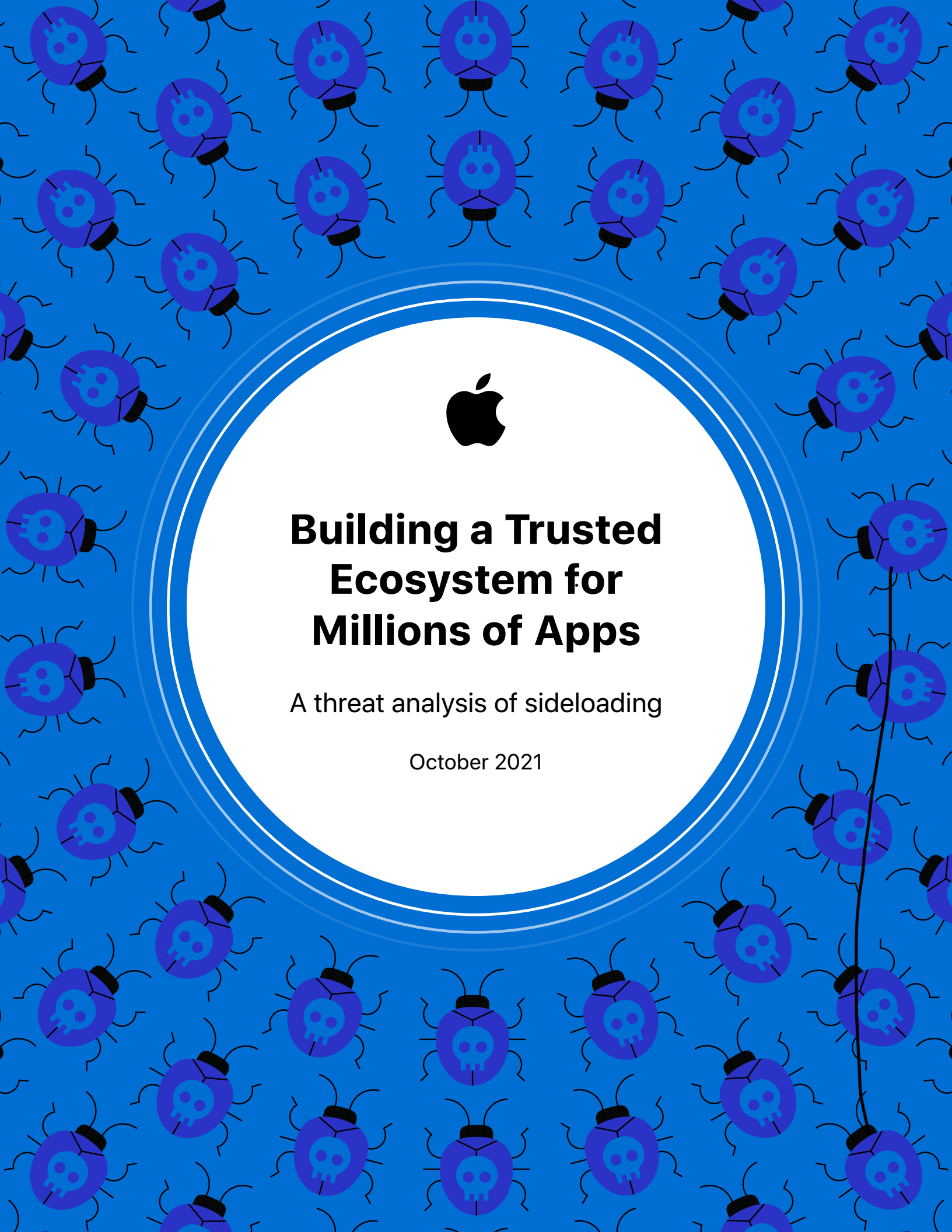


Building a Trusted Ecosystem for Millions of Apps

A threat analysis of sideloading

October 2021

Key Insights

iPhone is a highly personal device where users store some of their most sensitive and personal information. This means that maintaining security and privacy on the iOS ecosystem is of critical importance to users. However, some are demanding that Apple support the distribution of apps outside of the App Store, through direct downloads or third-party app stores, a process also referred to as "sideloading." **Supporting sideloading through direct downloads and third-party app stores would cripple the privacy and security protections that have made iPhone so secure, and expose users to serious security risks.**

Mobile malware and the resulting security and privacy threats are increasingly common and predominantly present on platforms that allow sideloading.

A European regulatory agency reported **230,000 new malware infections per day.**

Over the past four years, **Android devices were found to have 15 to 47 times more malware infections than iPhone.**

Nearly 6 million attacks per month were detected by a large security firm on its clients' Android mobile devices.

Mobile malware harms consumers, companies, developers, and advertisers. Attacks on users employ various tactics and techniques. Common types of mobile malware affecting consumers are adware, ransomware, spyware, and banking and other credential-stealing trojans that masquerade as legitimate apps. Cybercriminals often reach their targets through social engineering or supply chain attacks, and sometimes use popular social media networks to spread the scams and attacks. Most rely on third-party app stores or direct downloads to spread malicious apps. Developers and advertisers are also harmed by these attacks, mostly through piracy, intellectual property theft, and loss of advertising revenue.

If Apple were forced to support sideloading:

- **More harmful apps would reach users because it would be easier for cybercriminals to target them – even if sideloading were limited to third-party app stores only.** The large amount of malware and resulting security and privacy threats on third-party app stores shows that they do not have sufficient vetting procedures to check for apps containing known malware, apps violating user privacy, copycat apps, apps with illegal or objectionable content, and unsafe apps targeted at children. Users would now be responsible for determining whether sideloaded apps are safe, a very difficult task even for experts. In the rare cases in which a fraudulent or malicious app makes it onto the App Store, Apple can remove it once discovered and block any of its future variants, thereby stopping its spread to other users. If sideloading from third-party app stores were supported, malicious apps would simply migrate to third-party stores and continue to infect consumer devices.

- **Users would have less information about apps up front, and less control over apps after they download them onto their devices.** Users may not get accurate information about apps they sideload through third-party app stores or via direct downloads because these app stores would not be required to provide the information displayed on the App Store product pages and privacy labels. And features like App Tracking Transparency and parental controls that allow users to control what iPhone data, hardware, and services can be accessed by those apps (such as the device's location, microphone, and camera) either would not be available or would be much easier for malicious actors to manipulate. Large companies that rely on digital advertising allege that they have lost revenue due to these privacy features, and may therefore have an incentive to distribute their apps via sideloading specifically to bypass these protections. Privacy on the iOS platform would therefore be eroded.

- **Some sideloading initiatives would also mandate removing protections against third-party access to proprietary hardware elements and non-public operating system functions.** This would undermine core components of platform security that protect the operating system and iPhone data and services from malware, intrusion, and even operational flaws that could affect the reliability of the device and stop it from working. This would make it easier for cybercriminals to spy on users' devices and steal their data.

Even users who don't want to sideload and prefer to download apps only from the App Store would be harmed if sideloading were supported.

- **Users could be forced to sideload an app they need for work or school.** Users also may have no choice other than sideloading an app that they need to connect with family and friends because the app is not made available on the App Store. For example, if sideloading were permitted, some companies may choose to distribute their apps solely outside of the App Store.
- **Cybercriminals may trick users into sideloading apps by mimicking the appearance of the App Store, or by touting free or expanded access to services or exclusive features.**

By reviewing every app before it becomes available on the App Store to ensure it is free of malware and accurately represented to users, and by swiftly removing apps from the App Store if they are found to be harmful and limiting the spread of future variants, Apple protects the security of the ecosystem. **Sideloading, through either direct downloads or third-party app stores, would undermine Apple's security and privacy protections, and is not in the best interest of users' security and privacy.**

"We're trying to do two diametrically opposed things at once: provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. This is no easy task."

Steve Jobs, October 17, 2007

Contents

When iPhone was developed, PCs were the world's primary computing tools, and they were riddled with viruses. PC users often encountered serious reliability issues because downloading software or visiting a website could result in their machines becoming infected with malware. Apple designed iPhone with the knowledge and intention that it would be a highly personal device where users would store some of their most sensitive and personal information, and could be used by a much larger and more diverse user base than was the case with PCs. They would keep it with them wherever they went and rely on it during emergencies. iPhone could not fall victim to the fate of PCs – it needed to be different.

To provide reliability and security for users while establishing a platform for third-party developers to create and distribute apps, Apple built industry-leading security protections into iPhone and created the App Store, a trusted place where users could safely download vetted third-party apps. This approach has been effective: It is extremely rare for a user to encounter malware on iPhone. However, some are demanding that Apple support the distribution of apps outside of the App Store, through direct downloads or third-party app stores, a process also referred to as "sideloading." Supporting sideloading would cripple the privacy and security protections of the iOS platform and expose users to serious security risks.

You can read Apple's June 2021 paper, **"Building a Trusted Ecosystem for Millions of Apps: The important role of App Store protections,"** to see how a family's everyday experience using their iPhone would be different with sideloading.

