

Threat report on application stores

The risks associated with the use of official and third party app stores.



Contents

4	Introduction
	Related NCSC guidance
6	Use of apps and app stores in the UK
	UK app developers
	What is the risk?
8	Cyber attacks on compromised apps
	Systemic vulnerabilities of app store developer submission checks
10	Overview of app stores
	Mobile app stores
	Third party app stores
	IoT voice assistant stores
	IoT smart device stores
	Gaming stores
13	Case studies
	Official mobile app stores
	Third party mobile app stores
	Voice assistant stores
	IoT smart device stores
	Gaming stores
21	Summary

Introduction

Over the last decade there has been an enormous increase in the availability and use of smartphones and smart devices. Many of these devices feature application stores ('app stores'), which allow users to download additional applications and content. The vast majority of users, particularly on mobile platforms, download apps via these app stores.

There's also been increased demand for apps, primarily as a result of the COVID-19 pandemic as more people work, shop, and stay in touch online.

Since there is a great variety of devices (and supporting app stores), there are a number of disparate and complex security issues that can expose consumers and enterprises to online threats.

This report summarises the risks associated with the use of official and third party app stores.

It includes links to detailed guidance that describe how to mitigate the main threats.

This report was compiled to inform Department for Digital, Culture, Media & Sport's (DCMS) review on current threats associated with app stores. The report will aid in the development of policy interventions that will seek to improve app stores' security and privacy controls to protect both UK consumers and enterprises. It will also be of particular interest to the following audiences:

- developers of applications for both mobile and other connectable consumer devices (such as smart TVs and wearables)
- administrators responsible for managing the use of applications within their organisations (for example in BYOD scenarios)
- other governments with an interest in implementing policy to improve their security posture of app stores to protect their consumers and enterprises


This report identifies systemic vulnerabilities that have been used by attackers to exploit app stores. It includes a selection of case studies which describe how users of official and third party app stores have been affected, as well as users of smartwatches, smart TVs, and voice assistants.


Note:
The case studies are illustrative only, and security vulnerabilities are not unique to the organisations named. Their competitors' products may also contain security vulnerabilities that attackers can exploit.


This report is limited to *technical* security threats. It does not address privacy-related concerns, or the misuse of data by legitimate actors, or GDPR issues. These areas are considered in [DCMS's report 'Call for Views on App Store Security and Privacy Interventions'](#)¹.

Related NCSC guidance

The following guidance can help reduce the likelihood of being impacted by the threats outlined in this report. However, if your organisation is affected, you should follow [our Incident Management guidance](#)².

 [Using third-party applications on devices](#)³. Detailed advice on the assessment, distribution and use of third party applications on smartphones, tablets, laptops and desktop PCs. This guidance will help risk owners and administrators create organisational policies for the use of third party applications which minimises risk, without limiting utility.

 [Device Security Guidance](#)⁴. More general guidance for organisations on how to choose, configure and use devices securely. This guidance is primarily aimed at business users, with a focus on those deploying or managing large IT estates.

 Members of the public should refer to the NCSC's Cyber Aware guidance, in particular the section on [updating devices](#)⁵. In many instances, updating the apps and operating system will fix vulnerabilities (including those contained within this report).

¹ <https://www.gov.uk/government/consultations/app-security-and-privacy-interventions>

² <https://www.ncsc.gov.uk/section/about-ncsc/incident-management>

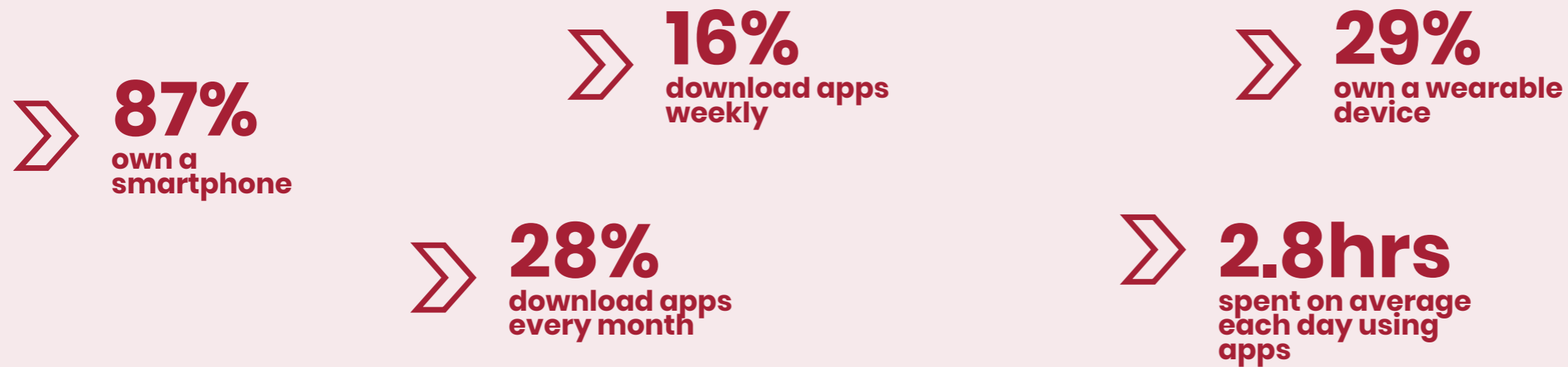
³ <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-third-party-applications-on-devices>

