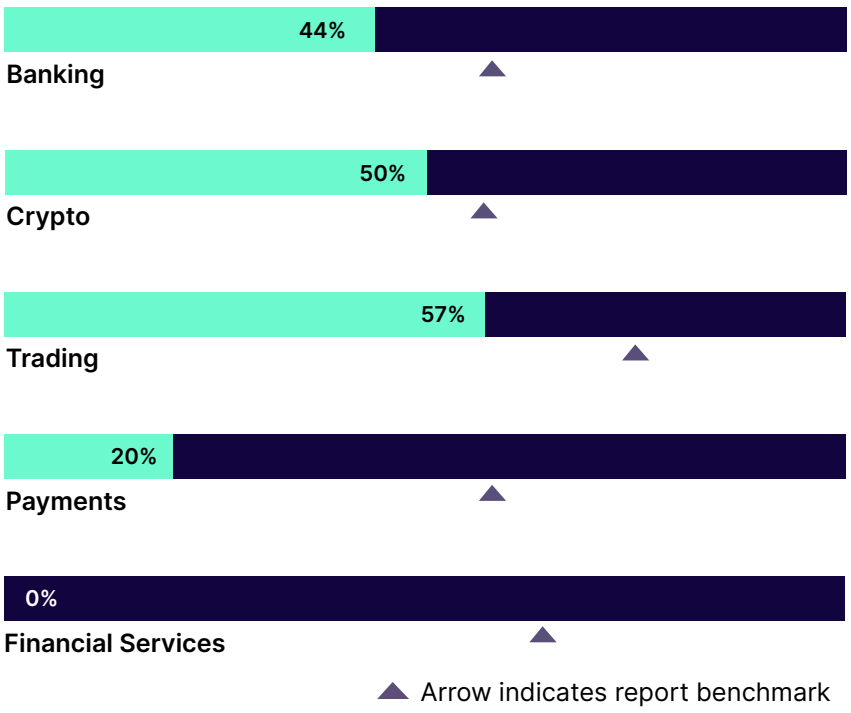
Promon Research analyzed 58 of the most-used finance apps in Norway's Google Play Store, of which 55 were able to complete the test (see "Methodology" for more information). Of those, 22 apps could be repackaged (40%), well below the Report Benchmark.



Zero Financial Services apps were susceptible, making it the clear category leader. Only 1 (20%) could be repackaged of the five Payment apps tested. Also, coming in just under 50%, 11 of 25 Banking apps (44%) were successfully repackaged.

Four of seven Trading apps (57%) and six of 12 Crypto apps (50%) were repackable.

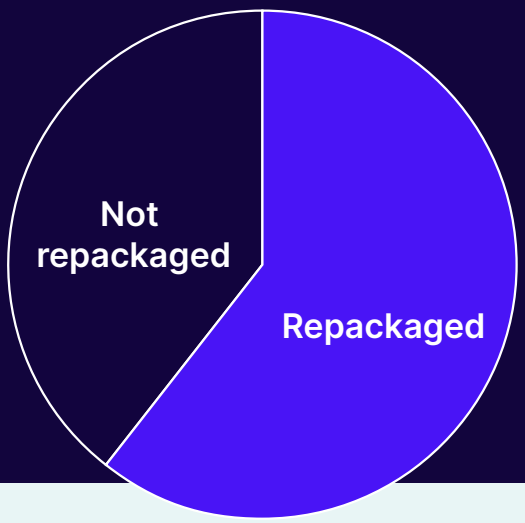
No Government Services apps were in the test set.