Sideloading on iPhone would open opportunities for cybercriminals. Malicious actors would be galvanized to develop tools and expertise to attack iPhone users because of the additional opportunities and distribution channels sideloading would provide. The increased risk of malware attacks would put all users at greater risk, even those who prefer to download apps only on the App Store. Plainly, sideloading is not in the best interest of users. Developers would be harmed as well, because the increased threat from sideloading would erode users' trust in the ecosystem, resulting in many users downloading fewer apps from fewer developers, and making fewer in-app purchases. **Developers would also be harmed by the proliferation of fake and copycat apps, as well as pirated apps.**

The current mobile threat landscape

Mobile security threats are increasingly common, especially on platforms that support sideloading. The European Union's cybersecurity agency, ENISA, reported the detection of 230,000 new malware infections *per day* – i.e., 84 million per year – in 2019 and early 2020.[1] Kaspersky Lab, Europe's largest cybersecurity services provider, estimated that in 2020, nearly 6 million attacks per month affected Android mobile devices owned by its clients.[2,3]

These threats are predominantly present on platforms that support sideloading: Recent studies have shown that devices that run on Android – a platform that supports sideloading – have an estimated 15 to 47 times more infections from malicious software than iPhone.[4,5]

Mobile apps containing security threats pose significant risks.[4,6] As a result, app review processes in first-party app stores (i.e., the App Store on iOS devices, and Google Play on Android devices) have become increasingly thorough and necessary to prevent security threats from reaching consumers. However, such app review protections are not always thorough, or even available at all, when users sideload apps from third-party app stores or direct downloads.

Malware-infected mobile apps put all stakeholders in the mobile ecosystem at risk. While consumers are often the primary targets, malware attacks can harm and expose developers, online advertisers, and even businesses that are not direct participants in the mobile app ecosystem. Consumers who are victims of malware attacks are defrauded by cybercriminals, have their privacy and sensitive data compromised, and waste time and energy dealing with the consequences of the attacks.[7] Malware-infected mobile apps are also often the first step in complex multi-step campaigns that allow cybercriminals to carry out a variety of attacks targeting a victim's financial resources.[8,9,10] On platforms that support sideloading, many consumers have also needed to add antivirus services on their devices to attempt to stem the problem – at a cost of $3.4 billion per year for those services. In 2021, an estimated 1.3 billion smartphones worldwide were equipped with security solutions – four times as many as in 2016.[11] Cybercriminals, however, are always a step ahead, meaning antivirus services are an incomplete patchwork solution to the growing malware problem.[12]

Malware designed to infect an individual's mobile device can also affect corporate data and corporate networks. There are many ways that hackers attack companies, for example by using phishing or attacking unpatched systems, and mobile malware has become an additional avenue to do so.[13,14,15] With many organizations around the world adopting Bring Your Own Device (BYOD) policies that encourage employees to use their personal devices on corporate networks, mobile malware attacks can provide bad actors a direct route into corporate networks, which has led to an increase in threats targeting mobile devices.[16,17,18] Many IT and security experts have attributed certain data breaches to employees failing to secure sensitive corporate information on their mobile devices, and a study of corporate data breaches identified Android apps as one delivery method for malware.[10,19] Once bad actors manage to gain access to a corporate network, firms then face all types of attacks and security risks, such as ransomware, data theft, or loss of control of their network, all of which can lead to the loss of customer trust and litigation.[20]

CORPORATE COSTS OF MALWARE ATTACKS

Firms face high costs from malware attacks, which can originate via mobile apps, among other sources:

One single mobile device infected with malware **costs an organization an average of nearly $10,000.**[19]

Among 1,800 US firms, **46 percent had at least one employee download a malicious mobile app** that threatened the company's network and data.[21]

DATA BREACHES

Data breaches, which can originate from mobile app malware, cost firms an average of **over $4 million per breach**, with estimates reaching up to **$50 million.**[19, 22]

LOST BUSINESS

Out of that $4 million, **over $1.5 million** is due to lost business. This cost includes the harm to reputation, which makes it more difficult for these firms to acquire new customers.[22]

RANSOMWARE

More than half of companies surveyed in France, Spain, Germany, and other European countries suffered a ransomware attack in 2019. Ransomware attacks, which can originate from mobile malware, cost companies **more than $750,000** to remediate on average.[23]

Developers and advertisers are also harmed by cybercriminals. When pirating an app, cybercriminals illegally distribute another developer's app, primarily through third-party sources (including third-party app stores), causing the developer to lose out on the app's revenue.[24,25] Cybercriminals may remove or replace the monetization tools that allow the developer to earn revenue, such as in-app purchases or advertising. In other cases, bad actors copy the design, branding, or content from another developer, profiting off of stolen intellectual property.[26,27] This means that app piracy and intellectual property theft cause developers to lose out on revenue. Several game developers, for example, have reported that 90 percent of their app installations on Android devices are pirated versions for which they earn no revenue.[24,25] Cybercriminals often target paid games, profiting by creating pirated versions of successful games such as Monument Valley, the Grand Theft Auto series, or Alto's Adventure.[24,25]

Advertisers are also harmed by mobile malware when cybercriminals and hackers use techniques such as click fraud and ad stacking, which frequently operate through sideloaded apps.[28] Click fraud malware automatically directs traffic to web pages containing ads or clicks on ads to generate revenue on a per-view or per-click basis, respectively.[29] With ad stacking, malware layers multiple advertisements over one another so that, while the user only sees the top one, the advertiser is fraudulently billed for all the ads.[30] Damages to legitimate advertisers from inflated, fraudulent ad traffic are estimated to amount to billions of dollars.[30,31]

Threats to mobile users have only compounded due to the increased reliance on mobile devices driven by the coronavirus pandemic. For example, consumers are now more likely to store personal health information on their devices, a type of valuable data that hackers can sell to multiple buyers.[32,33] Firms increasingly rely on BYOD policies to support remote work.[17] These dynamics have created more opportunities for bad actors and increased the number of threats to mobile users. For example, mobile phishing – using fake messages to trick users into revealing confidential information or downloading malware – has increased by 37 percent.[34] Hackers have embedded malicious malware in COVID-19 apps and resources.[35] And healthcare-related networks have experienced 15 percent more coronavirus-related malware attacks per user across mobile devices, tablets, and PCs than the average network.[34]

Snapshot of common consumer mobile malware

Mobile malware attacks against consumers take many forms and use various tactics and techniques to attack them. The most common types of consumer mobile malware are adware, ransomware, spyware, and banking and other credential-stealing trojans masquerading as legitimate apps. (See Snapshot below.) Once attackers gain access to a device, they often use multiple tactics to exploit their targets: For instance, they can infect the device with both adware and spyware.

Snapshot of common consumer mobile malware

	Adware	Ransomware	Consumer spyware	Banking and credential-stealing trojans
GOAL	Generate ad revenue by serving the user aggressive (or fraudulent) ads	Extract money from infected user, promising to "release" a hijacked device in exchange	Use data to target users Sell data to hackers Conduct intimate partner surveillance (IPS)	Access a device to steal banking information or other user login credentials
IMPACT ON USER	Nuisance in the form of excessive pop-up ads Harms performance of device	Loss of access to device and critical files Data loss Financial harm if user pays ransom	Violate users' privacy IPS: Enables abuse, potential physical and mental harm	Stolen credentials (e.g., banking login, social media account login) Harm from stolen credentials (e.g., fraud)

Note: This table reflects classifications proposed by cybersecurity firms such as Kaspersky Lab, Malwarebytes, WeLiveSecurity by ESET, Norton, and Nokia, and government agencies such as the European Union Agency for Cybersecurity (ENISA).

Adware. Present in over half of mobile attacks, adware serves users invasive advertisements to generate advertising revenue.[36,37,38] Adware can infiltrate mobile devices through apps, manifesting as pop-ups, redirections, clicker trojans, and unwanted installations.[39]

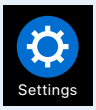
HiddenAds: Adware that hides inside free apps and games to display intrusive ads

WHO IT AFFECTS

Since its discovery in 2020, there have been over 30,000 recorded HiddenAds attacks, affecting users worldwide.

HOW IT REACHES A USER'S DEVICE

Apps infected with HiddenAds adware masquerade as genuine Android apps, such as fake versions of FaceApp – a popular photo modification app – and a Call of Duty game.[37] YouTube videos advertise these fake apps as free versions of legitimate apps and include download links.



HOW IT WORKS

HiddenAds displays various pop-up ads and website redirections in the device's browser to generate advertising revenue for the malicious actor.

HOW IT HIDES

Once installed, the app appears as a fake settings icon. The icon can even disappear with the adware still running in the background.

