wandera

Mobile Leak Report 2017

The "Panama Papers" of mobile leaks

A global analysis of almost four billion requests across hundreds of thousands of devices uncovers the new threats to enterprise mobile data

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In April 2016, 11.5 million sensitive documents were leaked in what became known as the Panama Papers scandal. These documents exposed an alarming array of sensitive data, revealing a number of controversial and confidential pieces of information in 2016.

This report, while not as far-reaching in scope, explores a similar theme. Researchers at Wandera have uncovered more than 200 well-known and reputable digital services that have exposed sensitive consumer and enterprise information. Mobile is well and truly the new frontier for data security, as this analysis reveals.

INTRODUCTION

Most CIOs are not so naive as to think that work-assigned smartphones are used exclusively for professional purposes. However, as is often the case, the extent to which these devices are used for recreational activities may startle a significant number of mobility leaders. The reality is that content such as video, news, entertainment and social media is among the most popular uses of corporate devices.

Despite the differences between perception and reality, where and how data allowances are being consumed is not the principle focus of this report. The emphasis is instead on where mobile data security risks are coming from, and why. Understanding this in the context of how heavily these services are used is critical to comprehending the extent of data leak threats in 2017.

This report will show that for certain categories of apps and websites, security and compliance risks are actually far more formidable threats than previously thought.

The key message is not that enterprises should be planning their 2017 mobile security strategy by limiting access to wholesale categories of domains or apps. This is impractical and would undermine the entire essence of enterprise mobility and potentially cause dissatisfaction in the workforce. Instead, this report highlights how varied threat vectors are and how many categories of apps and sites are affected – in fact, almost all of them.

The most practical response for executive teams is to routinely monitor the data that flows to and from each individual device, identify potential security gaps and dynamically respond through policy actions that help to manage the risk while simultaneously ensuring that employees stay productive.

"The more that employees and contractors use mobile devices to access organizational systems, applications and data, the more important it is to protect such access. Furthermore, it's essential to prevent the mobile devices that are supposed to boost productivity and add to the bottom line from opening unauthorized means of access to information and other assets; this turns them into a danger and a possible drain on revenue instead."

ED TITTEL, INTERNET CONSULTANT AND FORMER DIRECTOR OF TECHNICAL MARKETING AT NOVELL

DATA OVERVIEW

For a period of three months in 2016, Wandera's cloud gateway sampled 3.9Bn requests from mobile devices that were enrolled on its service and facilitated transactions with 2.9M unique Internet sites. These transactions included both traditional requests that came through the mobile browser as well as requests that originate in a native app on the mobile device.

During this time, Wandera detected data leaks containing Personally Identifiable Information (PII) from more than 200 mobile websites and apps as it monitored the corporate-liable devices for over 500 enterprise businesses around the world, who collectively have over two million devices under management.

These leaks were spotted on devices located in more than 20 countries, coming from mobile apps, websites and mobile-specific websites. The data put at risk varied in type, ranging from passwords and usernames, right through to entire credit card details, dates of birth, addresses, home phone numbers and passport numbers.

THE DATA

Defining a leak

For the purposes of this document, a data leak involves the unauthorized or unintentional transfer of sensitive information from an enterprise mobile device to an Internet service.

By not protecting the data, the app developer is essentially making the data available to anyone who utilizes the same network as the device with the vulnerable app.

By not using a secure network transport protocol (such as HTTPS), the developers simply sent the data over the network in a format that anyone with a simple network sniffer could capture.

