wandera

Understanding the mobile threat landscape

It should 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 as well as summarize thoughts for the mobile threat landscape for the year ahead.

Table of contents

Introduction

It was a scary time for IT and security teams in 2018. Attacks that exploited AI features, sophisticated malware in broad distribution, unrecognizable phishing techniques, and widespread abuse of location data were just a few of the trends that made 2018 a particularly tumultuous year for security teams.

As organizations fight to secure their valuable data against an ever-growing range of threats, the fear of a data breach is keeping CISOs up at night. In 2018, one breach headline after another captured public attention, with high-profile data leaks hitting Marriott Starwood Hotels, British Airways, MyFitnessPal, T-Mobile, Google and Facebook.

Additionally, 2018 was the year that GDPR (General Data Protection Regulation) came into effect. With heftier fines for data breaches and a shorter window of time for affected companies to report known breaches, 2019 is poised to be the "Year of GDPR Lawsuits". A prime case in point was Google being fined $57m under the GDPR regime in the first month of the year.

Why do malicious actors seek to infiltrate corporate devices? How are they getting past existing security measures? What makes the current mobile security climate so volatile? This report aims to answer these questions by reflecting on the latest wave of mobile threats and vulnerabilities, reporting on the threat landscape, and making projections for the year ahead. The data in this report comes from our network of corporate-enabled mobile devices across thousands of enterprise customers globally, making up the world's largest mobile security dataset.

"There have been so many prolific hacks like Equifax, that customers have low confidence in large companies or institutions guarding their personal data. The general sentiment is becoming 'if it's online, it's at risk'."

MATT BROOKS, PRODUCT MARKETING AT CITRIX

In the past year, we've seen:

32,846
malware incidents

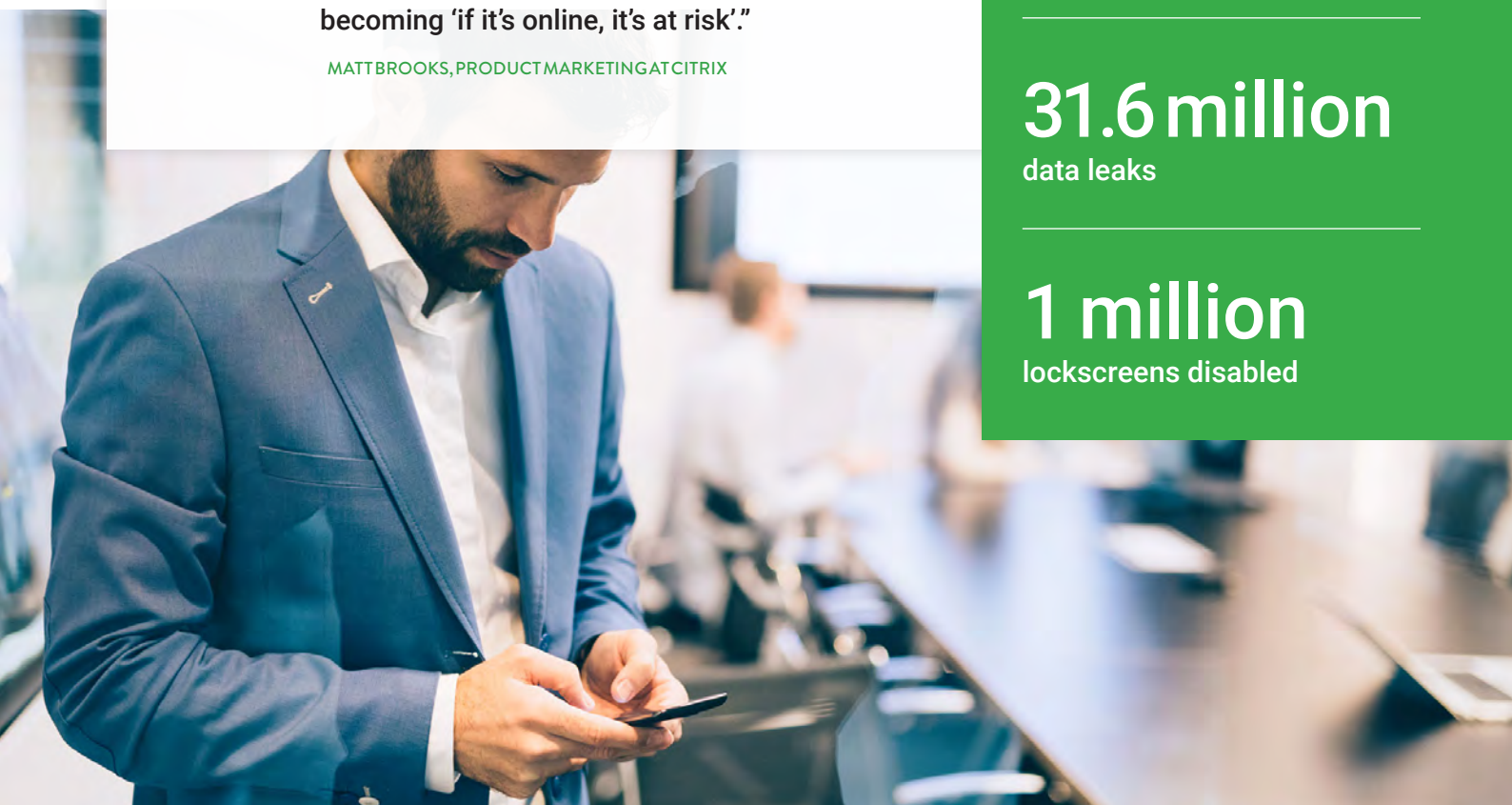
455,121
phishing incidents

1.9 million
Wi-Fi incidents

3.4 million
out-of-date operating systems

31.6 million
data leaks

1 million
lockscreens disabled



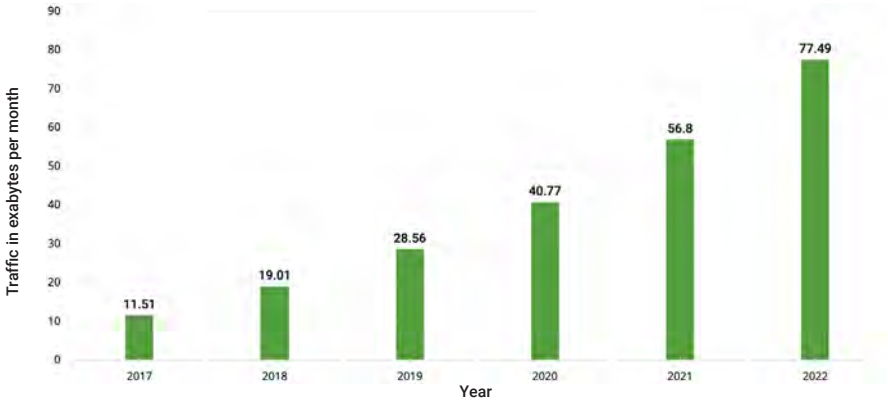
A changing landscape

Threats have increased in sophistication

Apple and Google took great strides to strengthen the security of their devices in 2018 and, as a result, attackers have increasingly looked to circumvent hardened platforms by turning to social engineering techniques. With the rise of BEC (Business Email Compromise) and spear phishing attacks, it has become abundantly clear that malicious actors are taking the time to research their targets' behavior and exploit weaknesses.