Other examples of adware

FakeAdsBlock, a sideloaded Android trojan posing as a legitimate ad blocker, pollutes the device with pop-ups and redirections. It is very difficult to remove.[40]

Android.Click.312.origin clicker trojan is embedded in many legitimate apps. It generates ads on the apps and can load websites without user knowledge.[41]

CopyCat infects Android devices with adware and rooting malware. It spreads through tampered copies of popular apps released on third-party app stores.[42] In two months in 2016, CopyCat malware infected more than 14 million Android devices around the world.[43]

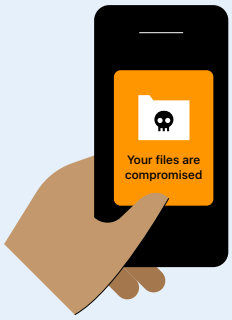
Ransomware. Another common type of mobile security attack, ransomware, generally targets individual users by blocking a device's interface, preventing users from using it until a ransom is paid, or by encrypting files in the device and only decrypting them after a payment is made.[44,45] Cybercriminals using ransomware often steal sensitive data and threaten to spread it.[46] In 2020, more than 4.2 million mobile users in the US alone were victims of mobile ransomware attacks.[47,48] These attacks have become more common, fueled by the coronavirus pandemic and the rise of cryptocurrency, which cybercriminals can trade to avoid being traced.[34,47,49,50]

Other examples of ransomware

Fusob ransomware trojans are designed to lock a device while stealing call history, location history, and other sensitive data. These trojans have targeted users in Europe and the US.[53,54]

MalLocker.B, a family of Android malware distributed via sideloading, displays a ransom note over every other app window, ensuring that the target cannot use any other features of the phone.[55,56]

CryCryptor: Ransomware poses as an official COVID-19 tracing app and encrypts users' files



CryCryptor ransomware poses as an official COVID-19 tracing app from government agency Health Canada to trick users into sideloading it. Once installed, CryCryptor encrypts files on the device and provides an email address to contact to proceed with ransom payment and file recovery.[51,52]

WHO IT AFFECTS

CryCryptor targets Android users in Canada.

HOW IT REACHES A USER'S DEVICE

In June 2020, mere days after the Canadian government announced plans to roll out a COVID-19 contact-tracing app, the cybercriminals behind CryCryptor created two fake Health Canada websites through which they offered their ransomware app. Preying on people's anxiety and uncertainty surrounding the COVID-19 pandemic, they tricked Android users into sideloading CryCryptor from these fake websites.

HOW IT WORKS

CryCryptor was developed from CryDroid, an open-source ransoware. Once downloaded, CryCryptor requests permission to access files on the Android device. Then, the malware encrypts common file types, including photos, videos, and PDFs. A ransom note is attached to each encrypted file directory, containing an email address to contact regarding payment and file recovery.

Examples of spyware

FluBot is a strain of spyware that behaves and spreads very similarly to FakeSpy. (See below.) FluBot poses as a DHL package tracking app across Europe, and focuses its attacks in the UK and Finland.[68,69]

SpyNote spreads as a sideloaded, fake version of Netflix that can take control of a device's microphone, contacts, and messages.[70]

HelloSpy, a type of stalkerware available only through side-loading, records the target's GPS location, phone calls, messages, photos and videos, and other data.[71] It is marketed to "catch cheating spouses."[72]

Consumer spyware. Spyware monitors the device's user and steals sensitive information, such as messages, photos, and videos.[57] Spyware can harm both individuals (e.g., via identity theft or stalking) and businesses and organizations (e.g., via corporate espionage).[58] Certain invasive forms of spyware can directly access a device's microphone or camera.[59,60] Consumer spyware is distinct from the highly sophisticated and narrowly targeted forms of spyware executed by nation-states via intelligence agencies. Unlike spyware developed or sponsored by nation-states, consumer spyware is designed to target a broad set of users, and is relatively cheap to produce and distribute on platforms that support sideloading. In 2020, a third of all Android malware attacks involved spyware.[4]

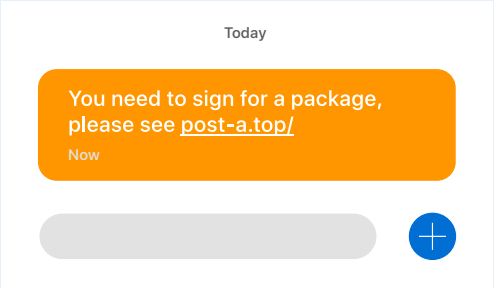
Spyware has also been used by abusers to surveil intimate partners and their mobile devices. Apps containing such software, known as **stalkerware**, are used to track location, messages, emails, and photos, and to access the device's camera in real time. The use of such apps is associated with harassment, stalking, and domestic violence. In the last few years, the FTC has taken action against two US companies that sold stalkerware that allowed stalkers and domestic abusers to track their victims on Android devices.[61,62] In both cases, even though the apps were not distributed on Google Play, abusers were able to sideload the apps onto victims' devices. The FTC's intervention was therefore critical in removing the apps from distribution.[61,63]

Kaspersky Lab **discovered over 50,000 users who were affected by stalkerware** in 2020.[65]

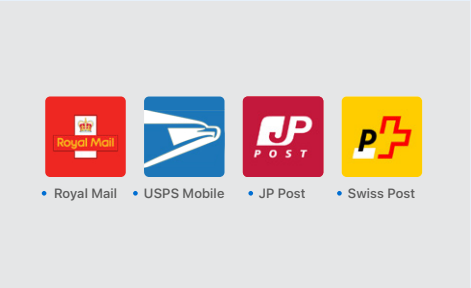
One survey found that **more than half of abusers tracked their victims' mobile phones** using stalkerware apps.[64]

The **vast majority of stalkerware is distributed outside of first-party app stores.**[65]

FakeSpy: Malware poses as fake package delivery messages to spy on users and steal their data



↳ Fake messages attempt to trick users into sideloading FakeSpy via fraudulent postal service apps.



↳ FakeSpy app icons mimic those of legitimate postal services around the world.

FakeSpy uses SMS phishing to trick people into sideloading an Android app that masquerades as a legitimate postal service app. Once downloaded, it steals sensitive information from the device.[66,67]

FakeSpy is actively evolving to include new evasion strategies and spying capabilities. FakeSpy proliferates by sending SMS phishing messages to the infected user's contact list.[66] It is also expanding to mimic more legitimate postal services around the world to target new groups of users.

WHO IT AFFECTS

Android users in France, Switzerland, Germany, the UK, the US, Japan, and Taiwan, among others.

HOW IT REACHES A USER'S DEVICE

A target receives a text message claiming that the postal service attempted to deliver a package, and that the user should track or sign for it. The message contains a link to a website that prompts users to sideload the fake delivery tracking app. FakeSpy has masqueraded as mail services in France (La Poste), Switzerland (Swiss Post), Germany (Deutsche Post DHL), the UK (Royal Mail), the US (USPS), Japan (Japan Post), and Taiwan (Chunghwa Post). To trick potential victims, the sideloaded app's icon resembles the official app icon for one of these official mail services.

HOW IT WORKS

Once the user has sideloaded the app, it requests permissions that allow it to obtain text messages, contact lists, call logs, network information, recently run tasks, and information about other apps.

HOW IT HIDES

After the user launches the app, it deceptively redirects them to the real postal service website, which helps the app remain undetected as malware.

Banking and other credential-stealing trojans. Common types of mobile malware are banking and other credential-stealing trojans. Disguised as legitimate apps, they aim to steal users' credentials from banks, government accounts, or social media accounts, for example. Some banking trojans are capable of bypassing two-factor authentication security measures.[73] The goal of banking trojans is to ultimately steal the credentials and money from the target's bank account.[74] Banking trojans are most commonly sideloaded.[74]

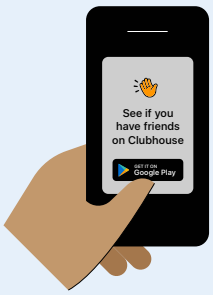
Other examples of banking and credential-stealing trojan apps

Banker.BR, an Android trojan, uses screen overlays to steal banking information in Spain and Portugal.[77]

TeaBot, a banking trojan, impersonates many popular apps in Western Europe to steal banking information and gain remote access to devices.[78,79]

Since 2017, Anubis banking trojans have posed as the apps of over 300 financial institutions and other types of apps.[80] Once installed and activated, the apps request unnecessary permissions that allow them to execute nefarious commands. The malware predominantly uses phishing to trick people into providing their bank account information.

BlackRock: An Android trojan poses as a fake version of Clubhouse to steal login credentials



BlackRock is an Android trojan that steals login credentials from over 450 online services, and tricks users into sideloading it by posing as the Clubhouse app.[75,76]

WHO IT AFFECTS

Android users in Europe and other parts of the world.

HOW IT REACHES A USER'S DEVICE

BlackRock spreads via a spoofed version of the Clubhouse website. When a user clicks "Get it on Google Play," the trojan is automatically downloaded.

HOW IT WORKS

The trojan poses as a Google update, and asks for Accessibility Service privileges. With those privileges, it can grant itself further privileges to function without requiring user input.[76] The next time the user opens one of the targeted apps, such as BBVA, Lloyds Bank, or Facebook, the trojan launches a screen overlay window over the app's interface that records the user's login credentials as they are typed. The trojan can access text messages, which allows it to defeat two-factor authentication.