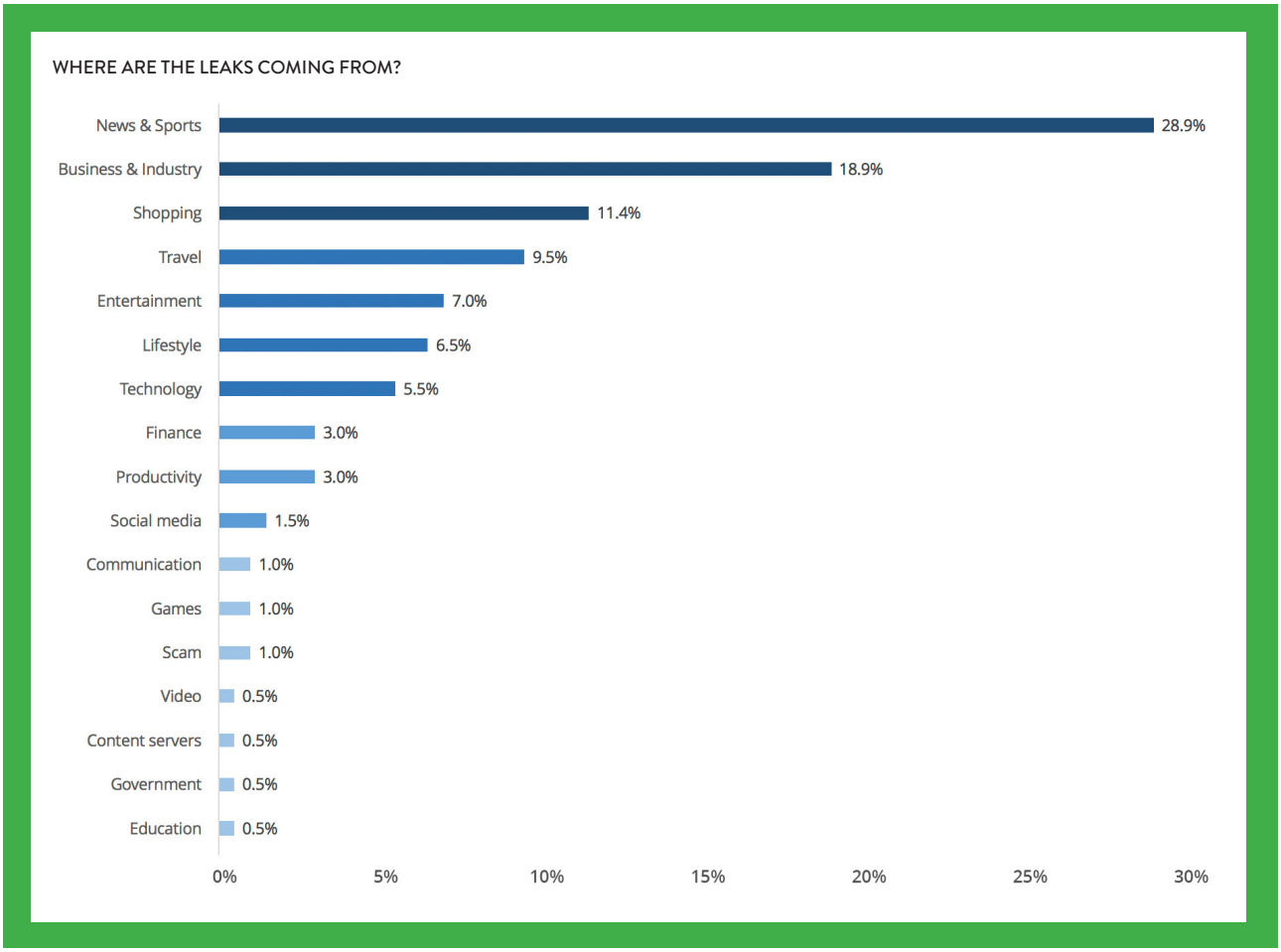
Detecting the leaks

A mobile device with a "leaky" app exposes sensitive data when an app developer or web programmer fails to use HTTPS to securely communicate over the network.

Wandera's service operates in the path of the data and inspects all outbound requests (from the device and inbound responses from the Internet) for risk. Sometimes those risks include malicious apps or phishing attacks. The risks identified in this report focus on the sensitive content that the apps and websites failed to protect adequately.

THE FINDINGS

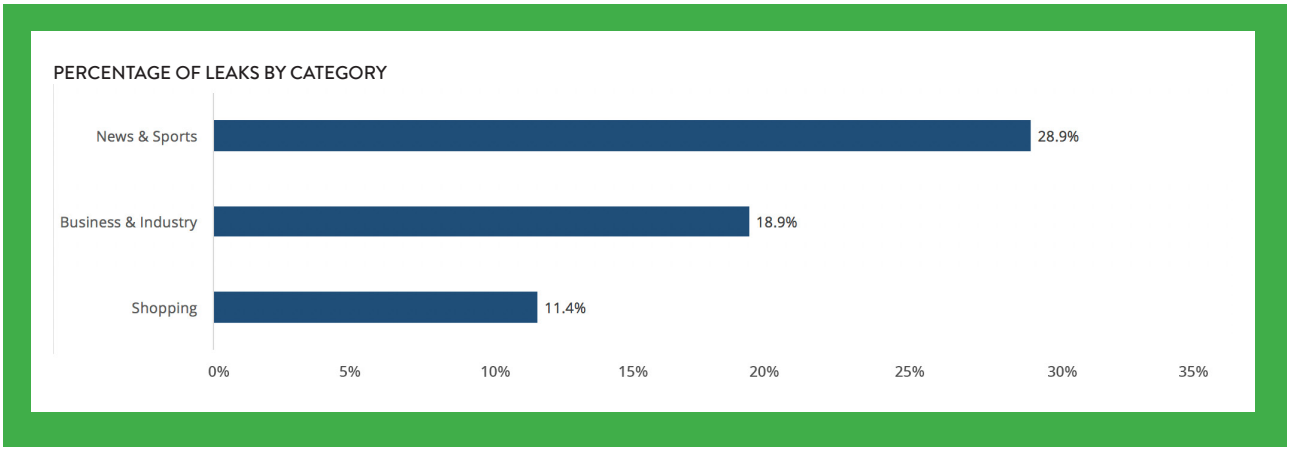
Analysis of the 200+ leaking services uncovers a wealth of insight about the type and origin of data leaks. Categorizing the content by its type reveals that more leaks were present in certain segments than others.



More than 59% of all the leaks identified were from just three categories: news & sports, business & industry and shopping. A further 28% were from another four: travel, entertainment, lifestyle and technology.

Volume of leaks: high risk categories

Alarmingly, news and sports websites were the most commonly featured category among those leaks identified. Perhaps even more worryingly, business and industry services accounted for almost 19% of every leak discovered.



News and sports websites, which include some of the best-funded and well-staffed organizations in the world, pose a far bigger risk than many CIOs may expect. The same is true of business and personal services, a category that comprises of company websites and other corporate entities.