With more web traffic now taking place on mobile than desktop, scammers are taking note by hitting victims with regular device-centric scams that leverage popular apps. Instead of casting wide nets with comparatively rudimentary techniques in the hope that some will take the bait, attackers have focused on creating the most effective social engineering techniques to bolster success rates.

Global mobile traffic from 2017-2022



Source: Statista 2019

Mobile has made us more exposed to attacks

Technological advancements, paired with a deeper understanding of how to manipulate victims, broadened the attacker's repertoire in 2018. As a society, we have come to accept invasive apps and services that collect rafts of personal data in exchange for more personalized services. This has reached a point where we've become somewhat blasé with whom we share our most personal information.

Many organizations embraced BYOD (Bring Your Own Device) policies with open arms. As a result, internal IT teams forfeited sovereignty over these devices, which reach deep into corporate servers and sensitive databases. Attackers found new ways to trick us into doing exactly what they want us to do: allow them to infiltrate organizations and retrieve highly confidential data.

The number of mobile phone users in the world was predicted to pass the 4.7 billion mark by 2019, so it comes as no surprise that mobile is now the focal point of attacks. Cybercriminals have developed a troubingly deep understanding of human nature, and they know exactly how to use it against us.

Understanding the mobile threat landscape in 2019

1. Network attacks
2. App-based phishing attacks
3. Leaky apps
4. Risky configurations
5. SMS phishing
6. Malware
7. Known exploits
8. Out-of-date OS
9. Risky web content
10. Cryptojacking

Phishing is still the number one mobile threat

A new phishing site is launched every 20 seconds and is only active for an average of 4 hours

To most people, the word "phishing" conjures up thoughts of poorly worded emails offering 'unclaimed lottery winnings' or 'hassle free' payouts from ominous third parties. Fast-forward to 2019, and things are very different. Phishing is not only pervasive, but it is also the most damaging and high-profile cybersecurity threat facing organizations today - supported by research from Google, Black Hat and the U.S. Department of Homeland Security.

57% of all organizations have experienced a mobile phishing incident

The prevalence of phishing within our network of corporate mobile devices is very high when you consider that a lot of them are purpose-built, single-function devices, such as point-of-sale iPads that have a single payment application running with no access to web browsing or email. The likelihood of encountering a mobile phishing attack also climbs even higher as the employee count does. Once an organization exceeds 1,000 employees, the likelihood of a phishing incident reaches 85% and continues to increase exponentially as the employee count climbs.

Phishing has moved beyond email

Having realized that email was a breeding ground for cyber threats, organizations responded by enlisting email-focused security solutions to protect data. However, this style of protection fails to provide comprehensive protection for the mobile workforce, as the proliferation of mobile technology has dramatically changed the phishing landscape. Wandera's 2018 Mobile Phishing Report revealed that 83% of mobile phishing attacks occur outside of email. Less scrutinized channels like SMS, iMessage, Facebook Messenger, WhatsApp and other popular messaging apps, games and social media platforms are being employed at scale to distribute phishing links in places employees previously thought were safe from cyber threats.

83% of successful mobile phishing attacks take place outside of email

"Unsuspecting victims are encouraged to click links, or run files to launch malicious code to start the attack. Mobile phishing is relentless within the enterprise and we don't expect this to change any time soon."

SACHIN SHARMA, VMWARE

Mobile is a fertile arena for phishing attacks for a number of reasons. First, people work quickly and act instinctively on their mobile devices. The smaller screen size makes it more difficult to inspect suspicious-looking URLs, and the on-the-go nature of mobile devices means more distracted users. Also, BYOD users tend to be more trusting of their personal mobile devices, and cybercriminals use this sense of security to their advantage in exploiting human error.

Phishing attacks are using high profile sites and brands

To increase the success rate of an attack, hackers need to be selective in deciding which companies to impersonate. It's simple – reputable brands with large user communities are less likely to arouse suspicion, since victims may already receive regular communication from these brands. Plus, the more users, the more potential targets.

Top 10 most impersonated brands in phishing attacks

90% of data breaches start with a phishing attack

Phishing URLs are almost impossible to detect

Attackers are increasingly using punycode in their phishing domains to make them harder to detect. Punycode converts unicode characters (in languages like Cyrillic, Greek and Hebrew) into ASCII characters so 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 is easy for an attacker to launch a domain name that replaces some ASCII characters with similar-looking unicode characters. Not only can characters of different alphabets be converted to ASCII using punycode, but also emojis.

