wandera

Understanding the key trends in mobile enterprise security in 2020

2020 promises to be another momentous year for mobile security, with cyber attacks growing rapidly in sophistication and distribution. This report will cover the key mobile security trends that emerged last year and offer high-level recommendations for the year ahead.

Introduction

2019 was a particularly tumultuous year for security teams who faced a number of hair-raising incidents. Popular gaming apps were being used as a platform to launch sophisticated phishing attacks, the official app stores failed to identify several advanced attack techniques and, ultimately, were responsible for distributing malicious apps, a series of iOS vulnerabilities were discovered affecting Apple's FaceTime and iMessage apps, and hackers were able to exploit a remote vulnerability in WhatsApp to install spyware, putting more than a billion users at risk.

As organizations fight to secure their valuable data against an ever-growing range of threats, the fear of a data breach and increasing regulations around data security and privacy are keeping CISOs up at night. In 2019, high-profile breaches continued to capture public attention, with data leaks coming from household names including Capital One, Zinga, Houzz, Quest Diagnostics, and Dubsmash.

Everybody is waiting for a breach to happen on a mobile device. But the reality is that mobile devices — just like all other enterprise endpoints — are where the attack starts but rarely finishes. Mobile devices expose data "bread crumbs" (such as log in credentials) that can lead hackers to the data jackpot. For example, although log in credentials are a relatively small piece of information they could be used by a bad actor to gain access to confidential information stored elsewhere.

This report aims to help you understand which threats you need to worry about by examining key security trends and data from organizations that have embraced mobile computing. The key trends we identified concern: app store security, malware, vulnerabilities, phishing attacks, and data privacy.

Our analysis includes data from Wandera's global network of 425 million sensors, and represents both corporate-owned and BYOD assets, making it the world's largest and most insightful mobile dataset. Wandera's unique architecture makes this annual report the most comprehensive look at the risks facing remote workers and mobile-enabled businesses.

Trend One

App stores aren't providing reliable security checks

App vetting is a laborious task, but a necessary one. Malicious apps are increasingly using clever techniques to evade detection. For example, more sophisticated malware will wait a certain number of days before initiating malicious behavior, they will only behave badly on a certain network, or they will contain dormant command-and-control code that can be activated by a hacker at any time. Basic checks, such as those performed by the app stores to ensure that apps are performant and adhere to the latest resolution guidelines or user interaction standards, will not catch truly malicious apps.

The official app stores

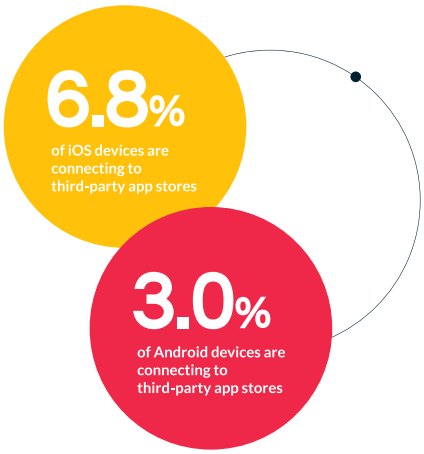
Apple and Google seem to have reached their limits in terms of how far their existing app vetting tools can scale. Currently, app store security checks focus on high-level usability factors. For example: Does the app do what it says on the box? Is the user experience good?

As a result, thorough security assessments can fall by the wayside. Apple has acknowledged that it needs to update its screening tools to better detect suspicious applications moving forward. Meanwhile, Google announced its new App Defense Alliance, aimed at improving the security of the Play Store by bringing in security partners to help detect potentially harmful apps.

Until the official app stores can bring more rigor to their security reviews, organizations need to acknowledge that there is risk on the official stores and start taking steps to protect employee devices. Simple measures like only downloading trusted apps and doing your own application vetting is a good place to start.

Third-party app stores

While the App Store and Play Store remain the two largest distribution channels for mobile apps, there's a big, bad world of third-party app stores and apps that exist outside of these two major players. In fact, there are more than 300 app stores worldwide, and that number continues to grow.