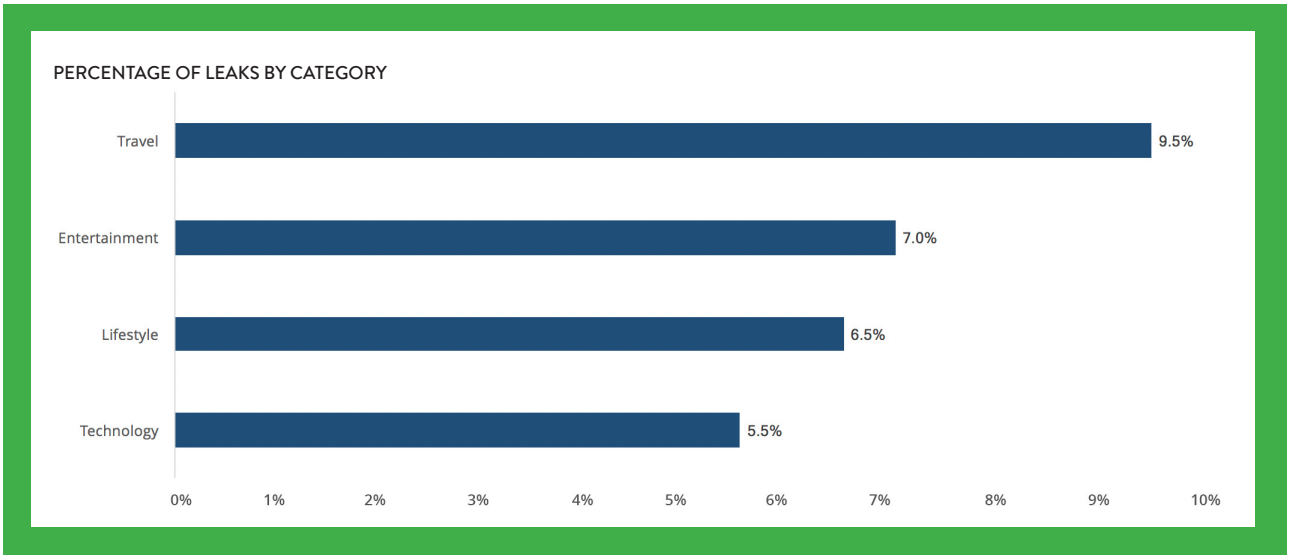
Shopping apps and sites typically require a great deal of personal information due to the nature of the content. In order to make purchases, users must hand over PII such as credit card information and their physical address. That such a high proportion of leaks have been discovered in these types of services should be an alarming signal for security leaders.

EXAMPLE:
FOX SPORTS AUSTRALIA

FOX Sports Australia was leaking users' full names, email addresses and passwords.

Volume of leaks: concerning categories

A significant number of leaks were identified in travel websites, accounting for almost 10% of all the leaks discovered. Entertainment, lifestyle and technology services - each mostly used for recreational purposes represent 19% between them.



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.

Lifestyle and entertainment categories span everything from Buzzfeed to Tinder and are unlikely to be used for work purposes, apart from in certain industries.

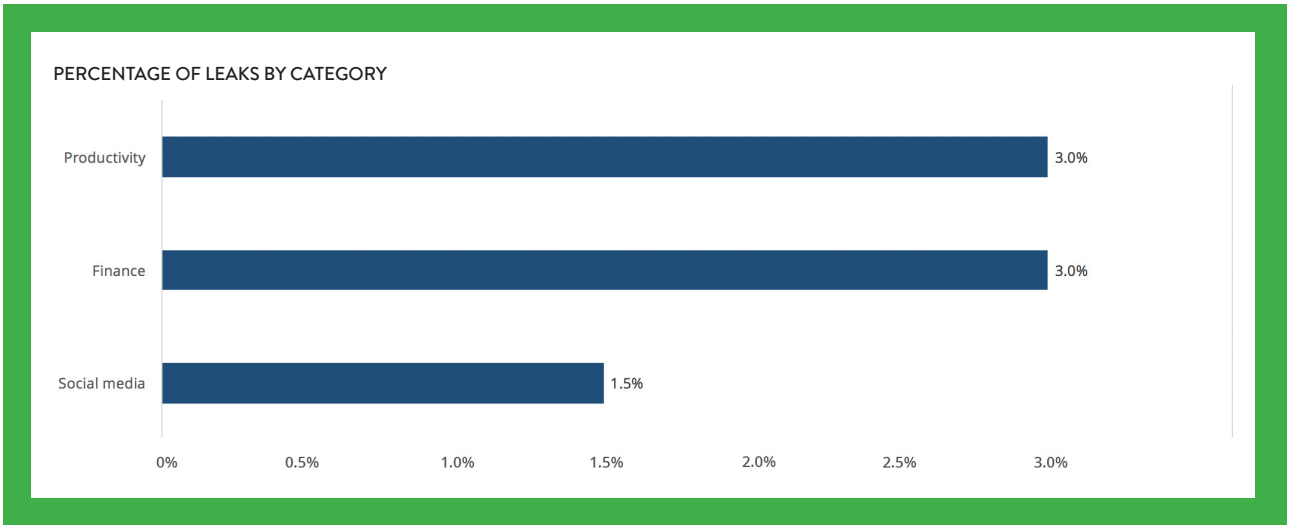
On the other hand, technology applications and websites are primarily used to meet professional needs, such as Google Analytics for web insights or Adobe's online services.

EXAMPLE:
THALYS

Thalys is an international high-speed train operator provided jointly by the Belgian, French, Dutch and German railways. Wandera identified unencrypted full names, passwords, addresses and phone numbers being variously transmitted 'in the clear' from Thalys' mobile website, iOS app and Android app.

Volume of leaks: surprising categories

Although the total volume of leaks spotted in the social media, finance and productivity categories was lower than elsewhere, that there were any at all will likely be of some surprise to many CIOs.