ANALYSIS RESULTS

United Kingdom

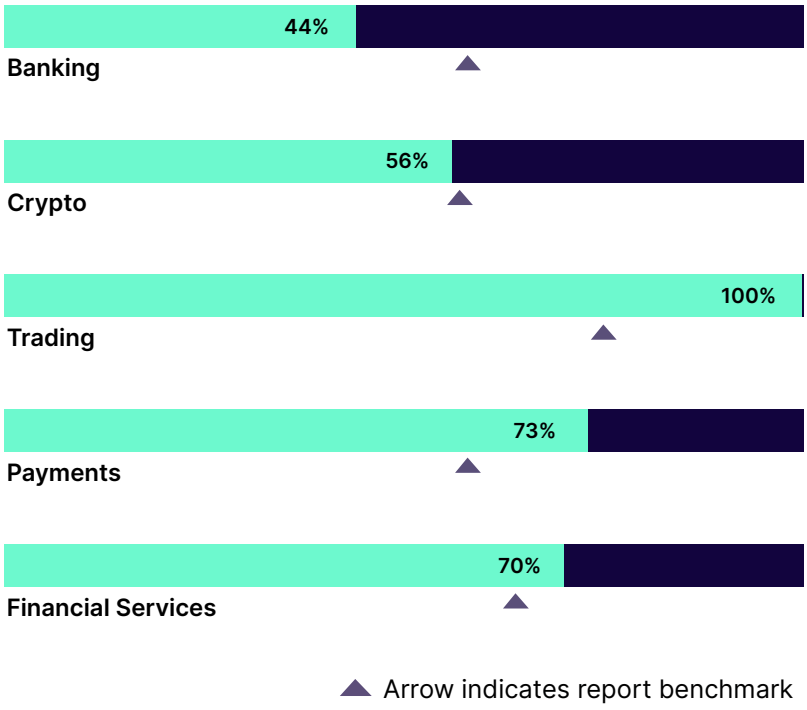
Promon Research analyzed 91 of the most-used U.K. finance apps as ranked by SensorTower, of which 74 were able to complete the test (see "Methodology" for more information). Of those, 45 apps could be repackaged (61%), in line with the Report Benchmark.



Banking apps performed best, with just 12 of 27 (44%) able to be successfully repackaged, well below the Report Benchmark.

Eight of eight Trading apps (100%), 8 of 11 Payment apps (73%), 7 of 10 Financial Services apps (70%), and 10 of 18 Crypto apps (56%) were vulnerable to a repackaging attack. Trading, Payment, and Financial Services apps exceeded their respective Report Benchmarks.

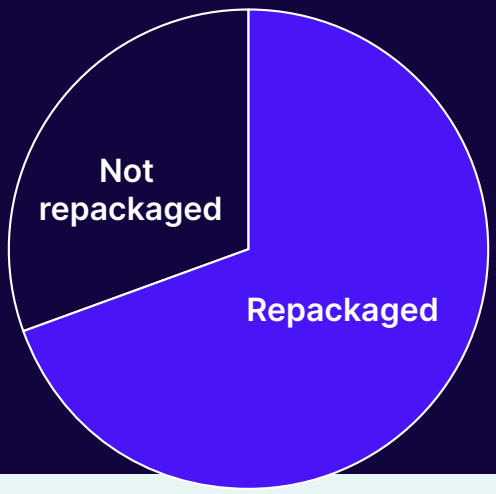
No Government Services apps were included in the test set.



ANALYSIS RESULTS

United States

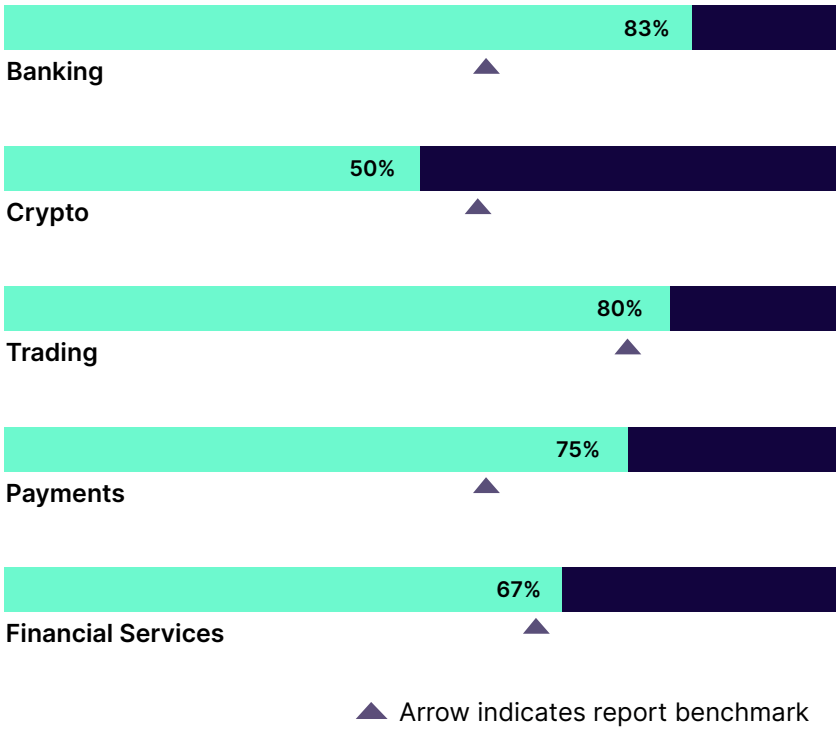
Promon Research analyzed 69 of the most-used U.S. finance apps as ranked by SensorTower, of which 56 were able to complete the test (see “Methodology” for more information). Of those, 39 apps could be repackaged (61%), in line with the Report Benchmark.