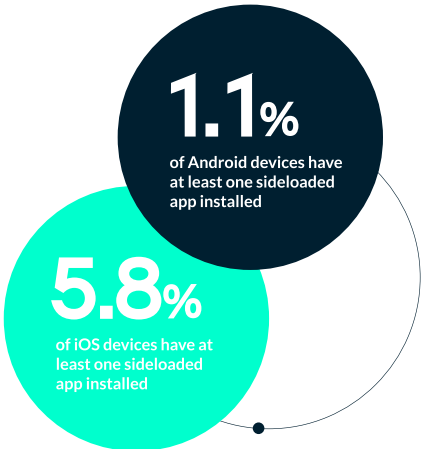
While some iOS users may jailbreak their mobile devices purposefully to install security enhancements, most users do it to install applications that aren't available on the official app stores. It is also possible to install third-party apps without the device being jailbroken; this is a process referred to as sideloading apps. All the user needs to do is configure the device to trust a specific developer and they can then install any app from that developer without going through the app store. This is how a lot of companies install apps for their employees without publishing those apps on the App Store.

Google does not lock down the Android OS as much as Apple does with iOS. While Android's default configuration does not allow sideloaded apps, it is possible to change settings to allow apps from third-party sources. According to our data, one in five Android users have their devices configured to allow third-party app installs.

Sideloaded apps

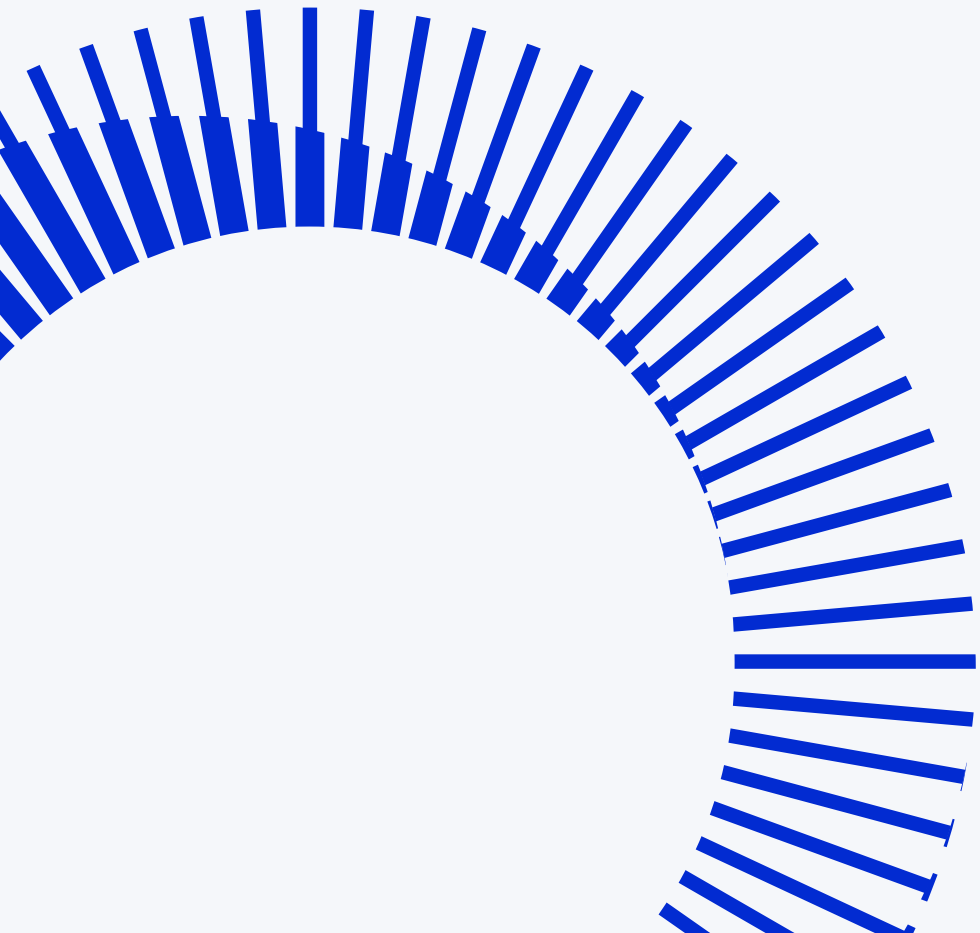
Users that sideload apps face increased security risks because the application review process enforced by Apple and Google on their official app stores is bypassed and, thus, the device has less protection against inadvertently installed malware.

