wandera

JULY 2017

Mobile data report: Focus on phishing

Mobile is rapidly becoming the most fertile landscape for the modern hacker to operate in. Every single hour a new, dangerous threat seems to emerge from mobile. That might be the latest man-in-the-middle exploit or a sophisticated variation of an Android ransomware file.

Our monthly Mobile Data Report is the world's first report purely focused on enterprise mobility data. It provides a complete analysis of mobile data security and usage trends along with traffic patterns across our global network of enterprise mobile devices. These are corporate liable devices (mostly corporate owned and BYOD) used domestically and whilst roaming.

TABLE OF CONTENTS

Introduction

Mobile is rapidly becoming the most fertile landscape for the modern hacker. Every single hour a new, dangerous threat seems to emerge. That might be the latest man-in-the-middle exploit or a sophisticated variation of an Android ransomware file.

One of the most overlooked and least glamorous threats is phishing. In the minds of many, phishing attacks feature phony members of the Nigerian royal family clumsily requesting the bank details of the victim in exchange for a supposed sum of money.

Phishing is not only far more prevalent than you might think, but it has become the cornerstone of almost every major attack over the past five years. It's demonstrably among the most potent and widespread forms of cyberattacks in the modern age, and mobile has offered a powerful new access and distribution network for hackers to exploit.

This report details the extent of this resurgent threat on mobile, and presents data on both how and where it is happening, with recommendations for reducing your organization's exposure to this risk.

MOBILE DATA REPORT

This paper also includes the monthly results from our regular Mobile Data Report series, looking at security and usage trends, and uncovering insights from across enterprise mobility.

To see the data, go to page 14 ›

Key findings from our phishing research

12%
OF ALL MOBILE SECURITY INCIDENTS INVOLVE PHISHING URLS

63%
OF PHISHING ATTACKS OCCUR ON IOS

81%
OF PHISHING ATTACKS ON MOBILE TAKE PLACE OUTSIDE EMAIL

26%
OF THESE ATTACKS ARE DISTRIBUTED USING GAMING APPS

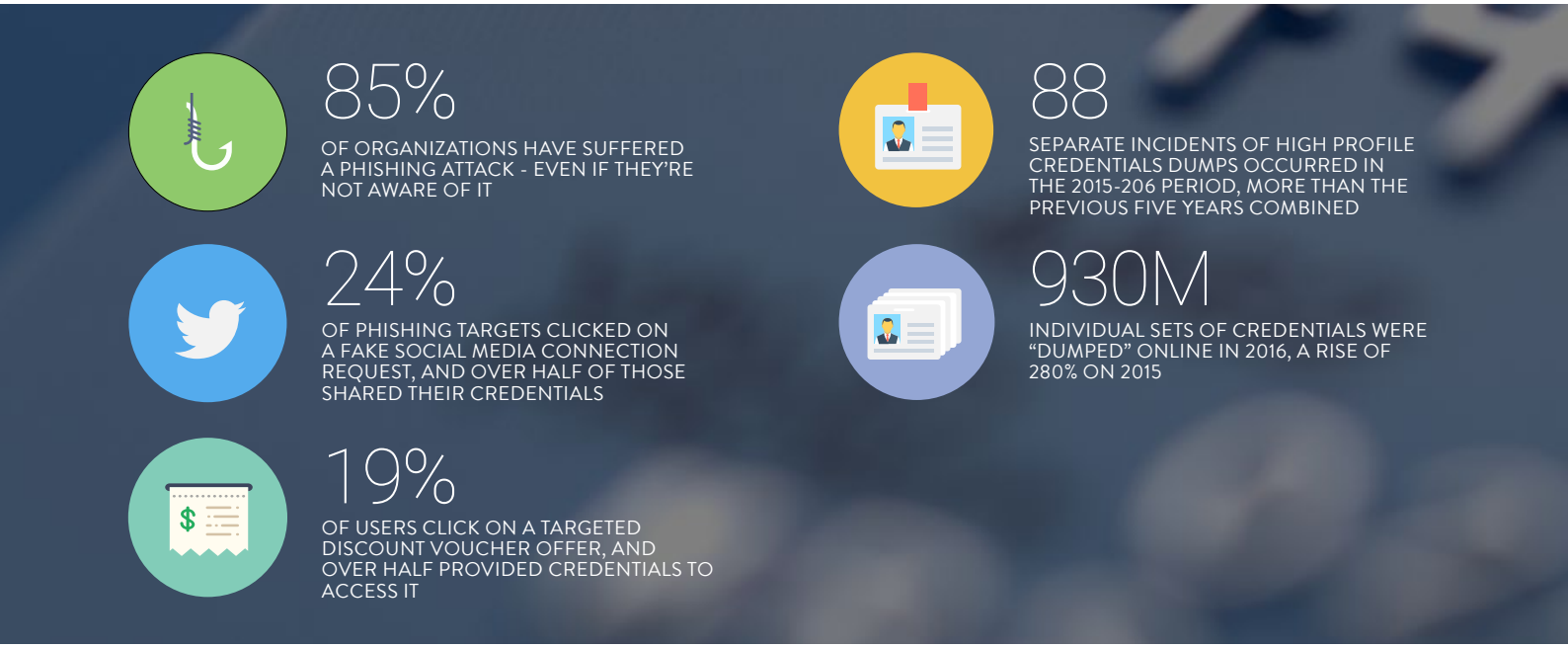
Why mobile phishing is the biggest security risk to organizations in 2017