⁴ <https://www.ncsc.gov.uk/collection/device-security-guidance>

⁵ <https://www.ncsc.gov.uk/cyberaware/home#action-5>

Use of apps and app stores in the UK

Key statistics for UK adults:



Source: Consumer Attitudes Towards IoT Security Summary Report, December 2020, Ipsos MORI for DCMS

An application, or app, is a software package that users can install or are pre-installed on a device to provide extra functionality or content to their device.

Most people will be familiar with downloading apps for their smartphones and tablets, but they can also be installed on laptops, computers, games consoles, wearable devices (such as smartwatches or fitness trackers), smart TVs, smart speakers (such as Alexa devices), and IoT (internet of things) devices.

Apple and Google provide their users with access to a dedicated app store (Apple's App Store, Google's Play Store) where they can download free and paid apps. Original equipment manufacturers (OEMs) also provide stores, such as the Huawei AppGallery, the Samsung Galaxy Store, or Amazon's App Store. Users of IoT devices typically are only able to download apps onto their devices via a manufacturer-supported store.

The UK is amongst the leading nations for consumer spends and downloads on Apple's App Store and the Google Play Store. [A survey conducted by Ipsos MORI](#)⁶ on behalf of DCMS reveals that the majority of users download applications using official app stores for their smartphone/tablets. 52% of UK consumers have downloaded apps from Google Play Store. 44% of UK consumers have downloaded apps from Apple's App Store.

Furthermore, the effect of COVID-19 (with remote working and socialising becoming more widespread) has accelerated the number of installations of applications across all devices. Six in ten households have increased their use of IoT devices, with the average household purchasing [two more smart devices since the beginning of the pandemic](#)⁷. Meanwhile, [the gaming population in the UK has increased by 63%](#)⁸ during the course of the pandemic.

UK app developers

While the UK is a major consumer of applications, it also significantly contributes to applications available within app stores with over 10,000 developers publishing more than 40,000 apps. [Popular apps published by UK developers](#)⁹ on the Google Play Store include Tesco Clubcard, Deliveroo, All 4, ITV Hub and Just Eat UK. The UK government is also producing apps, in domains such as public health and travel.

What is the risk?

Given the market for apps in the UK, it's important that UK consumers can trust apps (and the stores that host them). If popular apps available on app stores are compromised, millions of users are potentially vulnerable, whilst vendors could face financial and reputational damage.

As the following sections in this report explain, even official app stores (such as Apple's App Store and Google's Play Store) with vetting processes to detect malicious functionality in apps have been impacted by malware. Furthermore, the current well-known third party app stores (that is, stores which are **not** provided by the manufacturer or the operating system provider) appear to have less robust vetting processes, and so represent a greater risk.

Cyber attacks on compromised apps

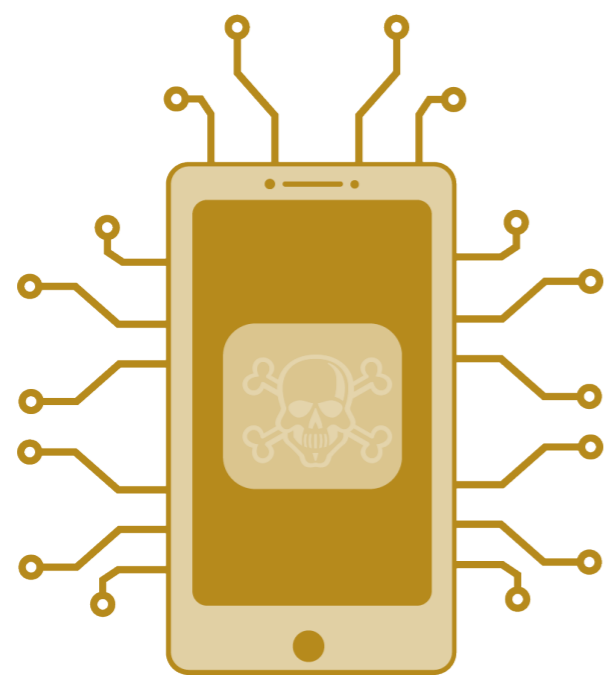
Malicious software (Malware)

Malicious software – also known as malware – is the main security issue faced by users of app stores (other concerns such as privacy and data sharing are out of scope of this report).

Malware is any kind of software that can damage computer systems, networks or devices. If devices are compromised with malware, they may be at risk from numerous threats, such as specific types of malware including spyware and ransomware, or an attacker gaining administrative access or committing toll fraud (when infected devices are charged to access premium services). These threats can result in users and organisations losing sensitive data, being unable to access data or systems, or suffering financial and reputational impact.