HOW IT HIDES

When the trojan is first launched on the device, it hides its app icon, thereby making itself invisible to the user.

Other forms of malware. Other well-known forms of malware, while similar to consumer malware, are typically not delivered through mobile apps and not targeted at everyday consumers.

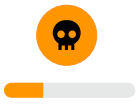
- **Nation-state spyware** is developed and sponsored by state actors via intelligence agencies or private contractors, often with the goal of advancing a nation's intelligence or national security objectives. Unlike consumer spyware, nation-state spyware is highly sophisticated, costs millions of dollars to develop, is typically not delivered via apps, and is used to target specific individuals.[81,82,83]

- **Enterprise ransomware** occurs when criminals take control over corporate networks and demand ransom from the affected company in exchange for restoring access or preventing the cybercriminals from publicly releasing sensitive data stolen from the victim's network.[84] Enterprise ransomware differs from mobile ransomware attacks (in which a consumer's device and personal data are held ransom), although employees' mobile devices can be an entry point for cybercriminals targeting corporations.

How mobile malware attacks access users' devices

Cybercriminals and hackers can distribute malware to users through third-party app stores and via direct downloads from websites or even as email attachments.[8] As described below, a huge majority of malware – over 99 percent – comes from sideloaded apps, because first-party stores like the App Store have protections in place that prevent these distribution techniques from targeting users. **The most common way for malware attackers to reach their targets is through social engineering or spoofing,** i.e., using deception and manipulation as techniques to obtain users' trust and get access to their devices. One study found that 98 percent of all cyberattacks rely on social engineering.[18] Hackers sometimes use social media networks to spread scams and attacks, exploiting people's trust in their friends and family.[85,86] There are many ways in which spoofing attacks, which are more likely to happen through sideloaded apps, try to obtain users' trust:

Copycat apps (or fake apps) copy the name, interface, and functionalities of other apps to acquire some of their users.[87,88] They capitalize on users' trust in popular (and legitimate) apps, such as Netflix, Candy Crush Saga, and Clubhouse, possibly hurting the image and reputation of those legitimate developers.[70,89] Commonly downloaded via sideloading, these apps have fooled tens of millions of users worldwide.[43,90,91]



Fake system updates are a common spoofing technique in which malware pretends to be a system update, tricking users into downloading it and providing access to their devices. For example, a sideloaded Android app posed as a system update to infect users' devices.[92]

Email and phishing messages are another technique that malware attacks employ to convince users to download malware, appearing to be from senders the users trust.[8,93] These phishing messages commonly spread through social media apps. For example, FlyTrap, a malicious trojan on third-party app stores, spreads by hijacking users' Facebook accounts to send personalized messages to victims' social connections with links to the trojan.[85] In Spain, people received mobile messages advertising and containing a link to sideload a fake and malware-ridden "Coronavirus Finder" app.[94] In India, users received personalized SMS messages urging them to download a copycat of the tax-filing app from the official Income Tax Department of India. The app contained malware designed to steal their personal and financial information.[95]

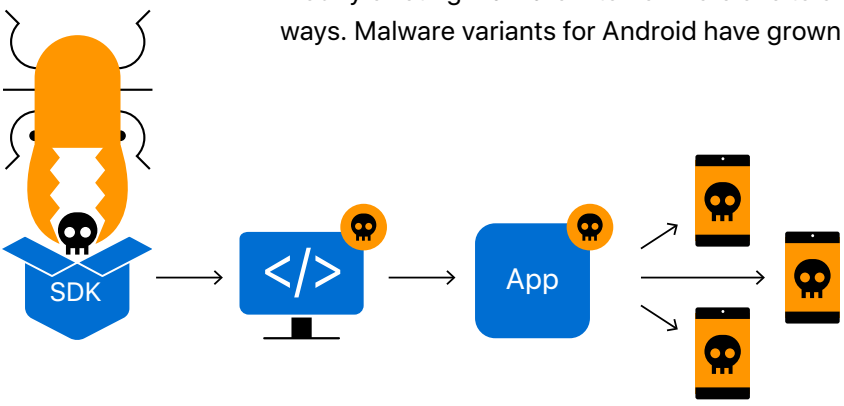
Website spoofing creates legitimate-looking websites that contain malware.[96] These websites frequently lead to malicious apps available for sideloading. Examples include the aforementioned BlackRock Android trojan that spoofs the website of the Clubhouse app, luring unsuspecting users into downloading the trojan app instead of the legitimate app.[76]

Scareware tricks users by claiming to detect threats to the device, often offering solutions to those threats that involve sideloading an app containing malware.[97,98] For instance, Armor for Android falsely warns people that malware has been detected on their devices, advising users to download its antivirus app, which then scams them.[99]

Potentially unwanted applications are software packaged along with genuine apps that tailgate their way onto devices when users install the genuine apps. They can contain malware and drain devices' resources.[100] For example, over 100 Android apps, with more than 4.6 million combined downloads, contain the Soraka potentially unwanted application adware.[101]

Hackers can also use supply chain attacks to infect user devices. Instead of tricking users into downloading infected apps, these attacks infiltrate and spread by tricking developers of legitimate apps.[102] One way those attacks have proliferated is through infected software development kits (SDKs), the building blocks used by app developers to build apps.[103] Cybercriminals and hackers can deliver malware to users by modifying and inserting malicious code in SDKs used by unsuspecting developers.[104] These attacks take advantage of the trust that users have in apps made by legitimate developers. For example, SWAnalytics, an Android data analytics SDK, hides Operation Sheep, a contact-stealing malware package. As of March 2019, 12 Android apps infected with this malware, with over 111 million downloads, had circulated in major third-party app stores.[105]

Hackers often reuse the same malware strain, which they repackage into variants. Rather than creating entirely new malware – a costly endeavor – hackers modify existing malware into new versions to either improve it or spread it in other ways. Malware variants for Android have grown significantly in recent years.[106,107]



The risks of opening the ecosystem

Because cybercriminals and hackers rely heavily on apps to spread malware, first-party app stores have invested in extensive processes to screen and remove malicious apps.[108,109,110] As the threat of malware has increased, these screening processes have become stricter and have dedicated a greater amount of resources to reviewing apps.[111,112] And, if harmful apps are found on first-party app stores, they can be removed from distribution, preventing further user exposure.[113,114]

On the other hand, the large amount of malware on third-party app stores shows they do not have sufficient vetting procedures to check for harmful apps (and direct download websites have no independent vetting), so cybercriminals and hackers have relied on third-party app stores or direct downloads to spread their apps, taking advantage of the lack of oversight and the inability to control the spread of malware: Over 99 percent of known mobile malware originates on third-party app stores.[15,18] A study of malicious apps on Android found that once a malicious app is detected and removed from one app store, it often simply migrates to other third-party stores, and thus continues infecting consumer devices.[115,116]

Because Android supports sideloading, malware has been able to spread on that platform more easily. Android smartphones are the most common mobile malware targets and have recently had between 15 and 47 times more infections from malicious software than iPhone.[4,5] A study found that 98 percent of mobile malware targets Android devices.[18] This is closely linked to sideloading: In 2018, for example, Android devices that installed apps outside Google Play, the official Android app store, were eight times more likely to be affected by potentially harmful applications than those that did not.[103] For example, as previously discussed, HiddenAds, CopyCat, FakeSpy, and BlackRock are all prominent malware strains that reached Android users via third-party sources. In addition, because cybercriminals and hackers rely on sideloading to spread pirated apps, piracy and intellectual property theft are more common on Android devices.[24,25,117] On the other hand, iOS users are unlikely to be exposed to malware, and many of the rare malware attacks on the platform are narrowly targeted attacks, often carried out by nation-states.[82,83,118] Experts generally agree that iOS is safer compared to Android, in part because Apple does not support sideloading.[5]

If regulations force platforms to support sideloading without any user protections, the harm to users could be even greater. The Android platform currently retains some features that discourage sideloading by adding "friction" for users – additional steps and warnings that prevent users from sideloading apps without realizing it. For example, devices are set up not to sideload as a default option, and corporate entities can disallow device-wide sideloading on employees' devices.[119,120,121] Should regulations force platforms to support sideloading without any friction, the threat of malware, piracy, and intellectual property theft on both platforms would likely be higher as a result.

The limited mechanism to distribute apps outside of the App Store

Apple's own experience with supporting the ability of a limited number of enterprise developers to distribute apps outside of the App Store shows that cybercriminals and even for-profit companies will go to great lengths to bypass the App Store so they can spread malware and other illegitimate apps. Apple created the Developer Enterprise Program to provide a way for large organizations to develop and privately distribute apps (for instance, confidential apps that cannot go through App Review), for use only by their organization's employees. Under the tightly controlled program, Apple issues certificates to businesses, which allow them to distribute apps directly to their employees under their IT departments' supervision.