In November 2016, mobile traffic surpassed desktop for the first time, representing a marked shift in how people access the web. It's a trend that has not gone unnoticed by hackers, who have retooled their arsenals to take advantage of this new landscape of opportunity. Years of hard work to defend businesses against email phishing has left many organizations complacent in staying protected from phishing conducted over mobile apps, social media and other more novel communication approaches.

Research from University of Texas blames overconfidence in detecting phishing attacks as the primary reason that so many users fall victim to these kinds of attacks, with most people believing they are smarter than the actors responsible for the attack. Data from Proofpoint suggests that phishing attacks conducted over social media jumped by 500% in the final three months of 2016, representing a wider trend in hackers looking beyond desktop and beyond email when executing phishing attacks.

These attacks have also grown more high-profile in their nature too, and are even able to bypass two-factor authentication and other seemingly secure defenses. The Clinton email scandal, some of the leaks involving the NSA and even the infamous private celebrity iCloud breach all used phishing techniques. The National Cyber Security Centre in the UK was even forced to issue a warning about the use of phishing in election campaigns in the UK, US and more. The reality is that humans represent a far easier target for exploitation than the comparably secure technologies that protect organizations.

Phishing is not only regular, but it's arguably the most damaging and high-profile cybersecurity threat facing organizations today.



Why mobile?

Mobile features a number of unique characteristics that make it a particularly fertile ground for phishing attacks when compared with desktop

OBSCURED URL

The limited screen space on mobile means that browsers typically remove visibility of the url a user visits, reducing their ability to easily double check suspicious domains.

LIMITED SCREEN SIZE

The aforementioned smaller screens also mean detailed scrutiny of web pages is more difficult.

DISTRACTION MODE

The fleeting, 'on the move' nature of mobile experience means that most interactions demand less concentration from the user. Phishers take advantage of this less focused mode of user attention.

SECURED MEDIUM

For a variety of reasons, people are typically more trusting of mobile devices and apps than they are of desktop software. This misplaced trust makes phishing attempts more successful.