The number of iOS devices with a sideloaded app installed rose significantly in 2019, up from 3.4% in 2018. The increasing use of BYOD in the workplace is likely to blame because users in that scenario have more control over their devices. Developer certificates also present a risk, and so do jailbreaks. These are both reduced when devices are under management, as companies are able to ensure consistent configuration over time.



Recommendations for effectively managing mobile app risk

Acknowledging that official app distribution channels are not running comprehensive security checks is an important first step; it enables organizations and users to take a more proactive and thoughtful approach to selecting applications. However, app vetting can be a challenge for organizations to adopt because it's difficult to scale, particularly for larger organizations and those where BYOD and personally enabled corporate devices are in the mix. The best way to manage the problem is to put a mobile security solution in place that includes an app vetting component that is coupled with automation and policy enforcement capabilities. This ensures a continuous evaluation of not only apps, but device and user behavior as well. Any time an app exceeds the tolerable risk, action can be taken.



Trend Two

All mobile malware has a purpose, it's just not always clear

Mobile malware is a widely known, high-priority security concern for organizations around the globe. When thinking about mobile malware, it's important to remember that malicious apps come in all shapes and sizes, and there is a lot that must be considered when assessing the riskiness of apps. If your limited definition of malware is 'software that steals your data,' then you might be missing the point. Malware developers are redefining their craft to evade detection, disrupt productivity, open back doors and, of course, steal data.

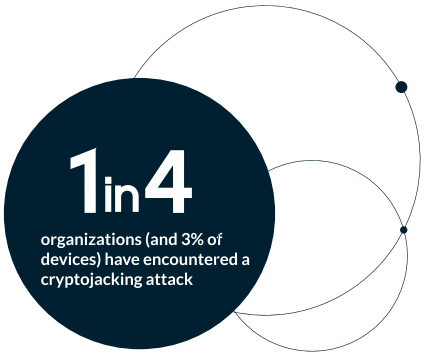
Evading detection

Apps with blatantly obvious malware embedded will rarely make it past the basic app store review process. However, apps that can disguise and layer malicious functionality are much more successful at making it onto the stores and into broader distribution.

> Seven dropper malware apps designed to pull down adware APKs from a GitHub repository were found on the Google Play Store. This essentially opens a backdoor on the device for any new application functionality to be installed. The droppers were cleverly crafted to evade detection — the apps waited before sending the request to GitHub and the embedded GitHub URL was obfuscated to prevent the URL string from being flagged by any human analysis or app store security checks. Because the adware APKs could self-execute without user interaction, and because the video ads required manual dismissal, this adware could seriously impact device battery life and data consumption.

Blocking productivity

Data theft is perceived as the most damaging implication of a malware infection but this doesn't mean that other risky behavior should be discounted as low-severity threats. A denial of service attack can occur when a user's device is flooded by persistent ads. For certain industries, like transportation and healthcare, having a device suddenly taken offline by malware can be devastating. Intrusive out-of-app ads interrupt users in the middle of their workflows, brick their devices and drain their devices' batteries. In some cases, when the adware is difficult to remove, infected devices need to be replaced altogether.



> Two selfie camera apps infected with adware were found on the Google Play Store with a combined 1.5M+ downloads. Once installed, the app icons were visible in the app drawer. But when the apps were opened, they created a shortcut and then removed themselves from the app drawer. Even after uninstalling the shortcuts, the apps stayed active and could be seen running in the background.

Malicious cryptojacking has a similar impact on user productivity, but it presents a more significant risk than adware. Cryptojacking malware doesn't typically steal data or lock a user out, but it can render a device unusable by slowing the processor down and draining the battery. We delve deeper into cryptojacking in the next section.