Crypto apps performed best, with 8 of 16 (50%) able to be successfully repackaged.

10 of 12 Banking apps (83%), 8 of 10 Trading apps (80%), 6 of 8 Payment apps (75%), and six of nine Financial Services apps (67%) were vulnerable to a repackaging attack. All of these categories exceeded their respective Report Benchmarks.

No Government Services apps were included in the test set.



Report

Methodology

Selection

Overall, Promon analyzed 434 unique Android apps. Apps tested from each region were determined by finding the apps with the most daily active users over the past year in the finance category on the Google Play Store, according to SensorTower.

U.S., E.U., and U.K. used both APK and AAB files for the analysis. All other countries used APK files only. Some apps were unavailable due to regional limitations.

Process

Promon created a script to install and run the unmodified app to ensure it runs in the test environment. To ensure that it runs successfully, we let the application run for 30 seconds while checking that it has not terminated. If the app did not terminate, we continued with our repackaging test. To repackage the app, the script would then decompile the Java code of the app, insert simple code into it that prints a message, then recompile the app and finally sign it. The script would then install the app, launch it, and monitor if it runs for 30 seconds.

If an application did not run at all, even if we did not modify it, we assume that there is either a problem with the app or our test setup. We did not investigate these problems further but classified them as not completing the test.

If we saw problems modifying the application, we also classified the app as not completing the test. There were several reasons why this happened. In most cases, it was because there was something in these apps that our tools did not support.

The apps that we classify as being repackable are apps that do not crash in the first 30 seconds after launch when we have repackaged them. This strongly indicates that the app does not prevent repackaging, as ideally, the app would crash when repackaging is detected. But there could be apps that launch successfully but have detected repackaging and do not (immediately) do something about it. This is challenging to determine but also far from ideal from a security standpoint. If the app knows that it has been repackaged, it should not trust that the functionality it uses to prevent the app from running correctly has not been manipulated.

The apps that we classify as not being repackable are apps that do not crash 30 seconds after launch when they have not been repackaged but do crash in the first 30 seconds after launch when being repackaged. In many cases, the crash is because the app detects repackaging and shuts down. But there can also be cases where the repackaging process has broken something in the app, and this causes the crash without the developer intending this to happen.

All apps were deleted following the test.

App Types

Promon created six categories with the following definitions:

1. Banking: retail banking apps or apps which allow diverse banking transactions, such as transaction lists, access to credit cards, and transfers
2. Trading: apps that allow diverse investment transactions, such as buying and selling stock, bonds, or other financial products
3. Payment: apps that authorize payments, either through an app or credit card
4. Crypto: apps that allow trading and transacting with one or more cryptocurrencies
5. Financial services: apps that did not fit into other categories, including currency converter apps and news apps. In any case, apps in this category had no explicit financial transaction permitted.
6. Government Services: apps provided by local, regional, or national governments that connect consumers to one or more different finance-related services provided by that government.

In cases where an app may fit into multiple categories, we looked at the nature of transactions permitted in the app. For example, an app that primarily discusses cryptocurrencies but does not allow transactions would be classified as financial services.

Promon SHIELD™ protects your mobile apps against:

- ✓ Malware
- ✓ Debuggers (Java, native debuggers)
- ✓ Emulator/fake execution environment
- ✓ Cloning of the device
- ✓ Rooting/Jailbreak
- ✓ Code injection
- ✓ Hooking-frameworks
- ✓ Repackaging (Fake, manipulated apps)
- ✓ And more

PROMON

Stortingsgata 4
0158 Oslo, Norway

info@promon.no
www.promon.co

Book a demo