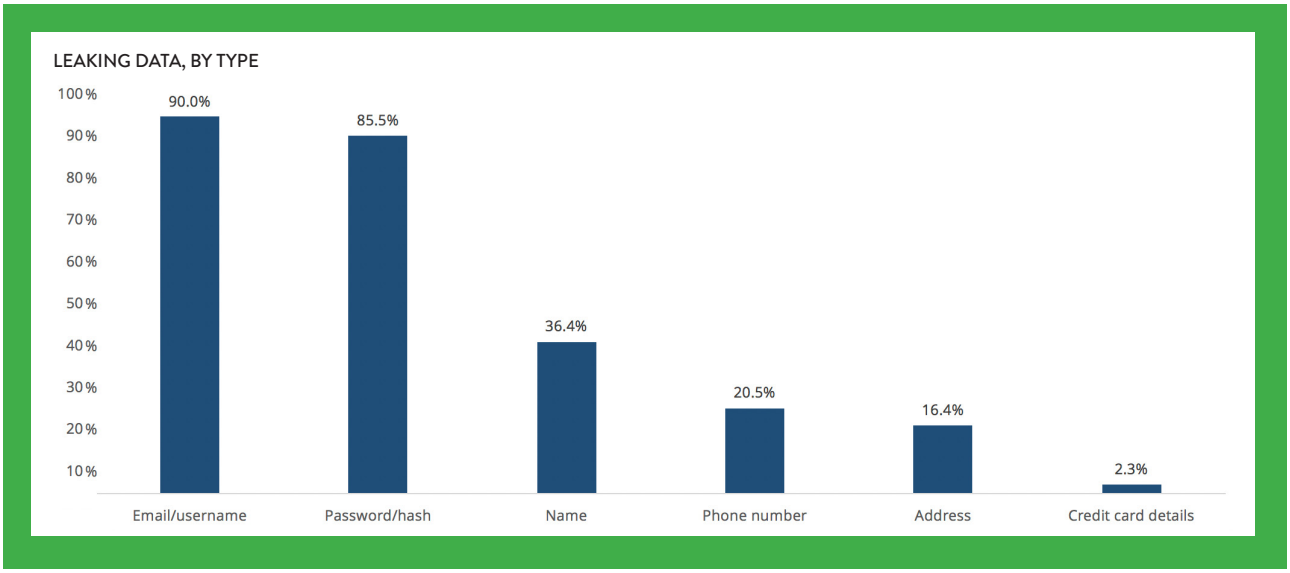
Productivity tools are critical to the mobility programs of most enterprises and without platforms like Microsoft's Office or Evernote, there might be far less need for smartphone-enabled workforces in the first place. Around 3% of the identified data leaks were in this category: troubling news for security-conscious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

Leaks in social media sites were rarer, but just 10 apps in this category - including Facebook, Twitter, Instagram and Pinterest - constitute the lion's share of this usage and many of them have already had their security scares and learned from them.

Stock-checking and banking services were similarly secure, but any leaks whatsoever in this category should be considered extremely risky due to the sensitive nature of the data involved.

WHAT GOT LEAKED?

Not all data leaks are equal. While of course none are desirable, those that expose financial information could be considered as more sensitive than the risk posed by leaking email addresses. However, all PII leaks are extremely dangerous, and all forms of exposed data may be used as part of a wider attack.



The pattern here is clear. The more perceived sensitivity the data has, the more security measures are put in place – hence credit card data being typically more rigorously protected. This is largely driven by the threat of fines for regulatory non-compliance and the spectre of legal liability for identified leads.

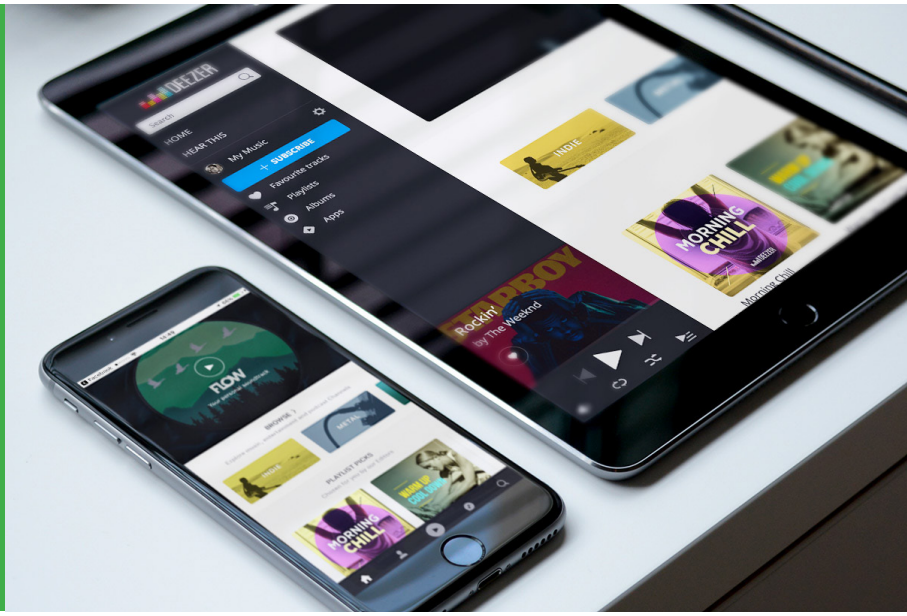
Despite all advice to the contrary, because of the overlap that this profile information inevitably has with multiple other services and systems, including log-ins to the enterprise network, these seemingly minor leaks can be catastrophic.

Indeed, for many attackers, this data leaked from apps and mobile websites on enterprise devices can be the 'keys to the kingdom'. In most cases, usernames and passwords are sufficient to provide full access to a user's online account. Even if the other bits of information did not leak, an attacker with access credentials could bypass any protections that are put in place and gain full access to the account.

What's even more alarming is the fact that the other personally identifiable information leaked as well. Research by Carnegie Mellon University revealed that 87% of all Americans could be uniquely identified using only three bits of information: ZIP code, birthdate and gender.