While apps uploaded to official app stores generally undergo a series of reviews and in-depth vetting processes before they are available for users to download, malware can still be found within apps on these stores through a range of different systemic vulnerabilities.

Moreover, there is limited evidence of coordination and alignment between app stores on their vetting processes and mitigations against these vulnerabilities. The case studies within this report cover examples of these – with the success of each demonstrating the feasibility at the time of bypassing mitigations that were in place.



Systemic vulnerabilities of app store developer submission checks

A number of systemic vulnerabilities within app store submission processes have been exploited by attackers, allowing them to successfully distribute malware via apps. [The following techniques](#)¹⁰ insert malware into already existing and published applications:

Application republishing

Occurs when an application is copied and redistributed through third party application stores, with malicious code added. If an app is banned in their native country (or has been removed from the official app store), a user may try and download it via a third party store.

Application updating

Occurs when a legitimate application has already been reviewed and published, but the next update contains malware. This may be due to the developer choosing to include malicious code, or an attacker compromises the developer's system and inserts malicious code into the release. With some app stores, this is less likely to be detected as the process of checking a pre-existing app may not be as rigorous as when it is first published.

Malicious SDKs

Many developers use third party SDKs (Software Development Kits) to include additional content within their own applications (such as displaying advertisements or additional functionality). Legitimate third party SDKs are often included within apps on the app store. However, these APIs can be configured or compromised to be malicious and perform malicious within an otherwise benign application.

Application acquisition

This occurs when an app with a large user base is purchased by an attacker, who then publishes an update containing malware. By doing this, an attacker is able to exploit the level of trust that consumers have built with the previous developer/app.

Infected development tools

This occurs when development tools (used for building and compiling the application) are infected, often when the tools are downloaded from an untrusted third party source. When a developer builds the app, they unknowingly insert malicious code.

¹⁰ <https://theconversation.com/explainer-how-malware-gets-inside-your-apps-79485>

Overview of app stores

This section provides a brief introduction to different types of app store. As mentioned previously, users download apps from stores for the platform they're using, which comprise:

- mobile app stores (including [third party stores](#)) for downloading apps to mobile devices
- [IoT voice assistant stores](#) for downloading apps to Amazon's Alexa and Google's Home devices
- [IoT smart device stores](#) for downloading apps to devices that form part of the IoT, such as smartwatches and smart TVs
- [gaming stores](#) for downloading games and additional content to consoles (Xbox, PlayStation, Nintendo) and PCs

Mobile app stores

Mobile app stores provide a centralised and trusted repository for mobile users to purchase apps and download them onto their devices.

Most mobile users download apps via the Google Play Store and Apple's App Store, the official stores for Android and iOS devices respectively, which come preinstalled on devices. Microsoft's mobile devices have their own app store, though only 4% of respondents to the [Ipsos MORI consumer survey](#)¹¹ said that they used the Microsoft Store (which includes users of the Xbox Store). Non-Google manufactured Android devices often come with an app store operated by the original equipment manufacturer (OEM) pre-installed, such as the Samsung Galaxy Store for Samsung Galaxy devices or the Huawei AppGallery.

Apple's App Store and the Google Play Store offer 4.3 million and 2.9 million apps respectively [as of November 2020](#)¹². The vast majority of the apps available on mobile app stores are produced by third party developers. Uploading an app to an official app store requires submitting it for vetting so the operators can check for any malicious behaviours. Although these stores provide certain details about their processes of [vetting and reviewing apps](#)¹³, most of the information is not in the public domain.

Despite these vetting processes, malware continues to make it onto stores, as the [case studies section](#) illustrates. Due to the sheer number of smartphone users, mobile app stores are a particularly attractive attack vector for cyber criminals seeking to infect as many victims as possible to maximise their returns, and even nation-state actors with a narrower, more defined targeting rationale.

In terms of the *type* of threat, mobile app stores do **not** fundamentally differ from other types of app stores. For example, an attacker could upload malware to either a mobile app store or a wearable smart device app store to track a user's location, given that both types of device are portable. The sheer number of smartphone users makes mobile app stores a more attractive target for attackers.



Third party app stores

Unlike iOS, the Android platform allows for third party app stores. These are app stores that users must download or access separately, typically characterised by their focus on user and developer freedom (as opposed to the safety and privacy of users).

The only way to install third party apps on iOS is to 'jailbreak' a device, a process that provides the user and apps with access to features in the phone which would otherwise be inaccessible. The process uses unpatched vulnerabilities to bypass the security controls that Apple put in place, which leaves the device more vulnerable attacks. [Apple strongly cautions users against jailbreaking](#)¹⁴.

While there's less people using the most common third party app stores (compared with official app stores), a lack of robust vetting processes means that their users are especially vulnerable to threat actors uploading malware, as the case studies show. The threats from official or third party stores include spyware, banking malware, and malware used for toll fraud.