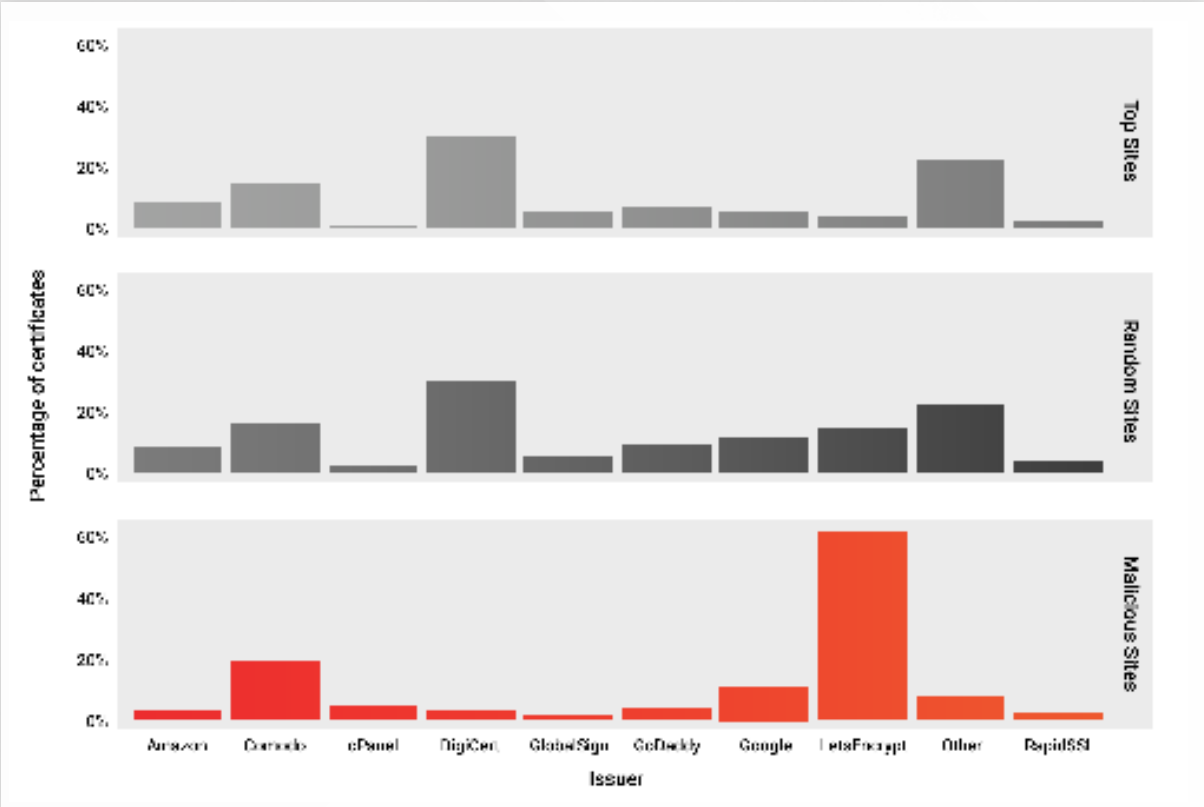
Punycode attacks are up 250% year over year, with 5.2% of mobile phishing attacks now containing punycode

Phishing sites use encryption to increase effectiveness

Our research shows significant growth in phishing sites utilizing HTTPS verification. It has been drummed into users' mindsets that HTTPS sites are secure, so a phishing attack over HTTPS is less likely to be suspected. Realizing this, hackers use free services such as 'Let's Encrypt' to gain SSL certification for malicious phishing sites.

10% of mobile phishing attacks occur over HTTPS

Most common issuers



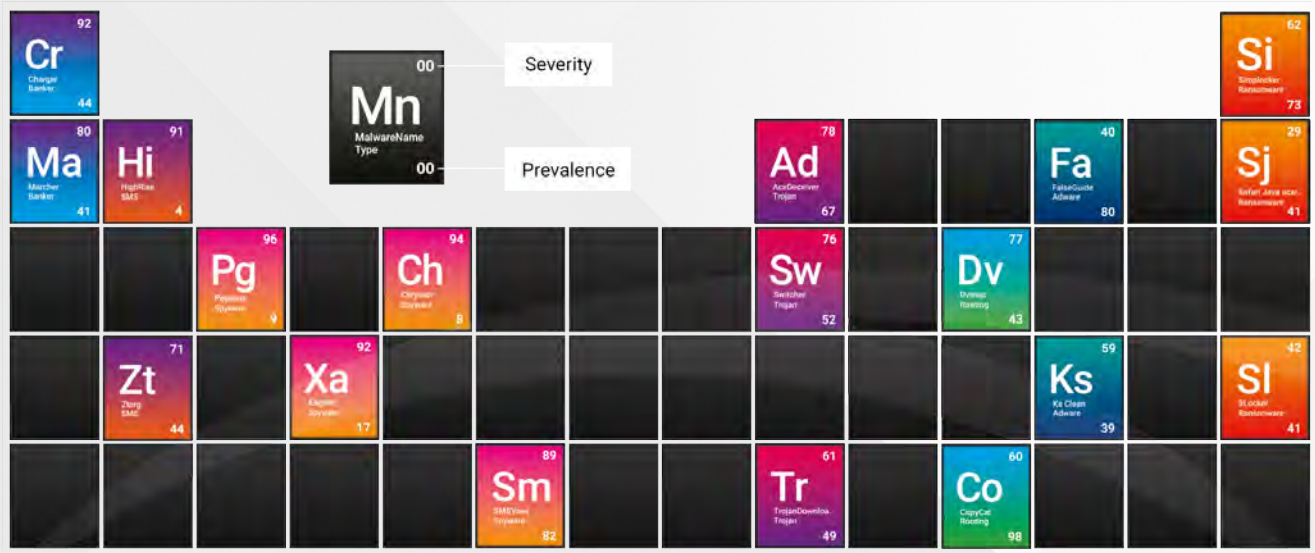
Mobile malware is growing more aggressive

Mobile malware has become a high-priority security concern for enterprises globally over the last few years. There are many factors to consider when assessing the riskiness of apps. Malicious apps come in all shapes and sizes. Which variants of mobile malware are most destructive, and what trends should enterprises expect to see over the next 12 months?

13% of all organizations have experienced a malware incident on a mobile device

Since there are many categories of malware (spyware, ransomware, trojan, banker, adware, etc.), and many types of malware that borrow characteristics from multiple categories, it's easier to analyze the impact of bad apps by asking: "What is it trying to do?"

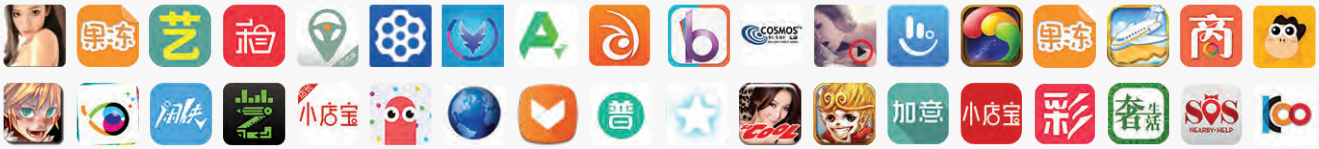
Some bad apps are designed to exploit OS vulnerabilities to steal data. Others change the configurations of devices to pull down even more malicious software with additional functionality. Some deliver pop-up ads or trigger spates of premium SMS messages for monetization. And others simply cripple devices so they becomes unusable for a period of time.



1. Is it stealing your data?

Many variants of malware are designed to reach into other applications and exfiltrate data to Command & Control (C&C) servers. One well-known example of mobile malware was RedDrop, which inflicted financial cost and critical data loss on infected devices. At the time of discovery in 2018, the 53 RedDrop-infected apps were exfiltrating sensitive data – including audio recordings – and dumping it in the attackers' Dropbox accounts to prepare for further attacks and extortion purposes.