Opening a back door

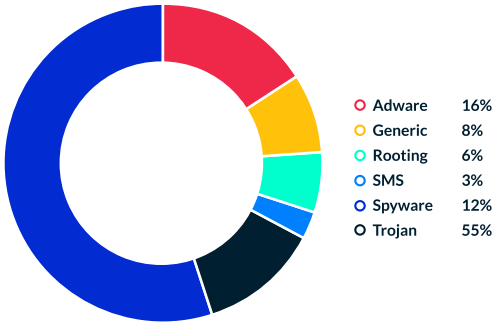
A cleverly designed command-and-control (C&C) infrastructure enables bad apps to bypass security checks because it activates a communication channel directly with the attacker, which is difficult to detect by analysis of the app alone. C&C infrastructure is a 'backdoor' into the app, which can lead to exploitation if and when a vulnerability is discovered or when the attacker chooses to activate additional code that may be hidden in the original app.

> 17 apps infected with clicker trojan malware were found on the Apple App Store. The apps were communicating with a known C&C server to simulate user interactions in order to fraudulently collect ad revenue.

Stealing data

The obvious aim of malware is to steal data, but having this functionality embedded in an app makes it more likely to be detected by app store security checks. However, apps are getting better at stealing data covertly, usually via social engineering techniques like phishing.

> A horror gaming app with layers of malicious functionality was found on the Google Play Store with over 50,000 installs. Once installed, the app triggered a persistent adware-style, Google-themed phishing attack on the victim's device. If the app was successful in capturing the victim's Google credentials, it would log in and scrape more PII from the victim's Google account and send it to a server silently in the background.



Recommendations for dealing with malware

The best way to protect your entire mobile fleet from malware is to have a security solution that continuously monitors for suspicious application behavior and characteristics present on the device and also monitors for command-and-control communication and data exfiltration at the network level. As we have seen in the above examples, many bad apps go undetected because app store security checks do not dynamically test applications and their related network activity. The most successful malware attacks are layered, so a layered approach to security — addressing both the endpoint and the network — is required. Additionally, the best solutions for malware detection are powered by machine learning engines that enable the identification of unknown threats, rather than relying on signature-based techniques that only address known threats.

Trend Three

More high-severity vulnerabilities are being found in mobile operating systems

Vulnerabilities are the 'lurking culprits' within your mobile enterprise. These weak points are either flaws in the OSs or flaws in apps that third parties can exploit to gain access to devices and the valuable data they contain.

High-profile vulnerabilities (and exploits)

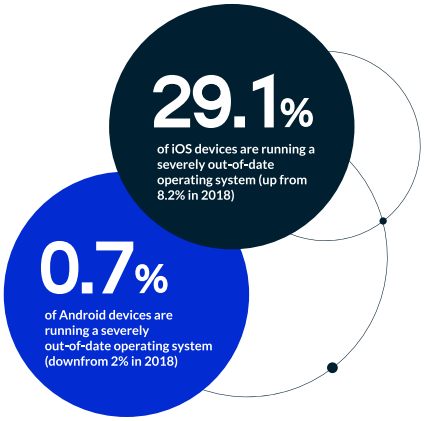
August 2019 was an unexpected wake-up call for many. In the space of a month, multiple iOS vulnerabilities were reported, including one that allowed an attacker to read files off an iOS device without any interaction from the end user. When the patch was released in iOS 12.4, it was quickly discovered that Apple had also reopened a previously patched jailbreak vulnerability. For a period of time, there wasn't really a secure iOS version available and users just had to pick their poison until the next patch was released. All of this followed the group FaceTime bug discovered in February, which allowed bad actors to eavesdrop on conversations.

Apple, which is widely regarded as a producer of some of the most secure devices in the industry, is quickly losing this reputation. iOS exploits have become common enough that Zerodium, a zero-day exploit broker, is offering more for Android hacking techniques than for iOS. This isn't to say that breaking into an iOS device or any other type of mobile device is easy — zero-click iOS attacks are still valued at around $2 million.