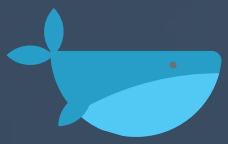
Types of mobile phishing

Financial fraud

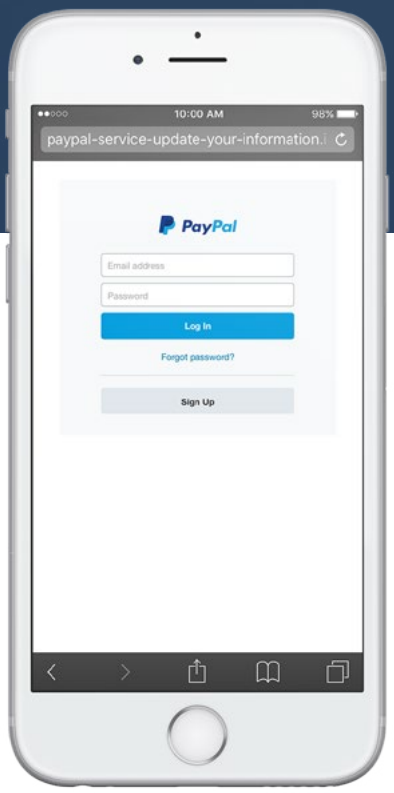
Service updates

Promotional offer

Spear phishing



Whaling



Financial fraud

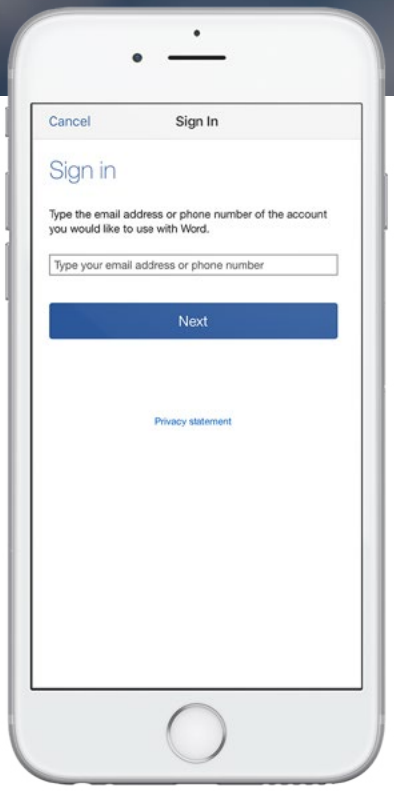
An attack that attempts to directly gain financial information, such as bank details or online login credentials.

One example is fake updates from PayPal look-a-likes that falsify spending receipts, upon which the user will be inclined to investigate. These are typically, but not always, distributed by email. There are also many instances of hackers using SMS to send information to targets as if they are originating from PayPal itself.

The message will often focus on an anomalous payment or important service update, such as confirming the purchase of an item for $29, for example.

The recipient is understandably tempted into inspecting this unrecognized transaction further, and clicks through the email to what appears to be the PayPal login page. Here, user credentials can be gathered by the host of the fake PayPal site, which can then be used to access the real PayPal service - offering hackers direct access to the target's finances.

Service updates

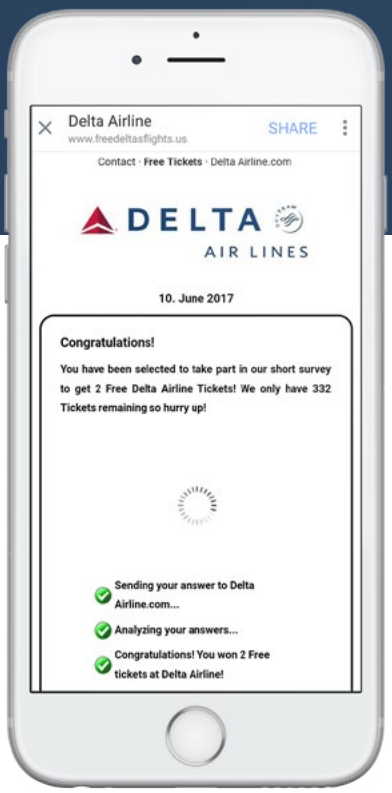


Much like financial fraud, this approach sees hackers pose as services such as Dropbox or a utility provider, often as an indirect means for financial gain. The nature of messages to users can be quite benign, but will attempt to look as legitimate as possible.