Despite the program's tight controls and limited scale, bad actors have found unauthorized ways of accessing it, for instance by purchasing enterprise certificates on the black market. Bad actors have used illegitimately obtained enterprise certificates to distribute apps that violate App Store policies, including apps containing malware such as Goontact (see below) and pirated versions of popular iOS apps.[122,123] Abuse of the Developer Enterprise Program is not limited to cybercriminals. In 2019, for example, Apple revoked Facebook's enterprise certificate because it was used to distribute a VPN app called Facebook Research that collected mobile data and usage habits – such as web searches and browsing history, messages, and location data from Facebook users – targeting some as young as 13.[124,125] Enterprise certificates are meant only for internal use by a company, and are not intended for general app distribution, as they can be used to circumvent App Store and iOS protections.

Apple has increased efforts to tighten controls on the program and add user protections, but abuse has persisted. **This demonstrates the enormous risk posed by forcing Apple to support the ability of any developer to distribute apps outside of the App Store to all iPhone users.** If the option to distribute apps via sideloading were available on a massive scale, without any restrictions, and with Apple powerless to revoke certificates from bad actors in cases of abuse, malware and other forms of illegitimate apps would run rampant.

Apple tightly controls the Developer Enterprise Program

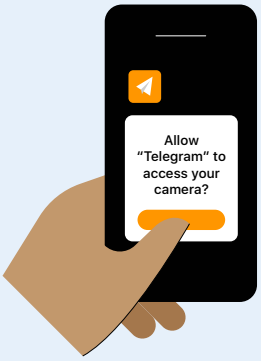
Only legal entities that have validated their reasons for using the program are eligible, and they can only distribute apps to their employees.

Apple can and does revoke the developer certificates of businesses that misuse them.

Employees who download apps created through the program must go into their device settings and affirm that they trust the business – their employer – which ensures users truly intend to download an app from outside of the App Store.

Most enterprise customers do not use the program, as Apple offers businesses alternative ways to distribute apps to their employees to limit participation in the Developer Enterprise Program. For instance, businesses can submit apps for custom app distribution on the App Store, a process by which each app goes through the App Review process before becoming available within the organization. Learn more here: **developer.apple.com/custom-apps/.**

Goontact: Adult video chat sites lure targets into downloading spyware



Goontact is multi-platform spyware that reaches users’ devices through infected adult video chat apps. The spyware targets Android users via sideloaded apps, and is also able to target iOS users by abusing the Apple Developer Enterprise Program.[122]

WHO IT AFFECTS

Goontact is currently active across both Android and iOS platforms, and primarily targets users in China, Japan, Korea, Vietnam, and Thailand.

HOW IT REACHES A USER’S DEVICE

Malicious actors lure targets to websites promising adult video chats. However, they are instead connected with Goontact operators.

Under the pretense of improving video or audio quality, operators prompt targets to sideload a well-known video-chatting app (such as Telegram) from a website that mimics the design of a first-party app store, guiding them through the process and coaxing them to enable access privileges. However, the sideloaded app is fake and infected with spyware.

HOW IT WORKS

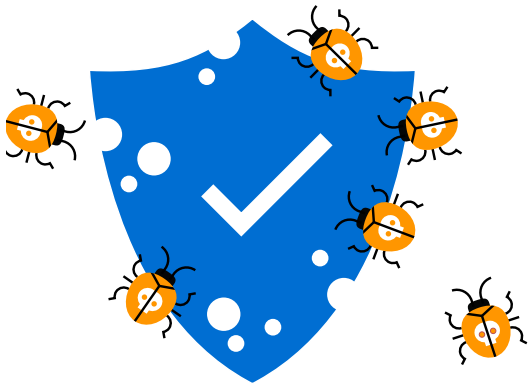
After Android users accept a prompt to grant Goontact permissions, it collects data on contacts, SMS messages, location, photos, and the device identifier. On iOS devices, the spyware can only collect contacts and device identifier data.

HOW IT TARGETS iOS USERS

Goontact abuses the privileges of the Apple Developer Enterprise Program by obtaining unauthorized enterprise certificates. While Apple revokes these certificates as soon as they are discovered, the malicious actors can keep spreading their malware through sideloading when they procure additional illegitimate certificates.

ADDITIONAL LAYER OF ATTACK

During the first video chats with a Goontact operator, the cybercriminals record a compromising video of the target to use as blackmail. After users download the app, the spyware steals their contacts and the cybercriminals threaten to release the video to their contact lists unless a ransom is paid.



The impact of sideloading on the iOS ecosystem

Forcing sideloading onto the iOS ecosystem would make iPhone less secure and trustworthy for users. This would be true regardless of whether sideloading occurred via direct downloads or through third-party app stores. Researchers agree that iPhone is the most secure consumer mobile device, and it is rare for any user to encounter malware on iPhone.[5] Because iPhone provides users with powerful and multi-layered security protections, it is usually not possible for cybercriminals and hackers to attack iOS devices at scale. Through the App Review process, Apple's goal is to ensure that apps on the App Store are trustworthy and safe. Apple is constantly improving this process, continually updating and refining App Review's tools and methodology.

Forcing Apple to support sideloading on iOS through direct downloads or third-party app stores would weaken these layers of security and expose all users to new and serious security risks: It would allow harmful and illegitimate apps to reach users more easily; it would undermine the features that give users control over legitimate apps they download; and it would undermine iPhone on-device protections. Sideloading would be a step backwards for user security and privacy: Supporting sideloading on iOS devices would essentially turn them into "pocket PCs," returning to the days of virus-riddled PCs.

First, if sideloading were supported, it would be easier for harmful apps to reach users. Direct downloads are unvetted, and the large amount of malware that proliferates on third-party app stores shows that those stores do not have sufficient vetting procedures to check for harmful apps. Users would now be responsible for determining whether sideloaded apps are safe, a very difficult task even for experts. Apple currently protects users by vetting apps and developers on the App Store, keeping illegitimate apps out, and quickly containing the spread of harmful apps.

You can read Apple's recent paper, **"Building a Trusted Ecosystem for Millions of Apps,"** to learn more about how Apple's device protection and App Review keep your device safe.

Malware: Sideloading would expose iOS users to apps that contain known strains of malware. App Review screens all apps and app updates submitted to the App Store to check for various types of known malware, including infected SDKs used in supply chain attacks. By contrast, known malware such as HiddenAds remains present on Android third-party app stores. (See above.)

Spoofing: If sideloading were supported on iOS, malicious actors would be able to distribute copycat versions of popular apps that trick users. On the App Store, apps come from known and vetted developers only, and their content is reviewed by a member of the App Review team. This process works to prevent, for example, a trojan app posing as a fake version of Clubhouse and stealing user login credentials. (See above.)

Illegal, pirated, and stolen content: Sideloading would expose users to apps with illegal content, such as illegal gambling apps, pirated apps, or apps containing stolen intellectual property. They would be able to spread on the iOS platform unchecked via third-party sources. Apple checks all apps submitted to the App Store for illegal content prohibited by Apple's policies.

Unsafe apps targeted at children: Supporting downloads outside of the App Store would mean that parents may inadvertently sideload apps appearing to be kid-friendly but which actually put their children at risk. App Store policies enforce strict guidelines around data collection and security on apps in the Kids category. For example, these apps may not include links outside of the app, send personally identifiable information to third parties, or contain third-party analytics or advertising.

Unchecked spread of harmful apps: In the rare cases in which a fraudulent or malicious app makes it on the App Store, Apple can remove it immediately once discovered, thereby stopping its spread to more users. Apple also identifies and blocks variants of the original malware that cybercriminals try to repackage in other apps, limiting its ability to mutate and spread further. For example, XcodeGhost was a form of malware that spread through an infected version of Xcode (Apple's environment for writing and compiling apps) that unsuspecting developers downloaded from a third-party website rather than from the Apple developers' website.[126] Because the infected apps were centrally distributed through the App Store, Apple was able to swiftly work with cybersecurity firms to identify and remove them.[127] A mechanism such as sideloading, without centralized review, would make it impossible to notify all impacted developers, and to control the spread of harmful apps, because removing them from the App Store would not prevent them from continuing to spread through third-party app stores and direct downloads. Researchers have found that when harmful apps are removed from an app store on the Android platform, malicious actors simply move them to alternative app stores.[115]

Second, if sideloading were supported on iOS, users may not get accurate information about apps they download via direct download or through third-party app stores. Also, features that allow users to control what data apps are able to access would either not work, or would be much easier for malicious actors to manipulate. The App Store requires all developers to provide reliable information about apps, and Apple has designed many features that give users the ability to control what data apps are able to access.

Permissions: App Review checks that the app doesn't request access to sensitive permissions or data that are unnecessary for the app to function (for example, a weather app requesting access to the microphone or to health data). App Review also checks that apps do not make misleading or false claims when requesting permissions from users. If sideloading were supported, however, sideloaded apps would not have to be checked to see if they are improperly requesting and obtaining sensitive permissions and data, such as access to the device microphone or location data, regardless of whether this permission is needed for the app to function. Sideloaded apps may also attempt to trick users into granting permissions using manipulative or false messages.