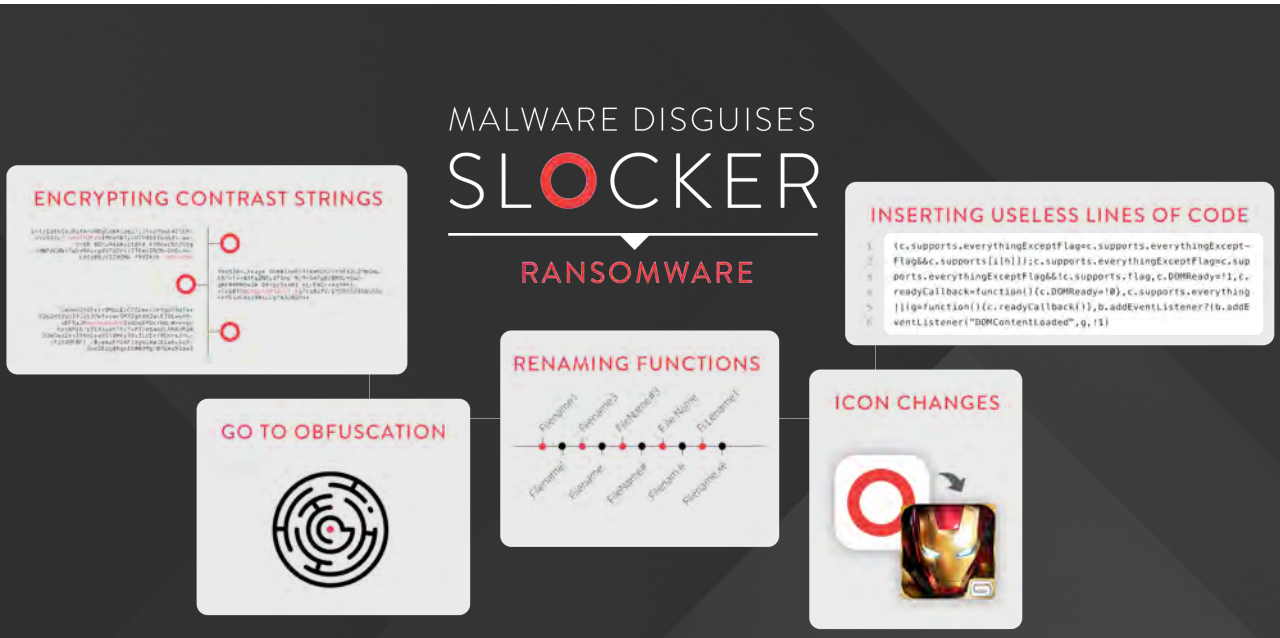
Selection of RedDrop apps



Apps within the RedDrop family provided clear functionality to the user and required some form of interaction. In one example, each time the screen was touched within the app, the user unwittingly sent an SMS message to a premium service, incurring substantial charges. The malware was able to delete these messages almost instantly, meaning the evidence was destroyed and the user remained unaware.

2. Is it locking you out so you can't access your data?

One of the most publicized types of malware that aims to lock out victims is ransomware. This type of malware demands money from victims and, in exchange, promises to release either the files or the functionality of the devices being held hostage. Ransomware tends to go in and out of popularity. For example, Wandera discovered the re-emergence of a destructive mobile ransomware called SLocker with 400 new variants. This so-called 'polymorphic' exploit is designed to evade detection by signature-based scanners, and it also contains new malicious functionalities. While initially operating stealthily, once the file encryption process is complete, the service will hijack a user's phone, block access, lock the screen, and constantly show intimidating messages until the ransom is paid.



3. Is it causing an inconvenience?

Adware is an example of malware that could fall under the less severe title of "potentially unwanted" because it doesn't cause critical damage to the device, nor does it steal data. It's more of an annoyance and a hindrance to productivity, but it can lead to more malicious attacks through links to suspicious servers. Adware is designed to show frequent ads to a user in the form of pop-ups, sometimes redirecting users to web pages or applications.

Whether you classify cryptojacking as malware, it has a very different intention, but a similar impact, compared with adware. Cryptojacking malware doesn't steal data or lock a user out, but it can render a device unusable by slowing the processor down and draining the battery. The next section delves deeper into cryptojacking.

"Malware is certainly a real threat. Our cursory research shows that there are more mobile malware samples in the wild, but they aren't taking hold on the end user devices in any meaningful way."

MICHAEL COVINGTON, VP OF PRODUCT STRATEGY, WANDERA

Mobile users are 18x more likely to click on a phishing link than they are to encounter malware

Mobile cryptojacking evolves

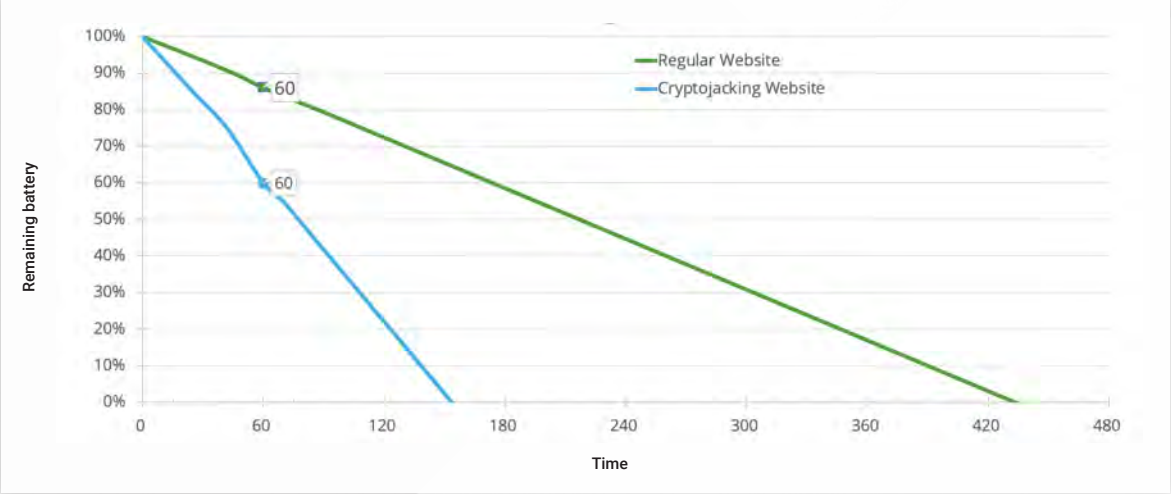
For a long time, dark web users have been utilizing cryptocurrencies for transactions. Many of these cryptocurrencies are untraceable, and their appeal is futher boosted by the simplicity of blockchain-powered fund transfers. Cryptojacking burst onto the scene in late 2017, as the price of Bitcoin was booming and people figured out that the processing-intensive act of mining for cryptocurrency was much less expensive if paid for by other people. Cryptojacking then evolved to secretly appropriating the computing power of other people's devices.