Spoof landing pages are designed to capture the real user credentials for these sites, which hackers then use to log in to the real service, and gain access to everything a user has associated with it.

Examples examined by researchers at Wandera reveal a variety of different approaches in this manner. These range from dummy login pages for Google, Microsoft and Apple online accounts, to scary and official-looking updates from Government agencies. This technique can even be used to bypass those that include two-factor authentication (2FA).

A variation of this attack requires a hacker to be online while a target enters their details into the fake page for Microsoft's services, for example. Attackers will then enter the credentials into the real Microsoft login page, which then triggers a 2FA prompt. The target receives a text from Microsoft, as expected, which they then enter into the fake login page. Meanwhile, the hacker reads the real 2FA code that has been submitted by the user, and enters it into the genuine Microsoft login page, thus surpassing even the strongest of 2FA systems.



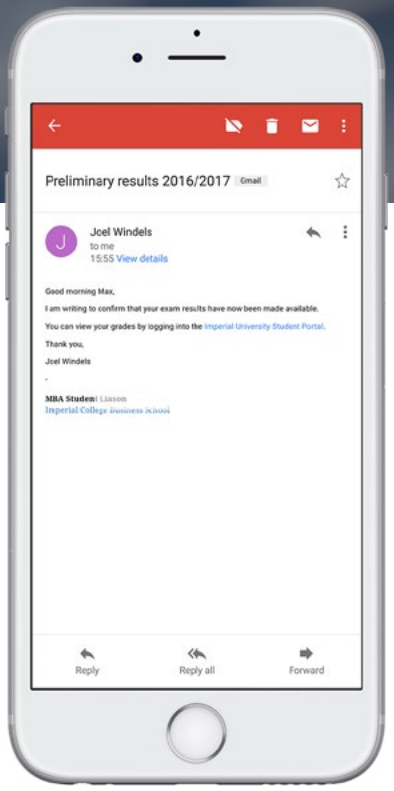
Promotional offer

This is a form of phishing in which some kind of coupon or special deal is promoted. This occurs on a mass scale, using entirely automated processes. This might feature tickets for a gig, or heavy discounting on retail purchases. The added benefit for hackers with this technique is that often the promotion involves resharing the initial link, helping spread the attack even further.

This type of attack is particularly successful on social media and messaging apps like Skype and WhatsApp, where it's more common to trust content from third party sources. Hackers also make frequent use of ad networks and promoted posts to reach even more victims with offers that really are too good to be true.

A popular example of this kind of phishing is a Starbucks promotional page distributed to consumers, where they are invited to sign up to a service so they can receive vouchers for free coffee. Of course, this user information is then accessible by the attacker and can be used for nefarious purposes, such as attempting to use those same signup details to access other more lucrative services. This tactic is more effective than you might initially think - a staggering 55% of web users use the same password for most, if not all, websites.

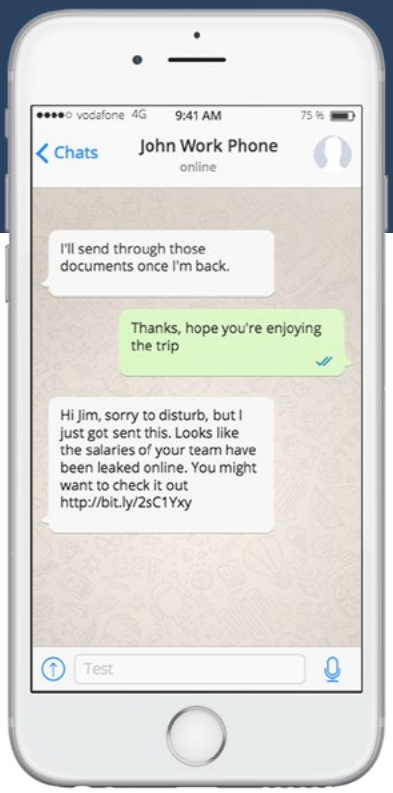
Spear phishing



This type of phishing is much more targeted than other approaches. Here, a particular individual or organization will be attacked using information specific to that target. This might include the impersonation of employees or contractors to extract a certain piece of data, often using manipulation and trust rather than online pages to execute the attack.