IoT voice assistant stores

Voice assistant devices such as the Echo range from Amazon (powered by Alexa) and the Nest devices (from Google) allow their users to download third party apps to further enhance their functionality. In Alexa these are referred to as 'skills', though they are functionally similar to apps. Skills can be downloaded through the main Amazon website. After downloading a skill, Alexa users can be informed of any updates to the skill via the notifications API.

Alexa and Google Home provide apps mainly through one store. While Amazon has opened up to other app providers through its [Voice Interoperability Initiative](#)¹⁵ (which would allow other voice assistants to run on Alexa devices), this does not include its main rivals in this area (namely Google, Apple and Samsung).

As with mobile app stores, the majority of apps available are provided by third party developers. There are currently over 100 million skills available to Alexa users and these cover a wide range of functionality, such as [gaming and ordering takeaways](#)¹⁶.

With over [100 million Alexa-enabled devices sold](#)¹⁷ as of January 2019, voice assistants represent an attractive target for attackers, who could use them to steal personal data and listen in on victims' conversations. This mirrors how malware is distributed within mobile app stores, with applications that conceal similar malicious capabilities (such as recording audio via a device's microphone). This highlights how both types of app stores are alike in terms of their threat profiles.

Voice assistant stores also face issues in terms of lacking robust vetting processes. [A research paper](#)¹⁸ published in February 2021 revealed that it was possible to upload skills to the Alexa skills store under the names of well-established companies, similar to how malicious apps on mobile app stores often attempt to spoof their true origins.

Furthermore, developers are able to update the code of their skills, once they are approved and published by Amazon, highlighting the systemic vulnerability of [application updating](#) that is shared across app stores. Amazon is responsible for setting the requirements for its app store and has [published documentation](#)¹⁹ for the security requirements developers must adhere to, but the evidence highlights that some issues remain.

¹¹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf
¹² <https://www.businessofapps.com/data/app-stores/>
¹³ <https://developer.apple.com/app-store/review/guidelines/>

¹⁴ <https://support.apple.com/en-gb/ht201954>
¹⁵ <https://developer.amazon.com/en-US/alexa/voice-interoperability>
¹⁶ <https://www.tomsguide.com/uk/round-up/best-alexa-skills>
¹⁷ <https://www.cnet.com/home/smart-home/amazon-has-sold-more-than-100-million-alexa-devices/>
¹⁸ https://www.theregister.com/2021/02/25/alexa_amazon_skills/
¹⁹ <https://developer.amazon.com/en-US/docs/alexa/ask-overviews/what-is-the-alexa-skills-kit.html>

IoT smart device stores

This section discusses stores for ‘smart devices that form part of the IoT’, such as smartwatches and smart TVs. The voice assistants that are part of the three major smart home ecosystems (Siri/ Homekit, Google Home and Alexa), are covered in the previous section.

The way that users interact with IoT smart device stores depend on the OEM and device. Smart TVs, for example, require that the [user download apps via the TV](#)²⁰. Meanwhile, smartwatches often make apps available through a dedicated mobile app. As with the other types of app stores, most apps are produced by third parties, all of whom must adhere to the IoT device developer’s app requirements. After installing an app, users are often informed of updates [via push notifications initiated by the developer](#)²¹.

There is little precedent for attackers exploiting these app stores given the relative lack of incentives. Someone looking to steal bank account data, for example, would have little reason to target a smart TV as opposed to a mobile device running a banking app. Despite the lack of incentives in most areas, an attacker could still find reason to target users via smart device app stores, for example to gather location data, or to hijack a smart TV’s processing power for use in an IoT-powered botnet.

Like other types, IoT smart device app stores require that developers undergo a vetting process for their apps, which is vital when most apps available on the platforms are third party. [The Fitbit App Gallery Guidelines](#)²² last updated in 2020, state that apps are to be approved by Fitbit before they are made available. However, Fitbit also allows developers to [upload apps to the store without checks](#), so long as the app is only accessible via a private link. This could allow for the targeting of individuals through malicious apps, similar to how mobile app stores can be used for more tailored campaigns alongside more opportunistic efforts (for details of Fitbit’s response please refer to the [case study section](#)).

Gaming stores

Gaming consoles have their own dedicated app stores, namely the PlayStation Store, the Xbox Store and the Nintendo eShop. These differ from other categories of app stores in that they focus almost exclusively on games. While companies like Nintendo make and publish their own games, most of the content on their stores, and others, are provided by third party developers. PC gamers have a choice of stores; Steam is the most popular store by a large margin, but there are alternatives, such as the Epic Game Store and EA’s Origin.

Gaming stores are accessed via their respective consoles. While some games are available for low prices if produced by independent developers, the economic model of game production means that many are sold at much higher prices than apps available on other types of store. Updates to games are typically downloaded automatically, though users can also choose to [download patches manually](#)²³. On Steam, notifying users that a game has been updated is largely the [responsibility of the developer](#)²⁴.