In addition to these platform vulnerabilities in 2019, there was a major vulnerability affecting one of the world's most popular messaging apps: Whatsapp. This vulnerability let malicious actors remotely install spyware on a still-unknown number of affected phones merely by making a call to a device. Wandera data showed that even six months after WhatsApp urged its 1.5 billion users to install a patched version in May, more than one in 15 users hadn't updated and remained susceptible to attack. These vulnerabilities are often used to target high-profile individuals, in a notable example it was revealed that the WhatsApp vulnerability was used to exfiltrate large amounts of data from Jeff Bezos' phone.

Security patch uptake is (absurdly) slow

The string of iOS vulnerabilities that occurred in August brought to light the threat posed by outdated operating systems. Manufacturers release frequent updates for their OSs that contain not only performance improvements, but important security patches for vulnerabilities that may have active exploits. The issue is that Apple's updates combine security patches with feature updates, and the notifications informing users of an available software update can be ignored. By way of basic human nature, some users will hold off on installing the latest software update due to the time it takes for the device to turn back on, while others will hold off for a variety of other reasons — the key takeaway here is that there is still a general lack of awareness around the importance of the security patches included in these software updates.



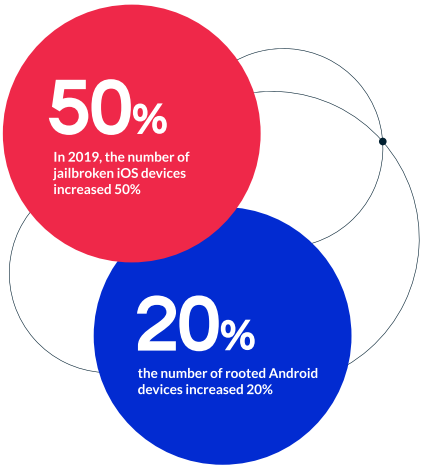
Google, on the other hand, rolls out security patches and feature updates separately for Android. However, these updates aren't always reaching devices in a timely manner since they are often delayed by manufacturers and carriers.

> While IT departments have struggled to get a handle on managing mobility, the percentage of out-of-date operating systems has been trending down on Android, but up on iOS. Wandera informs admins of out-of-date devices and what they are vulnerable to, and encourages them to update these devices. This decrease might also be due to both increased visibility into detailed vulnerabilities per platform and better upgrade notifications and processes instituted by device manufacturers and organizations.

User-introduced risks

Vulnerabilities don't always just happen for users — sometimes users make their devices vulnerable, whether intentionally or unintentionally. Jailbreaking and rooting are risky configurations that allow users to gain access to the operating system of a device and enable the installation of unauthorized software functions and applications. These tactics are also popular among users trying to free their device from a carrier lock.

Surprisingly, one of the simplest security measures available on a mobile device is still often neglected: the lock screen. Despite the lock screen setup being active by default on most devices, some users are going out of their way to disable it, leaving their devices more vulnerable if theft occurs.



Recommendations for reducing the exposed surface area caused by mobile vulnerabilities

It's not always practical or realistic to make sure every single device in your fleet is on the latest OS. Not all outdated versions pose the same degrees of risk. However, if you have the right security and device management solutions in place, it's possible to detect out-of-date OSs by severity rating and to enforce a strict policy regarding the installation of critical updates.

Trend Four

Phishing attacks have never been more effective

Phishing attacks have evolved far beyond poorly-worded emails offering 'unclaimed lottery winnings.' In 2020, phishing is not only pervasive, but it is also the most damaging high-profile cybersecurity threat facing organizations today.

Smarter distribution

Our research shows that a new phishing site is launched every 20 seconds. Making matters worse, scammers are now focused on device-centric social engineering to target users in places where they wouldn't expect to find these types of attacks, such as gaming, messaging and social media apps.

Not only are phishing attacks reaching users in more places, but they are more personalized. Business email compromise (BEC) attacks are moving to other forms of communication such as social media messengers, and spear phishing is made easier on mobile simply by knowing someone's phone number. Malicious actors are taking the time to research their targets' behavior patterns and work environments to exploit any weaknesses.