An example of this attack happened at Google and Facebook, where emails supposedly from suppliers were sent to members of the finance department. Fraudsters posed as Quanta Computer, a genuine Taiwanese electronics manufacturer that has both Google and Facebook as clients.

Shockingly, even the shrewd and highly intelligent employees of these tech giants erroneously paid invoices worth tens of millions to these phony suppliers, totalling more than $200m in payments between them. This clever blend of targeted, relevant information and convincing, tailored phishing attempts can prove extremely costly to many businesses.



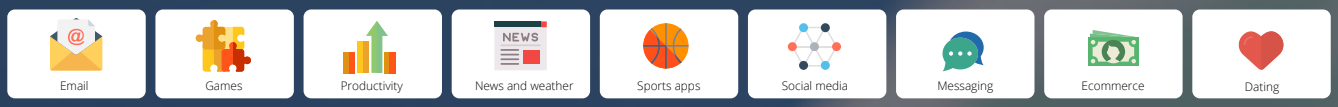
Whaling

Technically a branch of spear phishing, this type of attack is focused squarely on high profile individuals. Attackers can spend months researching their targets, working out their daily routine and mapping their personal relationships. Once equipped with this highly personalized information, the hacker will begin to use it to their advantage.

One example saw the COO of a well-known media company sent a series of messages from an attacker impersonating a remote colleague - itself an intensely researched bit of information. This email was sent using an almost identical domain name, for example using bloornberg.com rather than bloomberg.com. These were coupled with WhatsApp messages of a similar nature, complete with seemingly accurate images and personal details of the target employee stolen from their legitimate social media profiles.

After building a degree of trust in a back and forth series of messages, the imposter included a note informing the COO that the salaries of some of his direct reports had been publicly posted online. The COO, suitably alarmed, clicked through to see where the info had been published, and was asked to download and open an attached file. Included in the file was a nefarious piece of malware, designed by the attacker to gain access to the company's internal systems and steal vast troves of sensitive corporate data. This incident reportedly cost the organization tens of millions of dollars.

Distribution methods



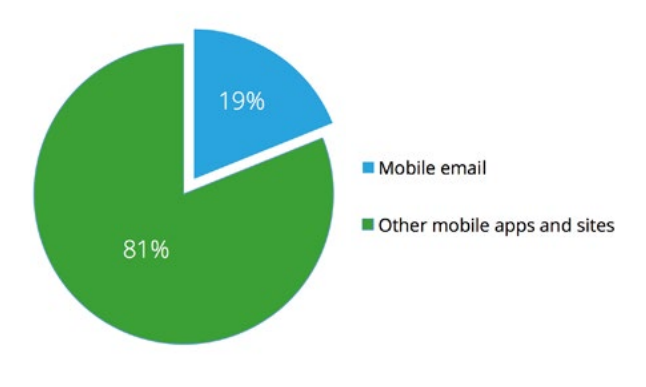
With more than 100,000 phishing urls live at any given moment, mobile phishing is clearly a common and successful form of attack. It's also clear that hackers have moved on from the trusted domain of email, and onto the multitude of new distribution methods made available by the explosive availability of mobile devices in recent years.

Phishing attacks are everywhere, and make use of layered, multi-touch distribution channels.