The technique involves the use of scripts that run on web pages or in mobile apps, which are designed to harvest the processing power (CPU) of the user's device to mine for cryptocurrency. Mobile is the perfect target for cryptojacking as these devices posses powerful CPUs and are typically always on.

1 in 4 organizations have encountered a cryptojacking attack

Individually, the amount of cryptocurrency extracted from each device tends to be relatively low, but when running on thousands of devices, cryptojacking can be extremely lucrative. Also, cryptojacking can be highly disruptive to a device as the battery drains faster and the device can overheat, slowing down the processor and making it impossible for the user to complete simple, everyday functions.

Battery decay of cryptojacked device vs. healthy device



To investigate further, Wandera conducted an analysis of 100,000 devices across its network of corporate-assigned smartphones and tablets. The data revealed that the number of mobile devices connecting to cryptojacking sites and apps grew by 287% month over month in late 2018, and almost all of the exposed users were unaware that an unauthorized script was running on their device. Additionally, more than a quarter of the organizations surveyed had at least one mobile device running a cryptojacking script in their fleet. Traditionally, healthcare and aviation are two sectors that have continuously raised concerns about cryptojacking and the negative impact on their end users.

Traditional use of cryptomining is tied to the price of cryptocurrency, so the likelihood of use declines if the value of cryptocurrencies drops. With the recent general drop in value of cryptocurrencies, cryptojacking may morph into DDoS attacks on IoT devices, which is a development we watching closely.

Wi-Fi threats are giving hackers access to your information

Mobile users tend to prefer connecting via Wi-Fi in favor of cellular networks for a number of reasons: Wi-Fi is typically faster, it doesn't drain your data plan, and it's widely available around the world. With airports, trains, buses, coffee shops, restaurant, bars and even gyms offering Wi-Fi, it's easy to see why connecting to open networks has become a normal part of everyday life.

3:1 is the ratio of Wi-Fi to cellular data usage

Every minute that an employee's smartphone has Wi-Fi enabled (but not connected), it is broadcasting to every Wi-Fi network in the nearby vicinity that it has joined in the past, regardless of whether that network has encryption or not. This means that while a user is walking around the neighborhood, a phone might connect to their gym, their favorite lunch spot, their office and their neary coffee shop. And along the way, the phone might make a connection to a subscription Wi-Fi network cable operator offer, like Xfinity. It's hard to stop this from happening since it's not always possible to check and clear a smartphone's list of known networks.

Wi-Fi hotspots are an enticing attack vector for cybercriminals to exfiltrate data from mobile devices used in the enterprise. For minimal cost, an attacker can obtain equipment advanced enough to set up his or her own hotspot, called a "rogue hotspot." These rogue hotspots often use copycat SSIDs that the user would expect to see in relevant locations, such as 'Coffee Shop Wi-Fi' or 'Airport Free Wi-Fi'.

Would you fall for one of these rogue hotspots?

Many attackers take advantage of familiar public Wi-Fi names (SSIDs) to trick users into connecting to their imposter networks. To the right is a list of SSIDs associated with Starbucks coffee shops that our users have encountered around the world. We identified each one of these networks as having some kind of risk, such as expired certificates or protocol tampering. This isn't to suggest that Starbucks uses risky Wi-Fi technology, but Starbucks is such a frequently visited location for mobile users that hackers are attempting to capture this huge audience by disguising their rogue hotspots as legitimate Starbucks networks.

Mobile devices make 12 Wi-Fi connections per day, on average

STARBUCKS
Starbucks
Starbucks FREE WiFi
Starbucks WiFi
Starbucks_InterContinental
Google Starbucks
Google Starbucks Roastery
#SmartWifi @Starbucks

Starbucks@BitCo
starbuckz free wifi
BTOpenzone-Starbucks
BTWifi-Starbucks
ChinaNet-Starbucks
at_STARBUCKS_Wi2
Beeline_WiFi_Starbucks_FREE

To detect a risky hotspot, you need technology that can inspect certificates, the location of SSIDs and whether or not they use encryption. Users can't be expected to know the difference between what is real and what is fake, so having a safety net in place is key.

4% of users connect to risky hotspots each week

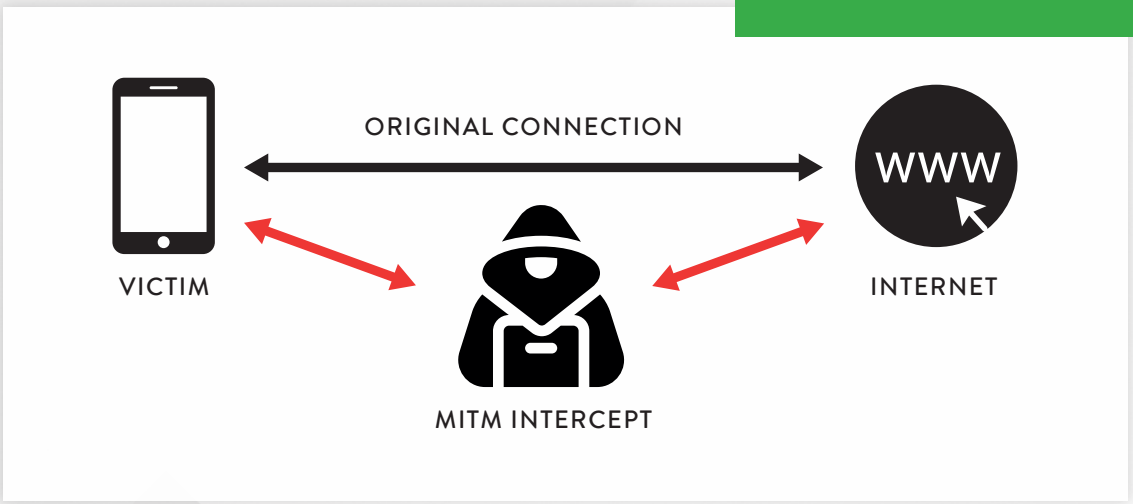
When an app sends unencrypted user information, the first barrier for a hacker is already removed. When the Wi-Fi network is also unencrypted, the attacker is free to parse through traffic and capture all unencrypted information passing through the network. A hacker can do this with a relatively cheap device that is designed to intercept and monitor nearby Wi-Fi traffic. This known as a man-in-the-middle (MitM) attack.