EXAMPLE:
DEEZER

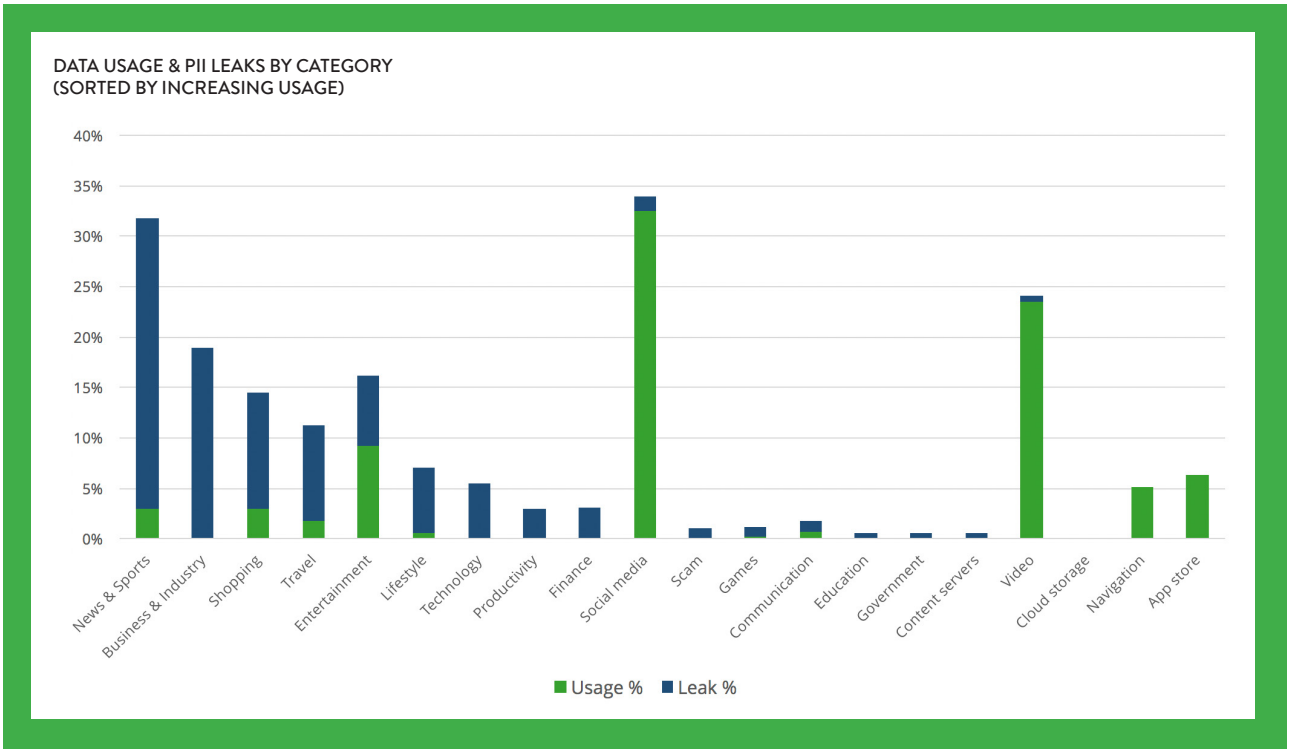
Deezer is an online music streaming service. Wandera discovered that both its app and mobile website were leaking name, password, date of birth and gender. Credit card details remained encrypted, making this appear to be potentially a good example of the 'keys to the kingdom' being neglected in favour of encrypting the more 'sensitive' data.



USAGE AND RISK

A gateway architecture enables admins to get visibility into the activity of smartphone users. This technology provides analysts with threat detection and insight on security events in real-time, including data leaks, but it also reveals the nature of data consumption on an individual, departmental, organizational or even global basis.

Analysis of this usage can be undertaken to highlight which content categories are used most heavily. By correlating this with the PII leak dataset, new patterns then emerge.



In this graph, the leaks were distributed again by content category, with the most frequently vulnerable types ordered from the left side of the X axis. The data is this time also populated by usage information, which displays how much mobile data is consumed for each category.

With the data visualized, a handful of problem areas immediately present themselves. News & sports, shopping, travel, entertainment and social media each featured frequently in terms of both the volume of leaks exposed and the volume of data that was spent on these categories.

USAGE AND RISK ANALYSIS

High usage, some risk of leaks

Video is a drain on data plans, with its demanding pull on mobile data to serve large video file sizes for streaming purposes. Leaks again were rare, with sites like YouTube, Netflix and the BBC iPlayer taking security extremely seriously. Furthermore, PII is not always required to use these services, meaning the chance for exposure is less common.

Social media is the single largest content type regarding data usage patterns. In fact, mobile data usage to and from social websites and apps is growing by double-digits - the last few months alone have shown over 20% growth in this category. Employees make frequent and sustained use of services like Twitter and Facebook, and they are putting more focus than most into delivering a secure product. They know that in a massively competitive market, they cannot afford not to.

In truth, it is not just competitive forces driving this security focus – it has its roots in geopolitics too. After the Arab Spring, Google and Facebook started to encrypt every search and every connection so that individuals could not be targeted by governments. Similarly, in the US and UK, the same providers maintain those protections after the Snowden leaks showed how much governments were eavesdropping on citizens.

While the above is positive, there are hidden warnings. At 1% of all the data leaks uncovered, social media security should be a significent concern for CISOs.

Consumers place a lot of faith in the security of social media, and it is this combined with the sheer popularity and usage volume of the networks that makes this a risk category that security leaders cannot afford to ignore.