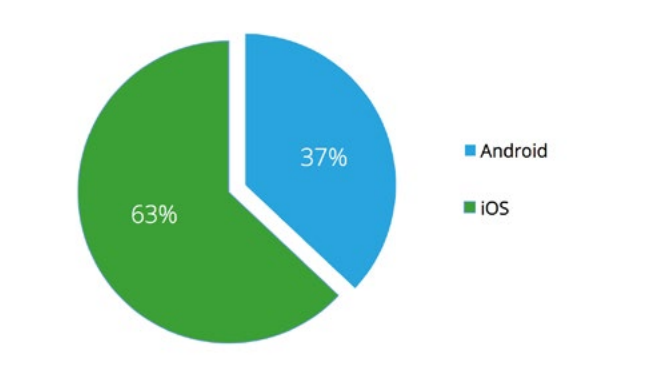
Wandera research focused on analysis of the traffic to known phishing domains and, due to Wandera's unique cloud infrastructure that operates in the pathway of mobile data, researchers were able to determine which apps and services are used to distribute the offending links. More than 12% of all security incidents involve these phishinig URLs.

The following data has been gathered from a sample of 100,000 Wandera-enabled devices for a three week period in June 2017.

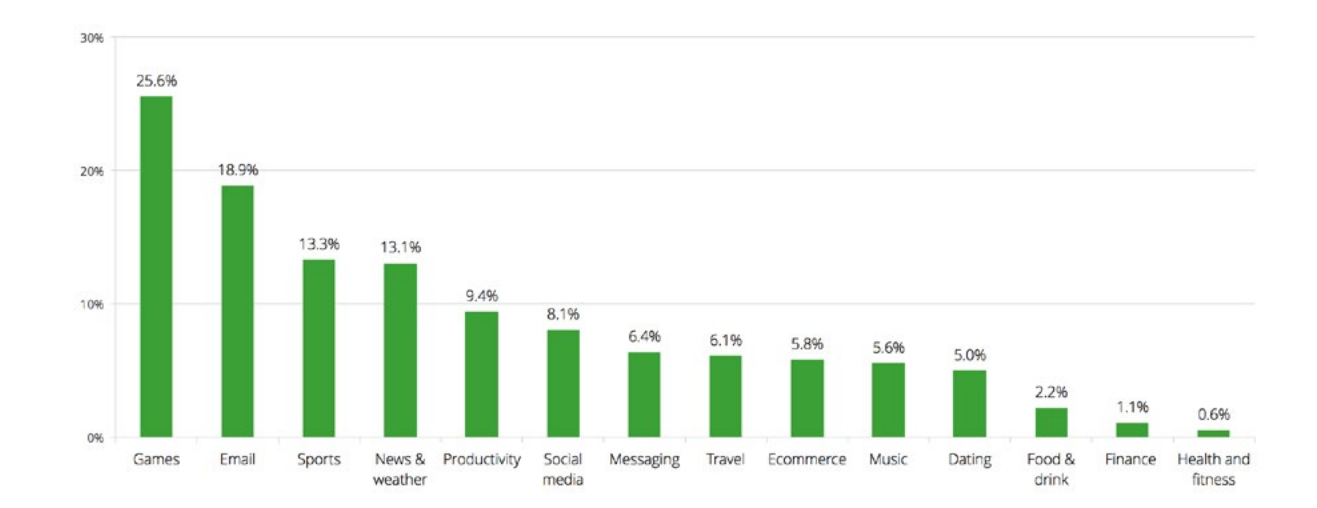
Beyond email: most web-based phishing attacks on mobile now take place outside email apps



Which OS do phishing attacks occur on?



Where does mobile traffic to phishing sites originate?



25.4% Gaming apps

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

In some instances, hackers quickly assemble lightweight and popular game types to capitalize upon player tastes. These titles usually offer similar gameplay to popular games like Football Manager or Mario, providing a free downloadable alternative. However, these apps are designed to harvest player credentials and should not be trusted with any personal data. Moreover, even perfectly legitimate gaming apps feature social functions that allow users to interact with one another. These communication channels are regularly exploited by attackers.