Reliable information for users: On the App Store, app developers are required to submit a description of their app and its features, screenshots of the app, and privacy information explaining what kind of data the app links to users' identities and whether that data is used to track them across third-party websites and apps. This ensures that users know what to expect when deciding whether to download an app and that they are not misled by malicious actors impersonating trusted developers. If sideloading were supported, users could not be sure that apps downloaded outside the App Store are what they expected to download, and they may not have information on the apps' privacy practices.

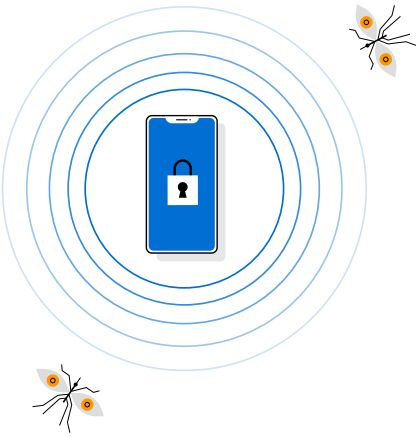
Privacy protections: Privacy is at the core of Apple's ecosystem. All apps on the App Store need to get users' permission before tracking them across third-party apps or websites through the App Tracking Transparency feature. Sideloading would render this protection ineffective: While users could prevent sideloaded apps from accessing their Identifier for Advertisers (IDFA), sideloaded apps could access other device or user data, and their developers would not be required to abide by choices made by users to opt out of tracking. As a result, users' data may be collected and shared without their permission. In addition, developers may have different incentives, and may choose not to protect users' data the same way that Apple does. Some developers allege that they have lost advertising revenue due to App Tracking Transparency, and thus would have an incentive to sideload their apps specifically to bypass these privacy protections.[128] Furthermore, some developers, including social media platforms, have a history of abusing user privacy and safety, and have created apps that violate App Store guidelines designed to protect iOS users.[124,129]

Learn more about Apple's privacy protections

To learn more about how the App Tracking Transparency and privacy labels on the App Store give you control and transparency on how apps collect and use your data, read **"A Day in the Life of Your Data"** and visit **apple.com/privacy/control**.

Parental controls: Apple has designed features that give parents control over how kids use iOS devices. Screen Time gives parents an understanding of the time kids spend using their devices, and allows parents to limit the amount of time they can spend each day on certain apps and websites. The Ask to Buy feature allows parents to approve or decline kids' app downloads and purchases made via in-app purchasing, and has a 15-minute timeout to prevent subsequent purchases. Sideloading would weaken these parental control features, which could be easily bypassed by apps downloaded outside of the App Store. For instance, a game app could identify itself as an education app to evade Screen Time limits on game usage. And non-App Store purchases on sideloaded apps would not be controlled by Ask to Buy.

Report a Problem: Apple provides features that allow users to request refunds for some purchases from the App Store, as well as to report app privacy violations or safety issues. These features ensure that users have recourse if something goes wrong, such as being a victim of fraud or scams. Under sideloading, there would be no guarantee that third-party app stores would offer fair, clear, and consistent refund policies, or provide customer support in cases where there is a problem with an app.



Subscriptions: Apple's subscription management tool allows users to view all their paid subscriptions made through in-app purchases in a single place. Users can see how much and how often they will be charged for in-app subscriptions, and they can easily cancel them. With sideloading, many developers could choose to make their apps incompatible with these features, and make it confusing and time-consuming for users to cancel subscriptions.

Finally, sideloading would undermine iPhone's core on-device platform security protections. For security reasons, Apple restricts apps from accessing sensitive hardware elements (e.g., NFC chip, secure enclave, memory space, ultra wideband) and does not permit apps to use non-public operating system functions. Special entitlements – the right or privilege to use a sensitive service or technology – are granted selectively to apps that require access for a specific purpose. For example, the HealthKit entitlement determines whether an app may request user permission to access health and activity data.

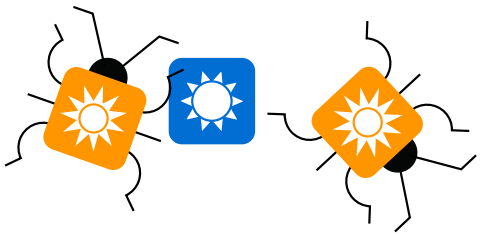
If Apple were forced to provide full access to proprietary hardware elements and non-public operating system functions, as some efforts to force sideloading on iOS would require, it would undermine core platform security features, such as the sandboxing of apps and the separation between apps and the operating system. The attack surface on iPhone would significantly expand, and fundamental security protections would be endangered. For example, under some proposals, the operating system would no longer be able to prevent apps from stealing or modifying data from another app, or accessing location data, the microphone, or the camera without user permission.

Sideloading would make it easier and cheaper to execute many attacks that are currently difficult and costly to execute on iOS.[15] This would expand the universe of attack techniques present on iOS, the set of users that are targeted, and the number of cybercriminals. Supporting sideloading would lower the cost of carrying out attacks on iPhone, incentivizing malicious actors to develop tools and expertise to attack iPhone device security and privacy at an unprecedented scale.

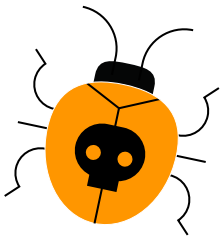
Cybercriminals and hackers would take advantage of the adtech industrial complex to reach their targets. They would use mobile ad networks to spread harmful apps to users by targeting them with ads to install sideloaded apps. Mobile ad networks earn billions of dollars a year from ads for mobile app installs, a practice that would likely expand to include ads for malicious apps distributed through sideloading.[130,131] Cybercriminals already use ads on social media platforms to target users with malware for PC and many other types of scams.[132,133,134] Users would face an onslaught of ads for malicious apps that these ad networks profit from and therefore have little incentive to police.[135] Cybercriminals and hackers may also rely on social media networks to spread malicious apps through social engineering, exploiting people's trust in their friends and family. As a result, users would bear the burden of determining what is safe to click on and download.

Even users who decide they don't want to sideload, and prefer to download apps only from the App Store, would end up being harmed. They could be forced to sideload an app they need for work, for school, or for social inclusion if it is not made available on the App Store. Furthermore, cybercriminals and hackers may trick users into unknowingly sideloading an app by mimicking the appearance of the App Store, or by touting free or expanded access to services or exclusive features.

If Apple were forced to support sideloading via direct downloads and through third-party app stores, iPhone users would have to constantly be on the lookout for scams, never sure whom or what to trust, and, as a result, users would download fewer apps from fewer developers. Developers themselves would become more vulnerable to threats from malicious actors who offer developer tools that contain and propagate malware. Developers would also be more vulnerable to piracy and intellectual property theft, which would undermine their ability to get paid for their efforts and innovation.



Sideloading and iOS users

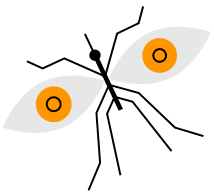


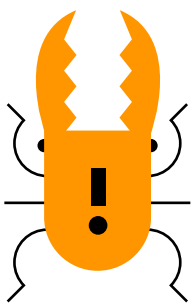
Supporting sideloading on iOS devices would harm iOS users, whose security, privacy, and personal data would be put at risk by the increased threat of attacks by malicious actors. iOS users store personal, valuable, or sensitive information on their mobile devices.[136] Many iOS users use mobile banking and payment apps, and purchase goods and services on their devices.[137] Employees also commonly connect to corporate networks on their mobile devices for work-related tasks. App Store users come from all walks of life and all age groups, speak different languages, and live all over the world. But one thing they have in common is that they are all protected by the App Store safeguards.

Smartphone users have access to millions of apps, and download a large and increasing number of apps. In many countries, users have over 90 apps installed on their devices on average, and iOS users download almost 50 percent more apps than they did five years ago.[138,139,140] Each sideloaded app could potentially pose a threat to the security and privacy of users' devices and their personal data.

As a result, Apple's security and privacy features are critical to protecting the hundreds of millions of iOS users. In fact, research shows that a majority of iOS users report that they have only some or no knowledge of cybersecurity issues, and do not change default security settings unless they run into specific issues.[136] Even among the small share of users with security expertise, when asked what they prioritize when making security choices, roughly as many chose convenience as chose security.[136]

By reviewing every app before it becomes available on the App Store to ensure it is free of malware and accurately represented to users, and by swiftly removing apps from distribution if they are found to be harmful and limiting the spread of future variants, Apple protects the security of the ecosystem and provides peace of mind to customers. **Sideloading is not in the best interest of users.**





Guidance from security experts

Government and international agencies worldwide, as well as security experts and cybersecurity providers, widely caution users about the risks posed by downloading apps from third-party app stores:

"Only install apps from official app stores."

"Companies should only permit the installation of apps from official sources on those mobile devices that connect to the enterprise network."

Europol[147]

"Users should only download applications from Google Play and not from third-party sources, to minimise the risk of installing a malicious application."

European Agency for Cybersecurity[141]

"Users should avoid (and enterprises should prohibit on their devices) sideloading of apps and the use of unauthorized app stores."

Department of Homeland Security (United States)[143]

"[Sideloading] if done incorrectly could make a mobile device extremely vulnerable to attack."