The more restricted purpose of consoles means they are (currently) less attractive to attackers, but they still represent a valuable target. Attackers can steal accounts and in-game tokens that have real monetary value. There have been [multiple reports](#)²⁵ of [accounts being compromised](#)²⁶ to gain access to paid content, which led to the NCSC publishing [our guidance covering online gaming for families and individuals](#)²⁷.

Gaming stores on PCs also represent valuable targets for attackers. In June 2021, security researchers discovered a campaign [hiding malware in Steam profile images](#)²⁸. While the campaign was not directly using apps, it nevertheless shows the cyber criminal intent to exploit the platform.

Information around the vetting processes used for these stores is limited. In 2018, Steam announced that it would allow any content on its store so long as it was [not illegal or highly controversial](#)²⁹. It is unclear what constitutes illegal content and what this means in terms of security or privacy matters. As for the stores on game consoles, there is little to no information on vetting in the public domain.

Case studies

In the following case studies, malware was able to breach a store, or a vulnerability was discovered within the store. They are grouped according to the categories previously discussed in this report, with the mobile app store section further divided into official and third party stores.

Note that:

- All information used in these case studies is available is the public domain, and was researched through open source methods.
- The case studies are illustrative only. The security vulnerabilities included here are **not** unique to any of the organisations featured below; their competitors’ products may also contain security vulnerabilities that attackers can exploit.



²⁰ <https://www.samsung.com/uk/support/tv-audio-video/how-do-i-manage-apps-on-my-smart-tv/>
²¹ <https://developer.samsung.com/smarttv/develop/api-references/tizen-web-device-api-references/push-api.html>
²² <https://dev.fitbit.com/legal/app-gallery-guidelines/>
²³ <https://www.businessinsider.com/how-to-update-games-on-ps4?r=US&IR=T>
²⁴ <https://partner.steamgames.com/doc/store/updates>
²⁵ <https://conversation.which.co.uk/scams/gaming-account-hacked-fraud/>
²⁶ <https://www.techradar.com/uk/news/thousands-of-online-gaming-accounts-hit-in-major-cyberattack>
²⁷ <https://www.ncsc.gov.uk/guidance/online-gaming-for-families-and-individuals>
²⁸ <https://threatpost.com/steam-gaming-delivering-malware/167784/>
²⁹ <https://steamcommunity.com/games/59310/announcements/detail/1686776116200553082>

Official mobile app stores

XcodeGhost on the Apple App Store

XcodeGhost was a breach within Apple's App Store due to a tainted Software Development Kit (SDK) in 2015. [XcodeGhost](#)³⁰ was mainly prevalent in Chinese applications. Due to China, at the time, having occasionally slow network speeds when downloading large files, many developers obtained a third party distributed version of Xcode, which is Apple's development tool for iOS apps. When developers built their applications, they unknowingly inserted malicious code into their apps, which were then uploaded to the App Store.

A wide [range of applications were compromised](#)³¹ including instant messaging (IM) apps, banking apps, mobile carriers' apps, maps, stock trading apps, social networking service apps, and games. The malware enabled a large volume of personal data to be obtained, with the use of a Command and Control (C&C) server.

Apple responded to this attack by removing all applications that had been infected by XcodeGhost, [asking all developers to recompile their apps](#)³² with a clean version of Xcode before resubmitting their applications.

Furthermore, Apple advised that all developers have [Gatekeeper](#)³³ (technology designed to ensure that only trusted software can run) activated on their Mac when developing applications to ensure code signing and verifying downloaded applications were enabled.



Joker malware on the Google Play Store and third party app stores

[The Joker malware](#)³⁴ has been prevalent from 2017, to as recently as Summer 2020. The apps containing the malware were relatively unknown, often utility applications such as PDF scanners and photo editors. Despite this, some of the infected apps (such as 'Convenient Scanner 2') have been downloaded over 100,000 times.

The malware conducts fraudulent transactions that are charged to the bill payer, using SMS messages to a premium rate number and making purchases using WAP billing (resulting in financial gain for the Joker malware operators). Wireless Application Protocol (WAP) billing is a method to allow users to purchase content from WAP sites that are charged directly to their phone bill. The payload of the malware was delivered through a direct URL, received through a C&C server whose address was hidden within the code.

Google have [removed over 1700 applications on the Google Play store since 2017](#)³⁵. However, some malicious applications are still evading Google's mainly automated vetting process.

Torrenty Adware on the Microsoft Store

[Adware was found on the Microsoft Store in 2015, through an application called 'Torrenty'](#)³⁶, a peer-to-peer file exchanging tool. Within the application, a misleading '1 Update(s) Pending' message was displayed, which resulted in some unsuspecting users clicking and inadvertently downloading and running a 'Setup.exe' file. The program downloaded was a 'cross-platform (macOS and Windows) browser add-in', PremierOpinion, which reportedly delivers pop-up surveys and places unwanted ads in the browsers that were present on the device.

While this software may not be the most damaging malware, an existing vulnerability meant it had been inadvertently approved by a reputable software store. In theory, more damaging malware (such as ransomware) could have been unknowingly downloaded and run on the user device.