Over half of all organizations (55%) have at least one user who connected to a risky hotspot last month

Depending what the user is doing while connected to the Wi-Fi network, the hacker can capture valuable information such as banking credentials and sensitive corporate data. This is why it's recommended that users always turn off Wi-Fi when using a banking service or logging into online accounts in public places.

70% of Wi-Fi sessions are over an unencrypted connection

How a Man-in-the-Middle attack works



App permissions present a privacy risk

There are millions of apps available to users, and while some are in fact 'safe' and treat personal data with the utmost care, many are unsafe. This includes apps that make their way onto the Google Play and Apple App Stores. While seemingly harmless, these apps can be compromised, and personal or corporate data can be funneled through to unscrupulous third-parties.

App permissions determine what functions an app has access to on a user's device, and some are riskier than others.

It's important to pay attention to the permissions being granted to apps. Regardless of where these apps are found or how innocent they may seem, there's always a risk of compromise.

45% of the most requested permissions on Android are considered high risk by Wandera standards

As an example, we would consider the following regularly accepted permissions on Android to be high risk:

- 'Write to SD Card' - Allows the app to modify or delete the contents of an SD card (68% of apps)
- 'Read phone status' - Allows the app to access the internal features of the device such as phone number and device IDs (33% of apps)
- 'Read SD Card' - Allows the app to read the contents of an SD card (31% of apps)
- 'Precise Location' - Allows the app to get a precise location using GPS or network location sources (31% of apps)
- 'Find Accounts' - Allows the app to get the list of accounts known by the phone (27% of apps)
- 'Take pictures and video' - Allows the app to use the camera at any time (21% of apps)
- 'Read Contacts' - Allows the app to read data about contacts stored on a device (13% of apps)
- 'Record Audio' - Allows the app to record audio with the microphone at any time (11% of apps)

Less common but higher-risk Android permissions include:

- 'Call Phone' - Allows the app to call phone numbers without intervention (9% of apps)
- 'Receive SMS' - Allows the app to receive and monitor or delete messages sent to a device without showing them to the user (5% of apps)
- 'Read SMS' - Allows the app to read SMS messages stored on a device or SIM (5%)
- 'Write Contacts' - Allows the app to modify data about contacts stored on a device (5% of apps)
- 'Send SMS' - Allows the app to send SMS messages, which may result in unexpected charges (4%)
- 'Read Calendar' - Allows the app to read all calendar events stored on a device (4%)

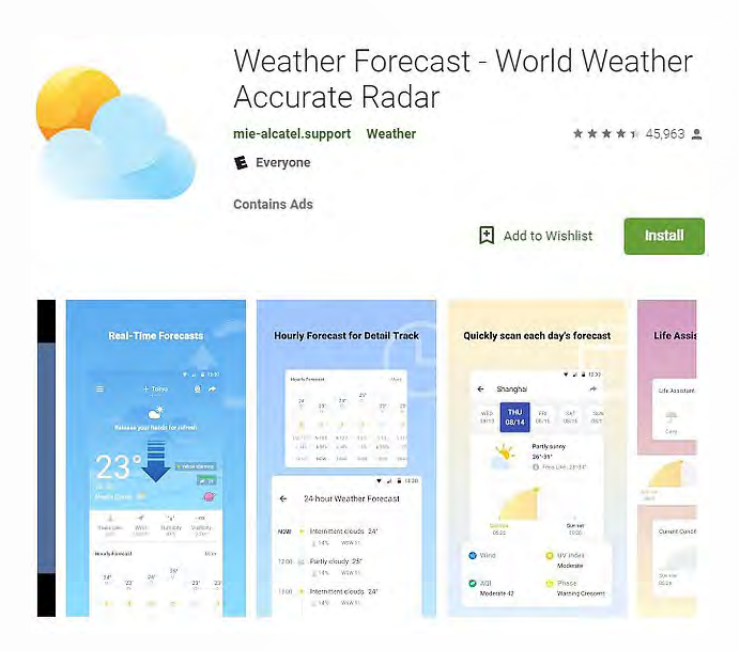
Most iOS apps request 5 or fewer permissions

When we look at iOS apps, the story isn't too different. Some categories of apps are worse than others. For example, more than 60% of social networking apps request the "Location When In Use" permission, which, depending what a user is doing, can be a necessary part of an app's functionality. Users are placing a high amount of trust in social networks to safely handle and not exploit their data, as in the widely publicized Cambridge Analytica scandal.

Social media and weather apps request the most permissions on iOS, followed by shopping and health/fitness

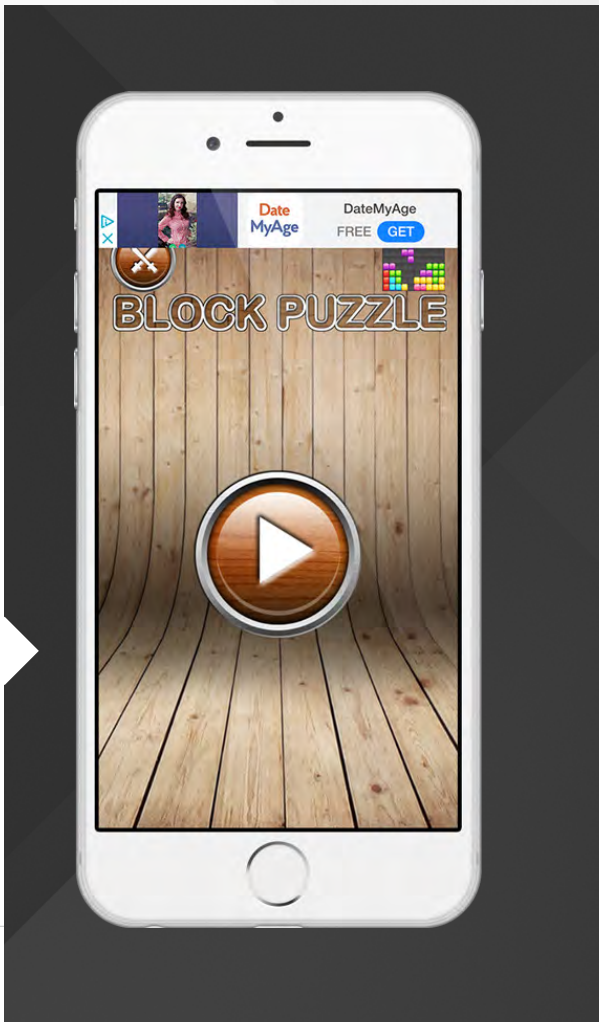
Some apps collect data without explicitly asking for permission. Others completely neglect a user's preferences. Wandera Threat Research Labs helped the Wall Street Journal investigate a popular weather app (10 million downloads on Google Play) that was asking for unusual amounts of user data. 'Weather Forecast - World Weather Accurate Radar' was found to be siphoning off detailed data from users, including geographic location information, email addresses and device unique identifier numbers without any explicit permission from users. Our investigation showed that the app even prompted users to opt out of sharing information but didn't change any behavior in the back-end - meaning the privacy prompt was essentially a gimmick.