Twitter, Facebook and LinkedIn have all suffered major data breaches over the past few years, with the latter having the PII of tens of millions of its users stolen. The nature of this form of breach means that CIOs should have a risk management strategy in place, including a system to react to a breach like this - such as an instant and temporary block across all corporate devices to the vulnerable service in the wake of a new breach.

Given their high profile and massive user communities, social media services face threats constantly. Breach risks are compounded by the fact that social media apps are updated frequently, meaning enterprise devices whose social media apps have not been updated can be at risk of breach.

Common usage, moderate risk of leaks

Cloud storage applications and websites follow a similarly cautious approach to social media firms in the knowledge that a single data breach could spell disaster for the entire business. As such, leaks in this category are extremely rare and none were discovered in the research period. The same is true of navigation apps, such as Google Maps and Foursquare. Both content types are very popular in how much data is used to access them, and generally secure from a leak perspective.

This serious approach to security cannot be said of entertainment services, which are even more popular in terms of how frequently they are used by employees on work devices.

Entertainment sites and apps are often built by an assortment of internal and external development resource, are constantly updated and operate in a “quick or dead” environment. Added to this is the pressure placed on them to deliver highly intuitive user interfaces, putting a premium on ease of use. In such circumstances, it is not unfortunately inevitable that security can be compromised in favour of speed and customer loyalty.

Some usage, high risk of leaks

There are a further three categories that should be of particular concern to CIOs and other security leaders. News & sports, shopping and travel services are used on a regular basis and are the origin of an alarming number of PII leaks.

Media sites and apps face stiff competition for eyeballs. This frantic, fast-moving environment means that focus is typically placed on rapid and expansive content production rather than security.

Indeed, this is a trend that is often seen elsewhere in the data, such as travel – the more dynamic and competitive the sector, the less attention is paid to securing the user's data, and therefore the greater the risk to the enterprise.

News and sport is the seventh highest category for data consumption, putting it in the top third, but also accounts for the highest proportion of leaks. It seems to be the nightmare combination for CIOs and CISOs – high volume of expensive data consumption, plus high likelihood of personal data being leaked.

As is the case with media services, there can be no surprise that traffic to and from corporately-liable devices is often on shopping and travel sites. However, it should be surprisingly – galling, even – that such a high proportion of leaks occur through these properties.

In theory, these sites should be amongst the most robust of categories given they constantly handle PII and credit card information. And in fact, this is largely the point – the payment information is handled responsibly, but the PII is not.

For many online retailers, time-to-market is the primary concern. In their haste, ecommerce websites are stitched together from multiple third party components. An open source shopping cart will be attached to a freely available hosting package and a content management system, and so on, and then finally it is all attached to a payment gateway.

The latter typically secure in its handling of credit card information between the retailer, credit providers and banks, but many of the leaks seen in the retail sector are in fact 'service to service'. In other words, PII data is leaking through the various services that hold the platforms together.

This is particularly prevalent in the shopping category because of its inherently competitive nature and the number of new players joining the market quickly, without giving due care and attention to data security in the process.

EXAMPLE:
AMC CINEMA HONG KONG

This retail website was shown to be leaking customers' names, emails, date of birth, user names. passwords and credit card details.

USAGE AND RISK: OTHER NOTEWORTHY FINDINGS

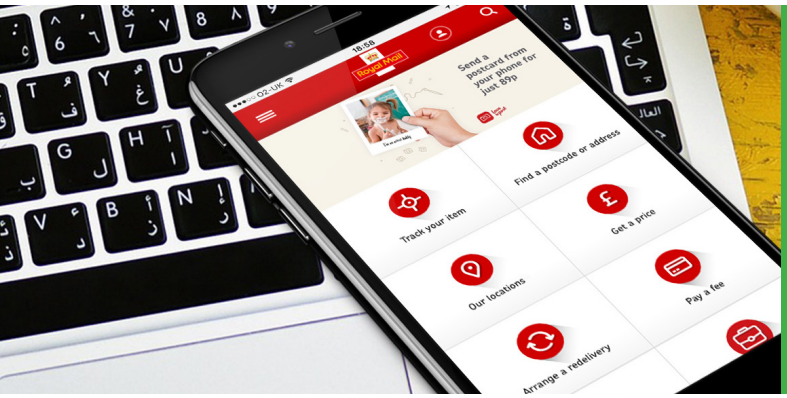
Many enterprises use third party applications and tools for a variety of internal and external tasks and functions. These range from collaboration and communication all the way through to industry- or department-specific requirements, such as online HR and finance services or online databases and information services.

These will almost always require log-in details, which concerningly will often be identical to those used to access other far more sensitive information.

One example of this was identified recently by Wandera's research team. A leak was discovered in the website and application of a meeting room software provider. On the face of it, the dangers were limited – attackers could only use the leaked usernames and passwords to log into the website, find available rooms and book them unnecessarily. However, this particular software tool was often deployed integrated with the security system of the entire business. Now, using the meeting tool, an attacker could not only reserve the room, but also have visitor credentials printed, thus allowing the attacker to gain physical access to the enterprise.

Imagine an attacker being able to walk into your business, sit in a conference room unchallenged, and use a networking jack in the wall which would grant him or her direct access to the corporate network.

This sort of integrated deployment of external software products is commonplace. Expenses tools tied to core finance systems; HR self-service portals tied to whole personnel databases; communication and presence apps tied to wider Unified Communications and even core networks. The warning of an enterprise's security only being as strong as the weakest link has never been more applicable.