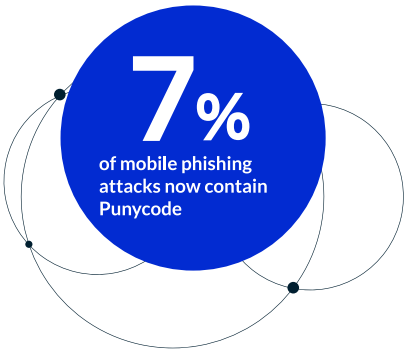
Using encryption

Phishing is also becoming impossible to detect visually. Double-checking the address bar for suspicious URLs used to be an easy way to catch a spoof domain, but now attackers use free services like Let's Encrypt to gain SSL certification for malicious phishing sites. Unfortunately, this is effective because users believe the padlock symbol preceding a URL is a reliable indicator that a website is safe.

Disguised with Punycode

Attackers are increasingly using Unicode to make their phishing domains harder to detect. Punycode converts words that use Unicode characters (in languages like Cyrillic, Greek and Hebrew, for example) into ASCII characters so that computers can understand them. Unicode characters make domain names that look familiar to the naked eye but actually point to a different server or link to an unfamiliar domain.

It's easy for an attacker to launch a domain name that replaces some ASCII characters with similar-looking Unicode characters. However, different alphabets are not the only sources of characters that can be converted to ASCII using Punycode — the ever-growing library of emojis can also be converted using Punycode.



Brand	What the user sees	The Punycode
Singapore Airlines	sıngaporeair.com	xn--sngaporeair-zzb.com
Rolex	rolẹx.com	xn--rolx-nu5a.com
IKEA	ikea.com	xn--iea-f6a.com
Google	google.com	xn--googe-95a.com

Using big brands

To increase the success rate of an attack, malicious actors need to be selective when deciding which companies to impersonate. It's simple — more users means "more phish in the sea."

Malicious actors are increasingly targeting applications used for work, such as Office 365 and Google's G Suite apps. As businesses strive to move their corporate assets to the cloud, this is a major concern. One slip up by an employee who receives a clever phishing attack (e.g., asking them to confirm their Google Drive login credentials) can give a hacker access to corporate assets stored on these types of popular cloud applications.

Top 20 brands used in mobile phishing campaigns

Apple	eBay	Netflix
PayPal	US Government	Bank of America
Runescape	Chase	Airbnb
Facebook	Wells Fargo	Twitter
Amazon	Microsoft	American Express
Google	Instagram	Yahoo
UKGovernment	Office 365	

Recommendations on how to mount an effective defense against mobile phishing attacks

Many phishing sites are published online for only a few hours before hackers move to an entirely new hosting server. This allows them to evade detection and maintain ongoing campaigns without being blocked. The risk to users is highest in those first critical hours before static, list-based threat intelligence is updated. In this short window of time, mobile devices are most vulnerable to newly published attacks, and the stakes are higher when they target corporate cloud applications. That's why a zero-day phishing solution -- specifically one that operates across all communication apps, not just email -- is critical in stopping both the common attacks and the more sophisticated ones that were just launched against your business.

Trend Five

Mobile users are losing control of their data privacy

As a society, we have come to accept invasive apps and services that collect rafts of personal data in exchange for more personalized services. We have embraced the mobile experience — the one-click access to information and services — and in exchange, we have to trust our devices to hold all our private information. There are a number of key elements that make data privacy a challenge. These include data mishandling, invasive app permissions, Man-in-the-Middle attacks, and data leaks.