The application in question was reported to Microsoft, who removed it instantly. The adware was added as Microsoft allowed Hosted Web Apps (HWAs) to be modified without having to get re-approval. Therefore, a developer with a pre-approved HWA in the Microsoft Store could add malicious code into their application. Likewise, the server hosting the app may become compromised and a completely legitimate application may have malware injected into it.

Since 2015, Microsoft have included within their [Advertising Conduct and Content policies](#)³⁷ that 'all advertising must be truthful, non-misleading and comply with all applicable laws, regulations, and regulatory guidelines', which would deem such adware as not acceptable within a Microsoft Store app. Apple aim to prevent such threats within their [review process](#)³⁸, by stating in their policy that ads within applications 'must not manipulate or trick users into tapping into them', therefore preventing the application being hosted on the App Store. Likewise, the [Google Play Store states](#)³⁹ that it does not 'allow apps that attempt to deceive users or enable dishonest behavior', therefore this should not pass their review with the adware present in the application.

³⁰ <https://unit42.paloaltonetworks.com/novel-malware-xcodeghost-modifies-xcode-infests-apple-ios-apps-and-hits-app-store/>
³¹ <https://unit42.paloaltonetworks.com/malware-xcodeghost-infests-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/>
³² <https://developer.apple.com/news/?id=09222015a>
³³ <https://support.apple.com/en-gb/HT202491>

³⁴ <https://www.zdnet.com/article/android-security-six-more-apps-containing-joker-malware-removed-from-the-google-play-store/>
³⁵ <https://www.zdnet.com/article/android-security-six-more-apps-containing-joker-malware-removed-from-the-google-play-store/>
³⁶ <https://www.zdnet.com/article/how-was-this-windows-store-app-able-to-download-adware-to-a-windows-10-pc/>
³⁷ <https://docs.microsoft.com/en-us/windows/uwp/publish/store-policies#1010-advertising-conduct-and-content>
³⁸ <https://developer.apple.com/app-store/review/guidelines/>
³⁹ <https://support.google.com/googleplay/android-developer/answer/9888077>

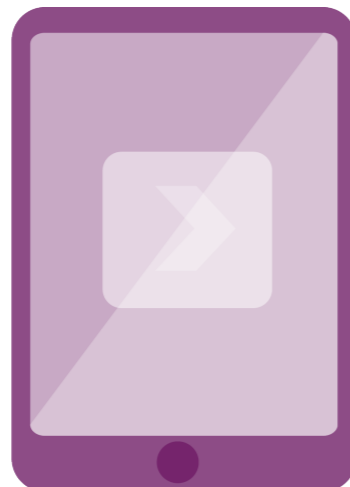
Third party mobile app stores

PhantomLance trojan malware on numerous Android App Stores

Believed to have been present since around the end of 2015, [PhantomLance is a trojan malware](#)⁴⁰ found within numerous Android applications. Its purpose is to steal credentials, finances, sensitive information and display ads.

PhantomLance has been identified within numerous apps, hosted on several third party and official app stores (in one case buried in an application called OpenGL Plugin, which had a [backdoor built in to exfiltrate users' data](#)⁴¹). As commonly seen, the initial version of the infected app was not believed to have the malicious backdoor built in, but added within a later version of the app.

The range of application stores this malware was discovered within reinforces the evidence that all app stores, regardless of their type or device, share the same threat profile.



Triada trojan malware within the APKPure Store

[Kaspersky Labs first reported in April 2021](#)⁴² that Triada malware had been identified within the APKPure Store, a popular alternative third party app store for Android devices.

Triada is a form of Trojan malware, which is obscured within applications within a malicious application software development kit (SDK). On this occasion, it was found within the actual APKPure Store client application, due to a malicious advertisement SDK. APKPure was quick to respond once it had been highlighted, and updated their app from 3.17.18 to a safe version (3.17.19) with the malicious advert SDK removed.

Further to this, in August 2021, [the Triada Trojan](#)⁴³ was found in a modified version of WhatsApp called 'FMWhatsapp 16.80.0' which has been reported to be available within numerous third party app stores.

This application allows users to add custom functionality to Facebook's WhatsApp messenger app, which was [modified and repackaged by a developer known as 'Foud Apps'](#)⁴⁴. In this instance, the malware was contained within adverts, which were added to the modified app using an advertisement SDK.

Rooting malware found on third party app stores

In 2016, security researchers at [Trend Micro published a report](#)⁴⁵ on malware discovered on third party mobile app stores. The malware, tracked as ANDROIDOS_LIBSKIN.A, was found on the Aptoide, Mobogenie, mobile9 and 9apps stores, disguised as popular mobile games, security apps, music streaming apps and more.

Once downloaded, the malware would root the device, which is a process that enables a user or app to access features of a device that the manufacturer usually makes inaccessible to users. The malware then used this access to harvest user data and bombard its victims with pop-up notifications with download links to unwanted apps.

