Mobile App Hackers Take Advantage of a Global Pandemic

Mobile app security during COVID-19

In the midst of a global health crisis that threatens the lives and livelihoods of millions, some hackers see opportunity. Malicious actors are preying upon vigilance and fear regarding the COVID-19, even as entire nations are under lockdown in an attempt to slow the spread of infection.

Organizations who build and deploy mobile apps—and their users—must be aware of what hackers are up to. In this fact sheet, we will share some of the exploitative vectors, as well as explore what creators and distributors of mobile apps can do to defend their assets.

There Are Thousands of COVID-19 Mobile App Attacks

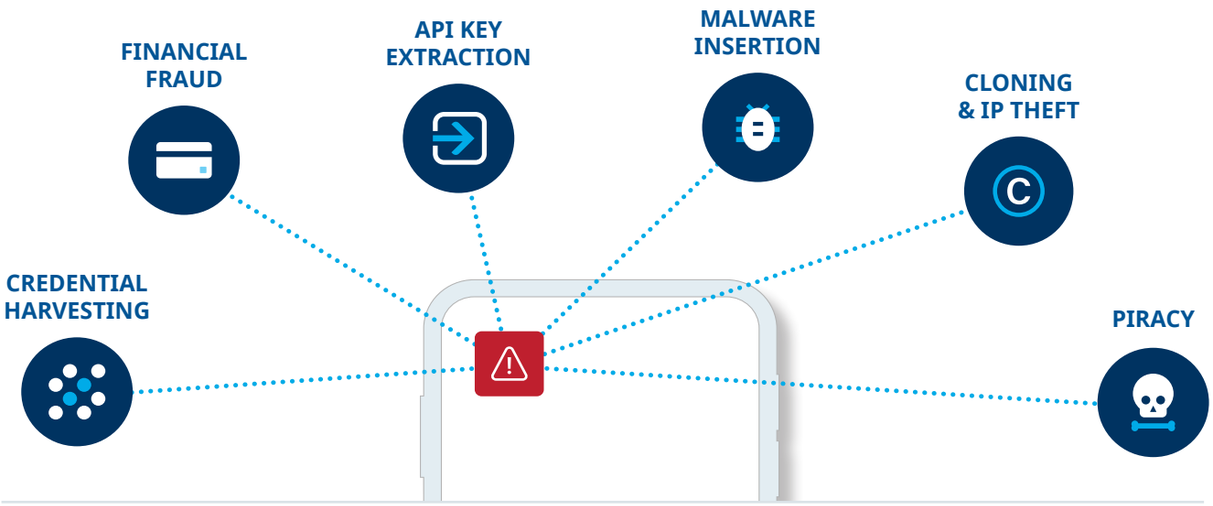
Both cybercriminals and nation-state affiliated hackers have been attempting to use malware and other attacks to steal money, exfiltrate data, spy on people, and more. In fact, **thousands of new websites and mobile applications** with malicious intent related to COVID-19 are being spun up **daily**. Here are just a few of the attacks that have been levied so far:

- **CovidLock**: Android ransomware app
- **Coronavirus Tracker app**: Android ransomware app
- **Corona live 1.1**: Android surveillance spyware

Security researcher Lukas Stefanko is updating **this blog post** regularly with new exploits.

Mobile app attacks were a widespread problem before COVID-19. According to the **McAfee Mobile Threat Report 2019**, nearly 65,000 new fake apps were detected in December of 2018—more than 6 times the amount reported in June 2018. The **2020 Mobile Threat Report** indicates hackers are now looking for ways to further extend their malicious goals by “hiding” app icons and using other forms of mobile “sneak attacks.”

If your organization’s mobile apps are not properly secured against these opportunistic hackers, your business, and your users, are at risk right now.



helloworld@guardsquare.com www.guardsquare.com

GUARDSQUARE
Mobile application protection

How to Protect Your Organization Against COVID-19 App Attacks & More

Fake mobile apps are Android or iOS applications that mimic the look and/or functionality of legitimate applications to trick unsuspecting users into installing them. Once downloaded and installed, the applications perform a variety of malicious actions. Unfortunately, more than half of users cannot distinguish between real and fake apps, according to this survey.

Two common malicious app strategies

1. Some cybercriminals will **build a fake app for a popular brand** that doesn't have one. In the era of COVID-19, they may simply build new apps around search terms that play on fears—such as virus trackers and infection maps.
2. In other cases, they may **clone existing, legitimate apps** and add malicious code. Unprotected mobile apps can be reverse engineered in minutes. Once an attacker has access to the source code, it's possible to tamper with and repackage it. In the case of COVID-19, hackers may target published apps legitimately designed to help in the battle against this pandemic.

Organizations can suffer **substantial financial and reputational damage** when their mobile applications are cloned and/or their brands become associated with fraud. Even if your business isn't a likely target for COVID-19 specific fraud, hackers are actively looking for creative ways to exploit people during this uncertain time and you must be prepared to defend yourself.

How to fight back against mobile app hackers

To protect your organization, businesses can take the following measures:

1. **Provide legitimate mobile applications**. Giving users easy access to legitimate apps through official app stores reduces the risk of them downloading fakes.
2. **Regularly check the Google Play Store and the Apple App Store**. Monitor the official app stores and report any abuse of their brands to reduce the negative impact of fakes.
3. **Protect Android and iOS applications**. Code hardening and runtime applications self-protection (RASP) effectively prevent mobile applications from being cloned and tampered with. **Guardsquare** helps organizations **secure mobile applications** against hacking and its consequences using both code hardening and RASP.

Protect your mobile apps: **Request a demo >**

helloworld@guardsquare.com www.guardsquare.com