National Institute of Standards and Technology (United States Department of Commerce)[144]

"One way to minimize danger from third-party app stores is to avoid them."

Norton (cybersecurity provider)[148]

"Third party apps pose a security threat to users who enable the installation of apps from unverified sources."

Interpol and Kaspersky Lab[142]

"The majority of [third-party] app stores don't enforce rigorous security vetting of the apps they offer, [and] this can make any device on which they have been installed particularly vulnerable to threats."

"[Sideloading] should be forbidden in [a company's] BYOD policy."

Wandera (mobile security company)[145,146]

Sources

1. Neville, Ann, "Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade," *European Parliamentary Research Service*, June 2021.

2. Chebyshev, Victor, "Mobile Malware Evolution 2020," *Kaspersky*, March 1, 2021.

3. Yablokov, Victor, "Why there's no antivirus for iOS," *Kaspersky*, September 10, 2018.

4. Nokia, "Threat Intelligence Report 2020," 2020.

5. Nokia, "Threat Intelligence Report 2019," 2019.

6. RSA, "2018 Current State of Cybercrime," *Dell Technologies*, March 20, 2018.

7. Hautala, Laura, "Android malware tries to trick you. Here's how to spot it," *CNET*, May 14, 2021.

8. Mitre ATT&CK, "Techniques: Deliver Malicious App via Other Means," February 9, 2021.

9. Mitre ATT&CK, "Tactics: Initial Access," January 27, 2020.

10. Verizon, "2020 Data Breach Investigations Report," May 19, 2020.

11. Anderson, Sophie, "Antivirus and Cybersecurity Statistics, Trends & Facts 2021," *Safety Detectives*, January 24, 2020.

12. Verger, Rob, "Your anti-virus software is not enough," *Popular Science*, July 7, 2017.

13. Huang, Keman, et al., "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Computing Surveys*, Vol. 51, No. 4, July 2018, pp. 1-36.

14. Algarni, Abdullah and Malaiya, Yashwant, "Software Vulnerability Markets: Discoverers and Buyers," *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, Vol. 8, No. 3, 2014, pp. 480-490.

15. RiskIQ, "2020 Mobile App Threat Landscape Report," 2020.

16. Burkhalter, Max, "Why BYOD culture poses a major risk to enterprises," *Perle*, April 6, 2020.

17. Bitglass, "Mission Impossible: Securing BYOD," November 2018.

18. PurpleSec, "2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends," 2021.

19. Ponemon Institute, "The Economic Risk of Confidential Data on Mobile Devices in the Workplace," February 2016.

20. Holland, Jake, "T-Mobile Hit With Class Action Suits After Consumer Data Breach," *Bloomberg Law*, August 20, 2021.

21. Check Point, "Mobile Security Report 2021," April 2021.

22. IBM, "Cost of a Data Breach Report 2021," July 2021.

23. Sophos, "The State of Ransomware 2020," May 2020.

24. Brown, Mike, "Android's Piracy Problem Is Forcing Developers To Give Away Games: 'Alto's Adventure' Latest Freebie," *International Business Times*, February 11, 2016.

25. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy," *Forbes*, February 2, 2018.

26. Vincent, James, "TikTok clone Zynn has now been removed from the iOS App Store as well," *The Verge*, June 16, 2020.

27. LeFebvre, Rob, "Apple pulls cloned games from App Store," *VentureBeat*, February 7, 2012.

28. Dong, Feng, et al., "FrauDroid: An Accurate and Scalable Approach to Automated Mobile Ad Fraud Detection," September 6, 2017.

29. La Porta, Liarna, "Trojan malware infecting 17 apps on the App Store," *Wandera*, October 24, 2019.

30. Trend Micro, "Mobile Ad Fraud Schemes: How They Work, and How to Defend Against Them," April 26, 2019.

31. Takahashi, Dean, "Adjust says mobile ad fraud rates doubled in the past year," *VentureBeat*, May 10, 2018.

32. Health Information National Trends Survey, "On your tablet or smartphone, do you have any software applications or apps related to health?," *National Cancer Institute*, 2020.

33. Firch, Jason, "10 Cyber Security Trends You Can't Ignore In 2021," *PurpleSec*, April 29, 2021.

34. He, Terry, et al., "2021 Cyber Threat Report," *SonicWall*, 2021.

35. Cohen, Jessica Kim, "Hackers taking advantage of COVID-19 to spread malware," *Modern Healthcare*, March 16, 2020.

36. Wang, Liu, et al., "Beyond the Virus: A First Look at Coronavirus-themed Android Malware," *Empirical Software Engineering*, Vol. 26, No. 82, June 12, 2021.

37. Chen, ZePeng, "Thousands of HiddenAds Trojan Apps Masquerade as Google Play Apps," *McAfee*, March 3, 2020.

38. Avast, "Avast Reports Continued Dominance of Adware Among Android Threats," June 16, 2021.

39. Kaspersky, "What is Adware? – Definition and Explanation."

40. Malwarebytes, "Android/Trojan. FakeAdsBlock."

41. Dr. Web Anti-Virus, "Clicker Trojan Installed from Google Play by Some 102,000,000 Android Users," August 8, 2019.

42. Osborne, Charlie, "CopyCat Android malware infected 14 million devices, rooted 8 million last year," *ZDNet*, July 7, 2017.

43. Check Point, "How the CopyCat malware infected Android devices around the world," July 6, 2017.

44. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it," *Avira*, August 13, 2020.

45. Grustniy, Leonid, "Mobile beasts and where to find them – part two," *Kaspersky*, August 3, 2018.

46. Holland, Tilly, "Ransomware Attacks: What You Need To Know," *Ontrack*, March 7, 2019.

47. PurpleSec, "2021 Ransomware Statistics, Data, & Trends," 2021.

48. Nicholas, Sarah, "You Can Beat the Latest Security Breaches," *Ameris Bank*, July 19, 2021.

49. Cyber Florida, "Research Shows a 715% Increase in Ransomware Attacks in 2020," *University of South Florida*, September 23, 2020.

50. Ostroff, Caitlin and Vigna, Paul, "Why Hackers Use Bitcoin and Why It Is So Difficult to Trace," *Wall Street Journal*, July 16, 2020.

51. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," *WeLiveSecurity by ESET*, June 24, 2020.

52. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices," *Threatpost*, June 24, 2020.

53. Emm, David, et al., "IT Threat Evolution in Q2 2016," *Kaspersky*, 2016.

54. Kaspersky, "KSN Report: Ransomware in 2016-2017," *Kaspersky*, 2017.

55. Venkatesan, Dinesh, "Sophisticated new Android malware marks the latest evolution of mobile ransomware," *Microsoft*, October 8, 2020.

56. Whitwam, Ryan, "Microsoft Spots Android Ransomware That Hijacks Your Home Button," *ExtremeTech*, October 9, 2020.

57. Osborne, Charlie, "How to find and remove spyware from your phone," *ZDNet*, August 9, 2021.

58. Kaspersky, "Avoiding Cell Phone Spyware Infestation."

59. Shatilin, Ilja, "Mobile beasts and where to find them – part four," *Kaspersky*, October 22, 2018.

60. Palmer, Danny, "AndroRAT: New Android malware strain can hijack older phones," *ZDNet*, February 14, 2018.

61. Federal Trade Commission, "FTC Brings First Case Against Developers of "Stalking" Apps," October 22, 2019.

62. Federal Trade Commission, "FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data," September 1, 2021.

63. Vaas, Lisa, "SpyFone & CEO Banned From Stalkerware Biz," *Threatpost*, September 2, 2021.

64. Citron, Danielle Keats, "Spying Inc.," *Washington and Lee Law Review*, Vol. 72, No. 3, June 1, 2015, pp. 1234-1282.

65. Securelist, "The State of Stalkerware in 2020," *Kaspersky*, February 26, 2021.

66. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," *Cybereason*, July 1, 2020.

67. Almkias, Ofir, "FakeSpy," *Mitre ATT&CK*, October 6, 2020.

68. National Cyber Security Centre, "Fake 'missed parcel' messages: advice on avoiding banking malware," August 19, 2021.

69. Finnish Transport and Communications Agency, "Android malware spread by SMS," July 15, 2021.

70. Desai, Shivang, "SpyNote RAT posing as Netflix app," *Zscaler*, January 23, 2017.

71. Black, Daniel, "HelloSpy App Review 2021: Will the App Resume Its Work?," *mSpy*, March 5, 2021.

72. Cox, Joseph, "I Tracked Myself With $170 Smartphone Spyware that Anyone Can Buy," *Vice*, February 22, 2017.

73. Kochetkova, Kate, "Mobile banking Trojans, explained," *Kaspersky*, October 14, 2016.

74. Stefanko, Lukas, "Android Banking Malware: Sophisticated Trojans vs. Fake Banking Apps," *ESET*, January 2019.

75. Owaida, Amer, "Beware Android trojan posing as Clubhouse app," *WeLiveSecurity by ESET*, March 18, 2021.

76. ThreatFabric, "BlackRock – the Trojan that wanted to get them all," *ThreatFabric*, July 2020.

77. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," *Threatpost*, April 21, 2020.