According to [Trend Micro](#)⁴⁶ "Aptoide has informed us that the malicious apps hosted on their store have been removed; they are also updating their own systems to block this threat in the future."

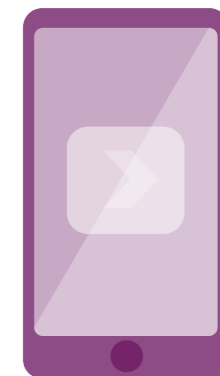
KeyRaider malware spread via Cydia app store

In 2015, WeipTech, in collaboration with Palo Alto Networks, [researched an app they dubbed 'KeyRaider'](#)⁴⁷ that was spreading via Cydia, a third party app store for iOS which requires the user to have jailbroken (the iOS equivalent of rooting) their device.

Cydia functions as an aggregation of apps hosted on third party repositories. KeyRaider was spreading via these repositories to infect users and steal their Apple account credentials via intercepting iTunes traffic on their devices.

These credentials were then used for additional jailbreaking activity, allowing malicious actors to download apps and make in-app purchases without actually paying. In total, KeyRaider was able to steal over 225,000 Apple accounts.

[As described in their report](#)⁴⁸, Palo Alto Networks and WeipTech provided services to detect the KeyRaider malware and identify stolen credentials.



⁴⁰ <https://securelist.com/apt-phantomlance/96772/>

⁴¹ <https://www.zdnet.com/article/phantomlance-spying-campaign-breaches-google-play-security/>

⁴² <https://www.kaspersky.co.uk/blog/infected-apkpure/22559/>

⁴³ <https://securlist.com/triada-trojan-in-whatsapp-mod/103679/>

⁴⁴ <https://threatpost.com/custom-whatsapp-build-malware/168892/>

⁴⁵ https://www.trendmicro.com/rn_u/research/tb/b/user-beware-rooting-malware-found-in-3rd-party-app-stores.html

⁴⁶ https://www.trendmicro.com/rn_u/research/tb/b/user-beware-rooting-malware-found-in-3rd-party-app-stores.html

⁴⁷ <https://unit42.paloaltonetworks.com/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/>

⁴⁸ <https://unit42.paloaltonetworks.com/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/>

Voice assistant stores

Vulnerability of Alexa Skills App Store

In early 2021, security researchers from North Carolina State University and Ruhr-University Bochum discovered a [vulnerability within the vetting process of creating skills for Amazon Alexa](https://www.theregister.com/2021/02/25/alexa_amazon_skills/)⁴⁹.

A malicious actor could develop a benign skill under an arbitrary developers' name, namely a trusted popular developer, which could then be modified to include malicious content afterwards (known as versioning). Such changes could be added to coax a user into revealing sensitive information, such as their payment details or a phone number.

This was tested by security researchers, who created a skill that allowed users to create a trip itinerary. As a phone number is a permission-protected data type, it should be included within an API and not directly requested, [according to Amazon](https://www.theregister.com/2021/02/25/alexa_amazon_skills/)⁵⁰.

However, [the skill was later tweaked without the use of the dedicated API](https://www.theregister.com/2021/02/25/alexa_amazon_skills/)⁵¹ to request a user's phone number so the users could be sent a text containing this itinerary.

Of the 90,194 skills that were analysed by the researchers, it was found that a further 358 skills were capable of [requesting information that should be protected by a permission API](https://www.theregister.com/2021/02/25/alexa_amazon_skills/)⁵².

While it is not known whether this has been used for malicious purposes, it has highlighted that this could be a potential attack vector. The ability to publish a skill under any developer name, [bypassing permission APIs and making backend code changes after approval to trigger dormant intentions](https://www.theregister.com/2021/02/25/alexa_amazon_skills/)⁵³ could all undermine the security of a user. Amazon has reportedly confirmed some of the report's findings and is working on countermeasures.

This highlights the same threat profile that both mobile and other device application stores contend with; the ability for malicious apps to gain access to users personal data and infringe on their privacy.



IoT smart device stores

Spyware vulnerability on Fitbit Gallery

In October 2020 a security researcher was successfully able to distribute malicious apps using the [Fitbit Gallery](https://www.fitbit.com/gallery)⁵⁴. Fitbit allows users to upload applications to their legitimate Fitbit store without checks, providing the application is only accessible via a private link. [Fitbit state in their documentation](https://www.immersivelabs.com/resources/blog/fitbit-spyware/)⁵⁵ that privately published apps are 'not visible within the Fitbit App Gallery, and can only be installed by clicking on a direct installation hyperlink from a mobile device that has the Fitbit mobile app installed'.

This may mitigate against many users downloading it directly from the store. However, malicious actors may use this to target specific individuals in a social engineering attack. As the link would be one to the official Fitbit Store, this may give users a false sense of security that what they are downloading is safe and legitimate.