EXAMPLE:
ROYAL MAIL

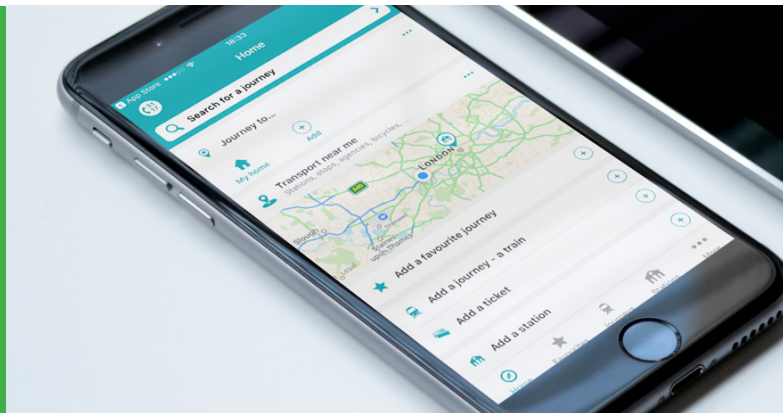
The Royal Mail's website was spotted transmitting customers' full names, passwords, addresses and landline and mobile numbers unencrypted. As above, these details can allow access to far wider services if captured by unlawful actors.

Another area worthy of further analysis can be found in the education and public sector categories. As is to be expected of analysis of thousands of corporately-liable devices, the traffic to and from education and government sites is comparatively very low. And yet, the volume of data leaks is disproportionately high.

The root cause of this is, sadly, budgets. The public sector is on the whole unable to invest sufficiently in technology, and particularly data security, in the way that the private sector can. While security scandals can destroy careers in public and private sector alike, the lack of competitive forces in the public sector means that there is no threat of the destruction of brand trust. This lack of fear means the security of "non-sensitive" public sector digital assets simply is not as high on the agenda, so sufficient budgets are not dedicated to it. Security leaders should be quick to scrutinize services hosted by public bodies and ensure that the selection of apps employed by the corporation are not exposed to unnecessary risk.

EXAMPLE:
SOCIÉTÉ NATIONALE DES CHEMINS DE FER FRANÇAIS

SNCF is the French state-owned railway company. Its website, mobile website, iOS app and Android app were all variously detected as having leaked usernames, full names and passwords.



ADDITIONAL RESEARCH: HIGH-RISK CATEGORIES

The 200+ data leaks in 2016 included in this report stem from categories that most CISOs would consider to be safe from threat. The findings of this research should, by now, have convinced readers of the significant risks that even seemingly secure services pose to the enterprise.

There are also other more obvious candidates for data leaks. While most Wandera customers opt to filter content from gambling, scam, adult and ad networks, not all organizations have these kinds of systems in place. These categories are by far the biggest risks for businesses, with adult sites exposing PII on a regular basis.

Adult content

Pornography and other adult content categories are notorious for lax handling of PII. The personal data of more than 800,000 users of the adult site Brazzers was exposed in September 2016, followed by a successful attack on 400 million accounts on the AdultFriendFinder network in November. A year previously, the controversial extra-marital dating app Ashley Madison was hacked, revealing the PII of every single user in its database.

Analysis of the top 50 adult sites revealed that a staggering 80% of these services were leaking some form of PII.

Rank	Website	Rank	Website	Rank	Website
1		21		41	
2		22		42	
3		23		43	
4		24		44	
5		25		45	
6		26		46	
7		27		47	
8		28		48	
9		29		49	
10		30		50	
11		31			
12		32			
13		33			
14		34			
15		35			
16		36			
17		37			
18		38			
19		39			
20		40			

40 OUT OF THE TOP **50** ADULT SITES ARE EXPOSED

Scam sites

There can be no surprise that scam websites lack rigour in their data security. Provided their websites are appealing visually, sufficiently functional to process payments and can be set up quickly, there is no need for security. Indeed, the particularly nefarious site owners may make this a deliberate omission.

Earlier in 2016, Wandera identified several websites selling fake sunglasses purporting to be from major brands. These were often recently set up websites and attractively designed, but were sending all personal payment information unencrypted. Many of these sites would be swiftly shut down through trademark disputes, but would reappear just as rapidly under new URLs and company details. These services were accessed on thousands of corporate devices, underlining the threat that even these seemingly niche sites represent. With each enterprise only as secure at its weakest point, CIOs should consider adopting technology that restricts access to suspicious sites and apps, preventing one of the most obvious forms of data leaks.

Advertising networks

While not listed as an independent category in the analysis, the Wandera data team has noticed a worrying trend amongst apps that allow advertising networks to access them and display content. This potentially affects any apps and mobile websites that partner with ad networks, most typically, gaming, retail and social.

Cyber criminals are increasingly launching sophisticated ad fraud campaigns to distribute exploits by turning the ad networks into incredibly efficient malware delivery vehicles. By incorporating malware into the ad networks that are used by thousands of legitimate websites, hackers can target a broad set of users without actually breaking into the distributing of publisher's sites directly. Suddenly, even the app with the most robust of security policies and procedures is potentially being put at risk.

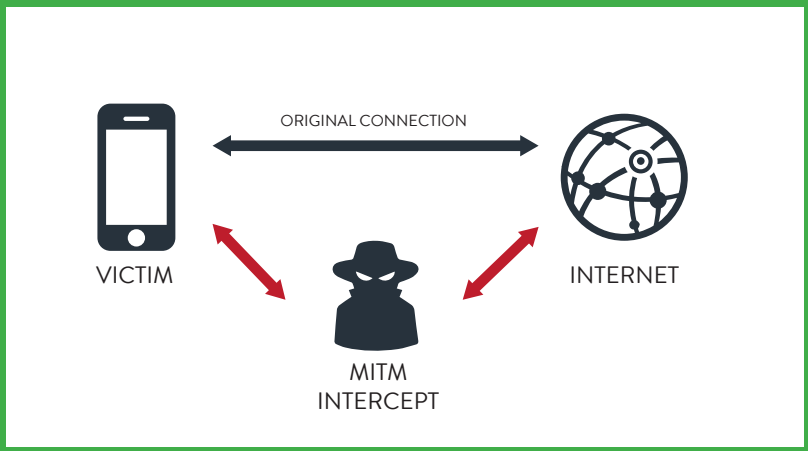
WHAT IS THE REAL THREAT TO THE ENTERPRISE?