78. Asoltanei, Oana, et al., "Threat Actors Use Mockups of Popular Apps to Spread Teabot and Flubot Malware on Android," *Bitdefender Labs*, June 1, 2021.

79. Cleafy, "TeaBot: a new Android malware emerged in Italy, targets banks in Europe," May 31, 2021.

80. Cyware, "Exploring the Nature and Capabilities of Anubis Android Banking Trojan," January 25, 2020.

81. Clark, Mitchell, "NSO's Pegasus spyware: here's what we know," *The Verge*, July 23, 2021.

82. Whittaker, Zack, "A new NSO zero-click attack evades Apple's iPhone security protections, says Citizen Lab," *TechCrunch*, August 24, 2021.

83. NPR, "Malware From An Infamous Hacker-For-Hire Group Was Found On Nearly 900 Phones," July 19, 2021.

84. Infrascale, "Enterprise Ransomware Survival Guide," May 25, 2016.

85. Yaswant, Aazim, "FlyTrap Android Malware Compromises Thousands of Facebook Accounts," *Zimperium*, August 9, 2021.

86. Hazum, Aviran, et al., "New Wormable Android Malware Spreads by Creating Auto-Replies to Messages in WhatsApp," *Check Point Research*, April 7, 2021.

87. Jama, Robleh, "The upside of copycat apps and how to deal with them if they get out of hand," *TheNextWeb*, April 9, 2016.

88. Hinchliffe, Alex and Palo Alto Networks, "Techniques: Masquerade as Legitimate Application," *Mitre ATT&CK*, April 8, 2020.

89. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove," *The Washington Post*, November 6, 2015.

90. Trend Micro, "Malware in Apps' Clothing: A Look at Repackaged Apps," May 15, 2014.

91. Toulas, Bill, "Researchers Found 164 'Copycat' Apps That Tricked 10 Million Users," *TechNadu*, January 14, 2021.

92. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'," *Zimperium*, March 26, 2021.

93. European Union Agency for Cybersecurity, "Phishing on the rise," October 12, 2017.

94. Eremin, Alexander, "People infected with coronavirus are all around you, says Ginp Trojan," *Kaspersky*, March 24, 2020.

95. Pak, ChanUng, "Phishing Android Malware Targets Taxpayers in India," *McAfee*, September 3, 2021.

96. Malwarebytes, "What is a spoofing attack?"

97. Fitriah, Andi, et al., "Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges," *Journal of Cyber Security and Mobility*, Vol. 7, No. 3, June 14, 2018, pp. 1-52.

98. Kaspersky, "What is Scareware?," *Kaspersky*.

99. Sims, Gary, "Exposé: Don't fall victim to this dodgy anti-virus app," *Android Authority*, February 5, 2014.

100. Malwarebytes, "Mobile PUP," June 9, 2016.

101. Satori Threat Intelligence and Research Team, "Bringing Starchild Down to Earth: Soraka SDK," *Human Security*, December 2019.

102. Korolov, Maria, "Supply chain attacks show why you should be wary of third-party providers," *CSO from International Data Group*, February 4, 2021.

103. Android, "Android Security & Privacy 2018 Year In Review," March 2019.

104. Clayton, Richard, "Mobile Supply Chain Attacks Are More Than Just an Annoyance," *Check Point*, 2019.

105. He, Feixiang and Polkovnichenko, Andrey, "Operation Sheep: Pilfer-Analytics SDK in Action," *Check Point*, March 13, 2019.

106. Trend Micro, "Variant."

107. Sen, Sevil, et al., "Coevolution of Mobile Malware and Anti-Malware," *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 10, October 2018, pp. 2563-2574.

108. Australian Competition & Consumer Commission, "Digital Platform Services Inquiry: Interim Report – App Marketplaces," March 2021.

109. Apple Developer, "App Store Review Guidelines."

110. Google Play Help, "Google Play Protect keeps your apps safe and your data private."

111. O'Donnell, Lindsey, "Google Play Cracks Down on Malicious Apps," *Threatpost*, February 14, 2019.

112. Mohan, Babu, "Google now takes three days to approve new Play Store apps," *Android Central*, August 20, 2019.

113. Apple, "App Store stopped more than $1.5 billion in potentially fraudulent transactions in 2020," May 11, 2021.

114. Guertin, Alec and Kotov, Vadim, "PHA Family Highlights: Bread (and Friends)," *Google Security Blog*, January 9, 2020.

115. Shen, Yun, et al., "A Large-scale Temporal Measurement of Android Malicious Apps: Persistence, Migration, and Lessons Learned," *Cornell University: Computer Science – Cryptography and Security*, August 10, 2021.

116. Lindorfer, Martina, et al., "AndRadar: Fast Discovery of Android Applications in Alternative Markets," *11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*, July 2014.

117. Smith, Chris, "Another crucial reason why app developers prefer iOS to Android," *BGR*, February 4, 2016.

118. Kujawa, Adam, et al., "2020 State of Malware Report," *Malwarebytes*, February 2020.

119. N-Marandi, Sara, "What's new in Android privacy," *Android Developers Blog*, May 18, 2021.

120. Johnson, Kyle, "How do you block sideloaded app installation on iOS or Android?," *TechTarget*, January 9, 2019.

121. Tee, Mike, "How to Install Apps from Unknown Sources in Android," *MakeTechEasier*, February 16, 2020.

122. Nickle, Robert, et al., "Lookout Discovers New Spyware Used by Sextortionists to Blackmail iOS and Android Users," *Lookout*, December 16, 2020.

123. Nellis, Stephen and Dave, Paresh, "Software pirates use Apple tech to put hacked apps on iPhones," *Reuters*, February 13, 2019.

124. Owen, Malcolm, "Apple has revoked Facebook's enterprise developer certificates after sideload violations," *AppleInsider*, January 30, 2019.

125. Axon, Samuel, "Apple revokes Facebook's developer certificate over data-snooping app—Google could be next," *Ars Technica*, January 30, 2019.

126. Xiao, Claud, "Novel Malware XcodeGhost Modifies Xcode, Infects Apple iOS Apps and Hits App Store," *Palo Alto Networks*, September 17, 2015.

127. Xiao, Claud, "More Details on the XcodeGhost Malware and Affected iOS Apps," *Palo Alto Networks*, September 21, 2015.

128. Fischer, Sara, "Facebook says Apple's ad changes are hurting its business," *Axios*, September 22, 2021.

129. Seetharaman, Deepa, "Facebook Removes Data-Security App From Apple Store," *Wall Street Journal*, August 22, 2018.

130. Rosenfelder, Shani, "Global app install ad spend to double by 2022 to hit $118 billion," *AppsFlyer*, February 13, 2020.

131. Brown, Eileen, "Facebook leads app install market share, but Google is rising fast," *ZDNet*, October 19, 2018.

132. Whittaker, Zack, "Facebook ran ads for a fake 'Clubhouse for PC' app planted with malware," *TechCrunch*, April 8, 2021.

133. Newman, Lily Hay, "Facebook Shut Down Malware That Hijacked Accounts to Run Ads," *Wired*, October 1, 2020.

134. McGuire, Michael, "The Web of Profit: Social Media Platforms and the Cybercrime Economy," *Bromium*, 2019.

135. Rastogi, Vaibhav, et al., "Understanding In-App Ads and Detecting Hidden Attacks through the Mobile App-Web Interface," *IEEE Transactions on Mobile Computing*, Vol. 17, No. 11, November 1, 2018, pp. 2675-2688.

136. Breitinger, Frank, et al., "A survey on smartphone users' security choices, awareness and education," *Elsevier: Computers & Security*, Vol. 88, October 11, 2019.

137. Centre for International Governance Innovation – Ipsos, "Global Survey on Internet Security & Trust," 2017.

138. App Annie, "The State of Mobile," 2019.

139. Nelson, Randy, "Store Intelligence: Q1 2016 Data Digest," *Sensor Tower*, April 18, 2016.

140. Sensor Tower, "Q4 2020 Store Intelligence Data Digest," 2020.

141. European Union Agency For Cybersecurity, "Vulnerabilities – Separating Reality from Hype," August 24, 2016.

142. Kaspersky and Interpol, "Mobile Cyber Threats," October 2014.

143. U.S. Department of Homeland Security, "Study on Mobile Device Security," April 2017.

144. Franklin, Joshua M, et al., "Guidelines for Managing the Security of Mobile Devices in the Enterprise," *U.S. Department of Commerce – National Institute of Standards and Technology*, March 2020.

145. Urwin, Matt, "Top 5 Types of Sideloaded Apps and the Risks They Pose," *Wandera*, December 19, 2018.

146. Velzian, Becci, "How to Create a Bring Your Own Device (BYOD) Policy," *Wandera*, January 13, 2021.

147. Europol, "Just a Game? Only install apps from official app stores," *European Cybercrime Centre*.

148. Gervais, Joe, "The risks of third-party app stores," *Norton*, July 18, 2018.