This vulnerability was exposed by a [security researcher from Immersive Labs](https://www.immersivelabs.com/resources/blog/fitbit-spyware/)⁵⁶, who successfully uploaded an application to the Fitbit domain containing 'spyware/stalkerware capable of stealing everything from location and personal body data to connecting to company networks for a range of malicious actions'.

A prompt response from Fitbit has seen the introduction of a 'warning message for users within the UI when installing an app from a private link' and 'adjusting default permission settings during the authorization flow to being opted out by default'. All applications uploaded to the Fitbit public store undergo a manual review to determine if the software contains malicious code. However, this does not address those uploaded privately such as in this case. The potential for malware being hosted and distributed to users, regardless of the device, is the most recognisable threat to application stores.

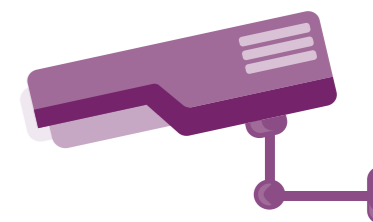
Vulnerabilities in Tizen OS used for smartwatches and smart TVs

In 2017, a security researcher disclosed that he had discovered [40 zero-day vulnerabilities](https://www.vice.com/en/article/ky9p7n/samsung-tizen-operating-system-bugs-vulnerabilities)⁵⁷ (that is, software vulnerabilities that are yet to be patched by the vendor) in Tizen, an operating system developed by Samsung for use in smart TVs, smartwatches and mobile devices.

The most critical of the vulnerabilities affected Tizen Store, the app store used on devices running Tizen. This vulnerability allowed for remote code execution, which is when a malicious actor is able to remotely hijack a device. Through the vulnerability, the researcher was able to push malicious code to his Samsung TV.

While this case study showcases the consequences of vulnerabilities in app stores as opposed to the actual apps, it nevertheless shows how a malicious actor could exploit these vulnerabilities to spread malicious apps and infect users of smart devices.

Samsung responded to this incident stating that they would cooperate to mitigate security issues discovered by security researchers.



⁴⁹ https://www.theregister.com/2021/02/25/alexa_amazon_skills/
⁵⁰ <https://developer.amazon.com/en-US/docs/alexa/custom-skills/request-customer-contact-information-for-use-in-your-skill.html>
⁵¹ <https://thehacknews.com/2021/02/alert-malicious-amazon-alexa-skills-can.html>
⁵² https://www.theregister.com/2021/02/25/alexa_amazon_skills/
⁵³ <https://anupamdas.org/paper/NDSS2021.pdf>

⁵⁴ <https://gallery.fitbit.com/>
⁵⁵ <https://dev.fitbit.com/build/guides/publishing/>
⁵⁶ <https://www.immersivelabs.com/resources/blog/fitbit-spyware/>
⁵⁷ <https://www.vice.com/en/article/ky9p7n/samsung-tizen-operating-system-bugs-vulnerabilities>

Gaming stores

Malware spread via fake Steam pages

In 2015, attackers [created a copy of the Steam profile page](#)⁵⁸ of the legitimate game Octopus City Blues in an attempt to spread malware. The page was made to look as authentic as possible, using trailers, screenshots and descriptions of the game.

The perpetrators even deleted negative comments left by victims who were attempting to warn others about the scam. These measures boosted the chances of a user downloading the supposed demo for the game and introducing malware onto their device.

Steam eventually removed the page, along with other similar scams. Similar threats can be seen across numerous platforms, with malicious software impersonating legitimate safe applications.



Summary

The report illustrates how app stores across all devices share the same threat profile, and how cyber criminals (and other attackers) seek to take advantage of weaknesses within the vetting processes of these stores to infect users with malware for either financial or privacy impacting outcomes.

While *all* app stores share the same threat profile, *mobile app* stores are the most commonly targeted due to the sheer number of smartphone users, and the wealth of data stored on modern smartphones. Users of third party mobile app stores are particularly vulnerable, due to their lack of robust vetting processes. App store operators that adopt the Code of Practice outlined in the [DCMS's report 'Call for Views on App Store Security and Privacy Interventions'](#)⁵⁹ (including through further development of technical solutions) will reduce the likelihood of malicious apps getting through vetting processes.

The Ipsos MORI consumer data shows that relatively few UK consumers currently rely on third party app stores. However, this could change in the future, depending on the outcome of various global antitrust bills and investigations.

Finally, the use of apps has greatly increased due to the impact of the COVID-19 pandemic. This dependence on apps further highlights the importance of users and organisations being able to securely install apps from a variety of sources, both official and third party and for mobile and non-mobile devices.

⁵⁸ <https://www.bitdefender.com/blog/hotforsecurity/steam-users-beware-bad-guys-hide-malware-inside-fake-game-demos>

⁵⁹ <https://www.gov.uk/government/consultations/app-security-and-privacy-interventions>

 @NCSC

 National Cyber Security Centre

 @cyberhq

© Crown copyright 2022. Photographs produced with permission from third parties.
NCSC information licensed for re-use under Open Government Licence
(<http://www.nationalarchives.gov.uk/doc/open-government-licence>).