The common perception of a threat – for enterprise CIOs, CISOs and consumers alike – is often based on an active attacker and a compromised device. However, in this report we have focused on leaks that are caused not because of an imprudent or careless attitude to cybersecurity by the enterprise, but instead because of the employees' legitimate use of an unsecure third party website or app.

The enterprise's data is therefore compromised through innocent usage rather than by any malicious behaviour. By implementing a Security Development Lifecycle and either forcing it on employees or demanding that contractors follow the same practice, enterprise customers can ensure that their own apps and websites are treating sensitive information with the protection it requires.

However, they cannot do anything directly about the third-party apps that their users utilize, and so must strengthen their own security processes to stay secure from the threats that these apps might expose them to - such as the adoption of a content filtering platform that operates at the data level.

As was shown at the opening of this paper, the nature of the data being leaked, while not always necessarily powerful on its own, can often amount to the keys to the kingdom.



But how great is the danger of the data being "leaked"? What is the practical risk?

In short, one such danger is a 'Man in the Middle' (MitM) attack.

This involves a malicious actor inserting themselves into a cyber-conversation between two parties, such as a device and the web server it's trying to communicate with. This may be via joining the same Wi-Fi network, or being nearby when the victim is using data. Research from Kaspersky suggests more than a quarter (28%) of public Wi-Fi hotspots are dangerously unencrypted.

If unencrypted, or "in the clear", the attacker can intercept the information being transmitted and exploit the data within the online communication. With just a little work, the hacker can also identify a person's location, gain access to personal messages and access stored information within the device. The potential threat to the enterprise device is suddenly very clear.

Of course, just because this information was leaked "in the clear" does not imply that an attacker was on the same network capturing that communication session. But what makes data leaks so difficult to quantify is the fact that they happen outside the device. Because mobile devices communicate over the network wirelessly, there is no way to know if an attacker was capturing that communication for nefarious purposes.

Without better understanding of what damage could be caused by having vulnerable apps on the device or from employees accessing unsecured mobile websites, enterprises are putting themselves in a very vulnerable position when their employees are working remotely. Within the enterprise, some individuals are more vulnerable to attacks than others. This includes those who hold senior and executive positions that may handle more sensitive information within their emails and on their devices, as well as those in finance, in HR departments, in R&D teams or in product development.

In truth, an argument can be made for any employee with remote network access via their mobile to be a prized target, making universal real-time scanning of data streams essential in protecting the enterprise.

THE COST OF A DATA BREACH

According to research from Ponemon, the average total cost of a traditional breach is more than $7m.

Most data breaches continue to be caused by criminal and malicious attacks. These breaches also take the most time to detect and contain the threat and have the highest cost per record.

This $7m figure is calculated from a number of different costs, the primary of which are listed below.

LOSS OF REVENUES

Put simply, a breached company's existing customers will choose to take their business elsewhere, amid fear that their data could be vulnerable. The same is true of prospective customers that will be put off buying its products.

REMEDIATION

Breaches typically take more than six weeks to resolve, and cost more than $20k per day - placing the total cost at around $1m per breach.

FINES

Depending on the areas of jurisdiction, companies could be slapped with large fines for failing to protect personal data. From 2018, once GDPR comes into effect, the cost of a fine could run into the billions.

DISRUPTION TO OPERATIONS

Dealing with a breach can be extremely disruptive to programs internally requiring resources to be pulled from other projects to handle remediation. This can be especially costly during key business periods.

LEGAL FEES

There might be a host of legal considerations to process in the wake of a breach, and legal costs are among the quickest to spiral in such events.

STOLEN ACCOUNTS

Depending on the nature of the attack, company accounts may be compromised as a result - potentially leading to a direct loss of funds.

UPDATING STAKEHOLDERS

For many breaches, a detailed communication plan will need to be drafted and executed. This means crisis teams and extensive communications to keep stakeholders and the media in the loop and on-message.

RECALLS

The affected app or product line may need to be recalled, or at the very least updated. This can be an expensive and lengthy exercise.

STAYING SECURE

As this report shows, data leaks are a credible and widespread threat that have increased in both frequency and severity since the advent of corporate mobility.

Wandera has been designed to monitor all of the data passing through corporate devices, analyzing suspicious activity and detecting threats in real-time. Not only does Wandera give admins complete visibility into the usage of these devices, but also equips them with the tools to control that usage and respond to security events as they are identified.

To find out more about how Wandera keeps more than 500 global enterprises safe from threats, including data leaks, get in touch with one of our experts and request a demonstration of the platform.

To find out how Wandera will reduce your organisation's exposure to security risks, request a free demo of the platform.

wandera.com/demo

wandera

Wandera's pioneering web gateway for mobile provides organizations with **enterprise mobile security** and **data usage management.**

The security solution encompasses mobile threat defense and content filtering to prevent targeted mobile attacks, identify data leaks, and filter access to risky or unapproved usage. Wandera also offers mobile expense management and policy enforcement, helping businesses reduce data usage, lower costs and improve productivity, delivering a measurable ROI.