Companies misusing data

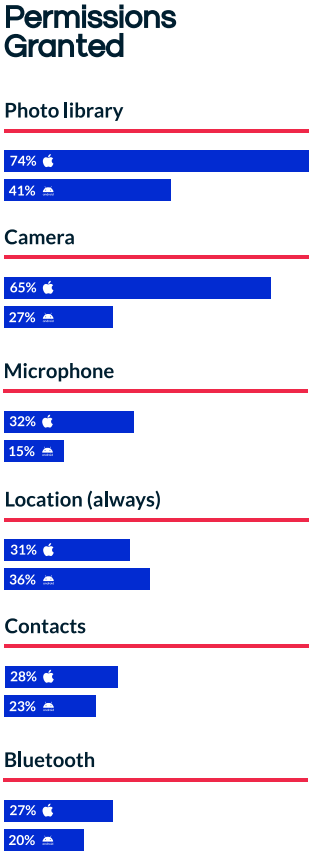
With so many cases of companies like Facebook and Uber misusing data and funnelling it through to unscrupulous third parties, users are becoming more sensitive to how their data is used. This sentiment is being carried over into the workplace, as IT teams struggle to balance the need for visibility and control over mobile devices with this growing demand for user privacy. Additionally, incidents like the WhatsApp spyware attack have caused consumers to be concerned about the security and stability of apps themselves.

> "In many ways, data is now more valuable than currency."
>
> Jamie Woodruff, Ethical Hacker

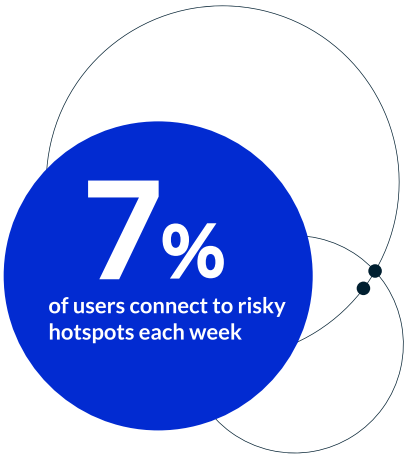
Apps asking for too much

It is important to pay attention to the permissions you're granting all apps (and not just to those apps you would consider to be risky). App permissions determine what functions and data an app has access to on your device, and some are riskier than others. Some apps collect data without explicitly asking permission, while others boldly neglect the user's preferences entirely (like this Chinese weather app that was using certain permissions, such as location, even if users denied access).

There are variations in app permissions between iOS and Android. iOS has more privacy-focused permissions, while Android tends to expose access to raw parts of the hardware and operating system. For example, iOS has separate permissions for apps to access the camera (to take a photo) and to access the photo library. The equivalent on Android includes access to the camera (same as iOS) and access to either read or write the actual storage device (e.g., flash memory). While it is not a perfect like-for-like, reading external storage is the permission that is required in order to access the photo gallery on Android. We have analyzed the app permissions for both iOS and Android to see how many apps are asking for some of the most common permissions.



Man-in-the-Middle attacks put data in transit at risk



Public Wi-Fi presents a serious privacy risk when a man-in-the-middle (MitM) attack occurs. There are two primary flavors of MitM attacks that we see impacting mobile users. The first is when the attacker has physical control of network infrastructure, such as a fake Wi-Fi access point, and is able to snoop on the traffic that flows through it. The second is when the attacker tampers with the network protocol that is supposed to offer encryption, essentially exposing data that should have been protected.

Many attackers establish fake hotspots that use naming conventions similar to popular access point names. A distracted user could easily be fooled into connecting to a malicious hotspot with a convincing name.

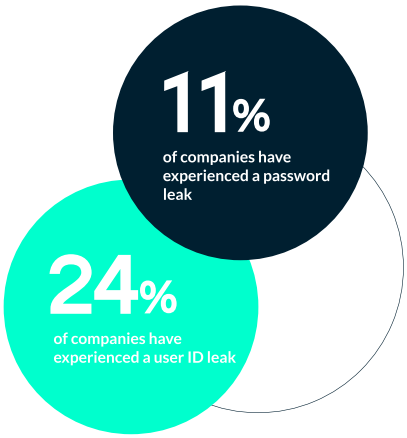
Would you fall for one of these rogue hotspots if you were near a Starbucks?