Weather Forecast



There is also a gray area between malware and legitimate applications. Just because an app isn't malware doesn't mean it's not using some underhand techniques to put data in the wrong hands.

Wandera discovered 14 retro game apps on the App Store that were communicating with a C&C server known to host Golduck malware. While the C&C server wasn't exfiltrating data or commanding the app to do anything other than display ads to the other apps in the group of 14, this communication represents a backdoor - essentially, the app presents a point of entry for a hacker to alter the server commands to display a link to something more dangerous, such as a malware download.



Not just threats, but risks

The previous section summarized the key threats apparent within the current mobile security landscape. However, for an organization to fully protect its employees' mobile devices, it is crucial to understand the vulnerabilities that place corporate data at risk in address the problem before attackers have a chance to exploit it.

Understanding the risk exposure across mobile devices used in the enterprise is a good way to get mobile data under control before bad guys get to it. Knowing vulnerabilities which are built into the device, or how many of an organization's devices are running an out-of-date operating system, is good practice in any assessments.

Lock screen configuration

It is one of the most simple and important security measures, but surprisingly, many people still don't use a lockscreen on their mobile devices. If a phone is lost, stolen, or left unattended, someone else could easily read messages or emails, access sensitive apps, social media, and other personal data. Creating a password-protected lock screen configuration would mitigate this risk. Those that do have lock screens in place, sometimes opt for a minimal four digit passcode, unfortunately convenience is often the overarching driver.

43% of companies have at least one mobile device with no lock screen

Out-of-date operating system

The WannaCry ransomware attack, first reported in May 2017, brought to light the threat posed by outdated operating systems active on corporate networks. While this attack threatened on vulnerable Windows computers, the threat remains very real for other mobile operating systems. Manufacturers release frequent updates for their OSs that contain not only performance improvements, but important security patches for vulnerabilities that may have an active exploit.

65% of organizations have at least one device with an out-of-date operating system

Wandera data shows that 57% of Android devices are running an OS at least two full versions behind the current one. By mapping the known vulnerabilities of these older versions (recorded in the CVE database) it can be concluded that there are an average of 451 known vulnerabilities per device with nearly two thirds of these rated "critical" or "high" on the CVSS scale.

While IT departments have struggled to get a handle on managing mobility, the percentage of out of date operating systems has been trending down. Within the Wandera network, we've seen a 60% decrease in out of date operating systems between February 2018 and January 2019. Wandera informs admins of out of date devices, what risks 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 implemented by device manufacturers and organizations.

Jailbreaking, rooting and sideloading

The term 'jailbreaking' can apply to any kind of mobile device, but generally refers to Apple devices. Apple maintains a high level of device security by restricting all devices to only allow apps downloaded from the official App Store. Apart from restricting which apps are installed on iOS, Apple restricts the access each individual app has to the overall device. Some of these restrictions are overcome with jailbreaking. Jailbreaking is a method of circumventing this restriction by increasing user permissions on the device. Users can still access all the normal functions of the device, but are able to install applications from sources other than the official App Store.

Google does not lock down the Android OS as much as Apple does on iOS – while the default configuration does not allow 'sideloaded' apps downloaded and installed from unofficial sources, it is possible to change settings to allow apps from third-party sources. Our research shows that around 20% of devices have this setting enabled. This method is easier or more convenient than jailbreaking, but opens up the device to threats in the exact same way.

Recently, leading video game creator Epic came under fire from the security community for offering the Android version of its incredibly popular game Fortnite (~200 million players) via its website instead of through the Google Play Store. This meant the huge number of Fortnite players had to have these risky settings enabled in order to install the game on an Android device.

10% of mobile devices in the enterprise run gaming apps each day

1 in 5 Android users have their devices configured to allow third-party app installs

Rooting is often confused as the Android version of jailbreaking. While rooting is similar to jailbreaking in the sense that they are both privilege escalation methods, rooting provides a great deal more control to Android users than Apple users gain through jailbreaking. So-called because the technique provides root access to the device, rooting allows much greater, superuser privileges, so users can make drastic changes – up to and including changing the device's operating system.

6% of organizations have at least one jailbroken or rooted device

These risky configurations allow the installation of unauthorized software functions and applications, and are also popular with users trying to free their device from a carrier lock.

While some users may jailbreak or root their mobile devices purposefully to install security enhancements, others may simply be looking for an easier way to customize the look of their OS or install applications that aren't available on the official app stores.

Sideloaded apps refer to application packages downloaded from websites or apps installed from third-party app stores. Users that sideload apps face increased security risks because the application vetting process enforced by Apple and Google on their official app stores is bypassed, and thus the device has less protection against inadvertently installed malware.

35% of organizations have at least one device with one or more sideloaded apps installed

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

7% of iOS and 3.0% of Android devices are connecting to third-party app stores

It is important to remember that our data is representative of mobile devices being used for work purposes. In most cases, use of UEM has been mandated by the organization, although not necessarily if the device is BYOD. Additionally, meaningful platform and OS updates over the past several years have provided users with less reason to tamper with the core functionality of the device. Users are more educated about the dangers of jailbreaking, rooting and sideloading than they were a decade ago.

Data leaks

Data leaks certainly don't get as much attention as threats like malware and phishing but a leaking app is one of the most common mobile security risks users will face. Data leaks are the unauthorized or unintentional transfer of sensitive information from an enterprise mobile device over the internet. By failing to encrypt the data, the app developer is essentially making the data much more readily available to anyone who utilizes the same network as the device with the vulnerable app - usually via a man-in-the-middle attack.