Starbucks FREE WiFi	Starbucks_InterContinental	starbuckz free wifi
Starbucks WiFi	Starbucks@BitCo	BTWifi-Starbuck

Data leaks

Data leaks certainly don't get as much attention as active threats like malware and phishing, but a leaking app is one of the biggest threats to users' data privacy. By failing to encrypt data, an app or website developer is essentially making user data much more readily available to a MitM sitting on the same network as the device with the leaking app.

Our research shows that a username is exposed in 90% of PII leaks, a password is exposed in 85%, and credit card details in 2.3%. Don't discount the implications of a password leak. Hackers can easily break into corporate accounts by capturing a user's credentials with a MitM attack and using a tool to instantaneously plug those credentials into thousands of login pages at once. The scary reality is that using a poorly developed app on public Wi-Fi could lead to a major data breach.



Recommendations for enhancing user privacy

Mobile users are already struggling to regain control of their privacy. That's why it's important for IT teams to support them. Most endpoint security solutions allow for basic man-in-the-middle detection by identifying rogue hotspots and suspected MitM activity. However, network-based detection can go a step further by monitoring network transmissions for unencrypted data transfers (data leaks). A network-based policy engine can do even more by blocking data exposures on unsafe networks, therefore enhancing user privacy while also guaranteeing the confidentiality of sensitive data as it is communicated across the network. What's more, an additional layer of encryption, such as a VPN or encrypted DNS, can help keep user data private and secure from online profiling and theft.

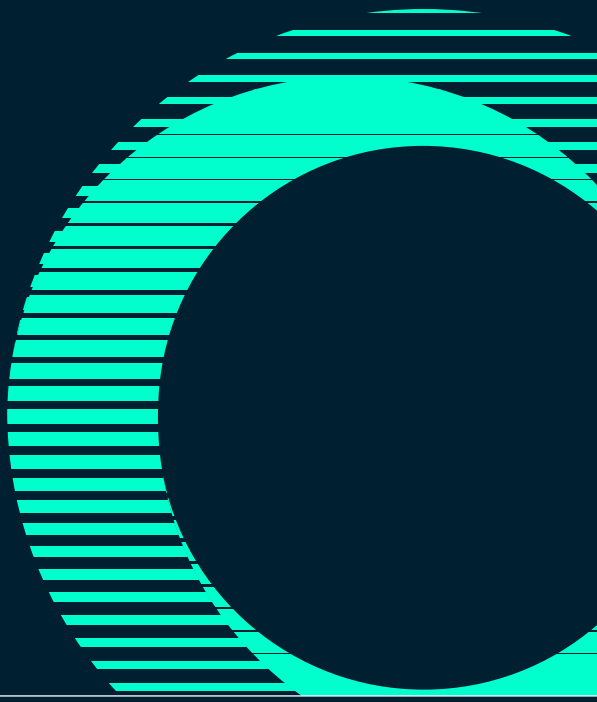
Protecting corporate-enabled devices

This coming year, these five trends will be the most concerning and pervasive among mobile enterprises. With data breaches costing upwards of $3.92 million, prevention is better than remediation. With the right security strategies in place you will be better positioned to protect your organizational data from attack.

> "A vicious cycle of low adoption of MTD solutions leads to low visibility of mobile risks, which, in the absence of spectacular mobile breaches, leads to a continued low perception of mobile risk."
>
> Gartner Market Guide for MTD 2019

Wandera's cloud-based security solution addresses all the threats mentioned above: zero-day malware and phishing detection powered by machine learning, application vetting, vulnerability detection for operating systems and applications, jailbreak and rooting detection, MitM detection, data leak detection, secure access to cloud applications, encryption technologies, and more.

If you'd like to learn more about protecting your organization from mobile threats, get in touch with one of our experts today.



The Wandera Security Cloud protects enterprises at the new edge, where data is in the cloud and users are remote. Unified security capabilities include threat protection, content filtering and zero-trust network access.

For more information, get in touch with one of our security experts at www.wandera.com/contact-us/

wandera.com

Wandera Ltd
45 Mortimer Street
London W1W 8HJ
+44 (0) 203 301 2660

Wandera Inc.
220 Sansome Street, Suite 1400
San Francisco CA 94104
+1 (415) 935 3095