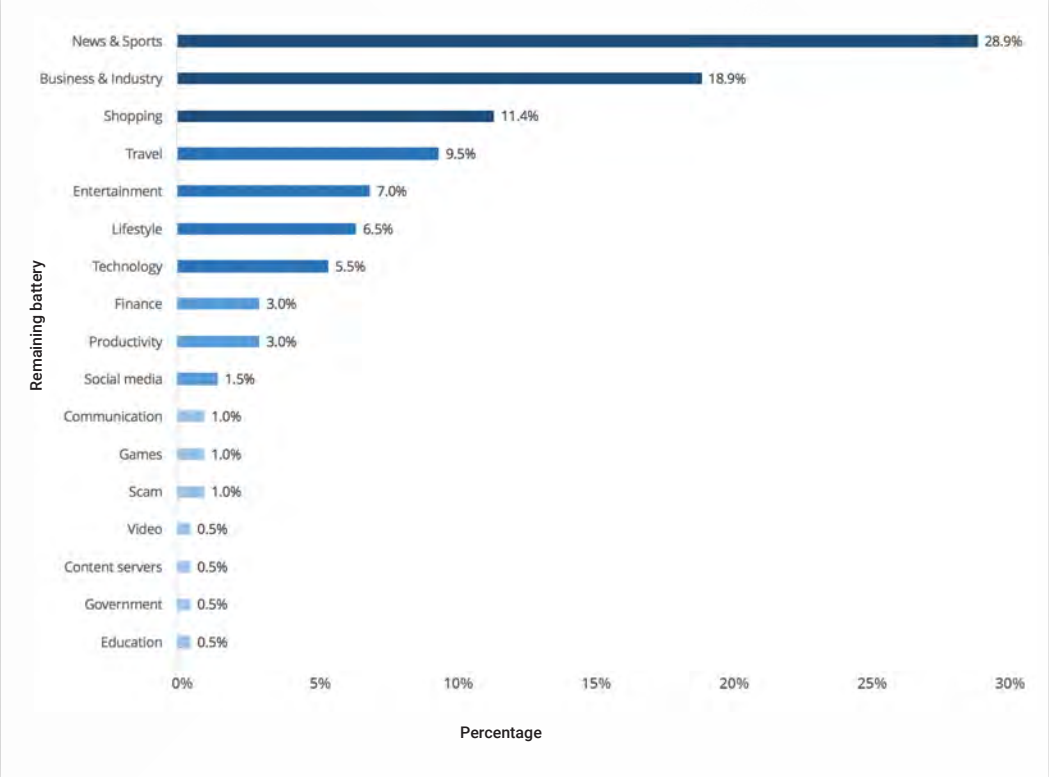
77% of users had some form of PII leak in 2018

Why are they so prevalent? Often app developers don't take into account regulatory compliance and security policies when building apps and instead focus on user experience.

Our research shows the Personally Identifiable Information (PII) most frequently leaked is username and password with credit card numbers/details being leaked the least frequently. Wandera considers PII to be any unique identifier for the user or the device, so this data leak analysis accounts for data such as location and device IP address. Clearly the more perceived sensitivity the data has, the more security measures are put in place by developers. Online transactions that transfer credit card data are typically more rigorously protected than other types of data. This is largely driven by the threat of fines for regulatory non-compliance and the specter of legal liability for identified leaks.

90% of mobile data leaks expose a username, 85% expose a password and only 2.3% expose credit card details

Not all data leaks are equal. While none are desirable, those that expose financial information could be considered more sensitive than those that leak email addresses. However, all PII leaks are extremely dangerous, and all forms of exposed data may be used as the building blocks for further, more damaging attacks. With usernames and passwords leaked so frequently, and over 90% of people reusing login credentials for multiple accounts, hackers can easily break into corporate accounts. They can do this by capturing a user's credentials with a MitM attack and then 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 data breach in exactly this manner.



A significant number of leaks were identified in travel websites, accounting for almost 10% of all the leaks discovered. Mobile travel applications are frequently used at work, as employees spend an increasing amount of time overseas and in transit for business. Leaks in journey planning, seat reservation and ticket booking features for services including train operators and airlines were among those discovered by Wandera. Entertainment, lifestyle and technology services - each mostly used for recreational purposes represent 19% of leaks between them.

Productivity tools are critical to the mobility programs of most enterprises and without platforms like Microsoft's Office or Evernote, there might be far less need for smartphone-enabled workforces in the first place. Around 3% of the identified data leaks were in this category. This is troubling news for security-conscious mobility leaders especially since productivity apps often need access to device components or data to function.

Beyond unstable operating systems and leaking apps, AI-driven features are being exploited. As more complex features are released, the harder it becomes to troubleshoot and assess for vulnerabilities. Wandera testing led to the discovery that the suggested contacts feature on iOS could be manipulated by hackers to trick a victim into thinking someone they know is calling - like their bank, accountant or CEO, for example.

Protecting mobile devices used in the enterprise

As we've seen throughout this report, mobile is undoubtedly the new frontier for cyber threats. In 2018, Wandera observed a threat growth of 59% YoY, and blocked 57 million mobile threats for its enterprise customers. Businesses must be able to do more than simply detect an attack - remediation actions must also be available.

There are a number of steps you can take to protect your employees' mobile devices from the wide range of threats and risks mentioned so far; however, there are several challenges that stand in the way. For example, educating your workforce - there may be reluctance to install security on mobile devices if it's not understood how much of a risk unsecured devices could be. Another challenge is ensuring your employees' privacy - they are even less likely to want the protection on their devices if they believe their privacy is compromised - especially if your company employs a BYOD policy.

Buy-in across the company is an important part of creating a fully secure environment. Even the most informed users can occasionally slip up - malware can hide in legitimate-looking applications, or tests have shown that a particularly convincing phishing link can catch a distracted user. A safety net across the entire organization is needed to ensure that your company's attack surface is mitigated.

It is imperative to have protection on both the device and network level, so that data is secure, and any threat can be identified and eradicated.

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

wandera.com/demo

wandera

Wandera is a leading mobile security company, providing multi-level protection against cyber threats for users, endpoints, and corporate applications. Security teams worldwide rely on Wandera to eliminate threats, control unwanted access, prevent data loss and enhance user privacy. The company pioneered the application of data science to tackle the complex challenges of mobile security with MI:RIAM, the industry's most effective threat intelligence. Recognized by analysts and trusted by thousands of enterprise customers, Wandera was founded in 2012 and is headquartered in San Francisco and London. To learn more visit www.wandera.com, or follow on LinkedIn and Twitter.