*Examples from the data: Top Eleven - Be a soccer manager, Clownfish Kill, Flick Golf!, Endless Road, Star Wars: Tiny Death Star, Steam**

Email apps 18.9%

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Remarkably, while email may be the preferred method of many attackers, data suggests that fewer than 1 in 5 successful phishing attempts makes use of email. This is likely the result of advanced anti-phishing software used in corporate mail servers, the shrewdness of employees when inspecting emails, and the major improvements that have been made to filters that flag suspicious emails in services like Gmail and Hotmail.

*Examples from the data: Outlook for mobile, Roundcube**

13.3% Sports apps

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Sports apps typically enable users to comment on posts, and interact with one another - indeed, some are simply forums for discussing the latest sports news and opinions. This provides an obvious avenue for phishing attempts, whereby attackers use affinities for particular teams to build trust with other users, who are then duped into clicking on links posted in comments that lead to phishing sites.

*Examples from the data: Leinster Rugby, Chicago Bears Official App, Onefootball**

13.1% News and weather

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Like sports apps, many publishers offer users the chance to comment on various articles. Attackers have been known to use these communications channels to spread links to promotional offers or scandalous fake news posts, which are little more than simple phishing attacks in reality.

*Examples from the data: CNBC, Flipboard, NYT Now, Surfline, Winnipeg Free Press News, theCHIVE**

Productivity apps 9.4%

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Productivity services include a wide range of different tools for enhancing usability and efficiency of workers. Some of these are apps that allow customization or 'upgrades' to devices. Users should be wary of apps that require invasive permission levels for cosmetic functionality. The same caution should be exercised in free apps for currency conversion, document creation, battery improvement and other unrecognized services.

*Examples from the data: Avertinoo, Camera360, Convert Units, Convert - the unit calculator, LockInfo+, Pebble App Manager, WPS Office**

8.1% Social media

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Social media connects people and helps strangers on opposite sides of the planet become close friends. That's the reason it becomes such an appealing target for attackers who exploit features such as connection requests, unsolicited messaging and misleading posts to entice users and distribute phishing links. These will typically be promotional offers but may also form a key part of spear phishing attacks.

*Examples from the data: Pinterest, LinkedIn, Facebook**

6.4% Messaging

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Services like SMS, Skype and WhatsApp provide the perfect alternative to email for attackers to reach targets. Impersonating brands or individuals, hackers use messaging apps to share all kinds of links, which in many cases will be re-shared by targets to their own contacts. One example is a nefarious Skype message that fools targets into thinking they feature in something they might not be aware of by using the simple comment 'is this you?' followed by a link to a phishing page.

*Examples from the data: Messenger, WhatsApp, WeChat, Skype, Kik**



Ecommerce 5.8%

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

Sites like Craigslist, Freecycle, Gumtree and even Ebay make it easier than ever to trade goods with other members of the public. Phishing attempts on these platforms make use of highly enticing listings, which are used to ensnare targets. During the sales process, attackers will attempt to solicit personal information from their victims, either via fake payments pages or through direct manipulation.


*Examples from the data: Kijiji.it, Ebay**

5% Dating Apps

OF ALL WEB-BASED MOBILE PHISHING ATTACKS

IT leaders might see the likes of Tinder, Grindr and Bumble as harmless apps that employees can use to find love on the go. The reality is that hackers know exactly how to trick hopeful singletons into sharing information with attractive people, who of course, may not even exist at all.

*Examples from the data: Tinder, Grindr**


How to combat mobile phishing

Tackling the mounting problem of mobile phishing is a complex one. The goalposts shift constantly and attackers are always on the hunt for new techniques to exploit.

Part of the solution must involve education and basic training around best practices for employee behavior is a must. It should include the principles of sensible communications practices, such as never clicking on links in unsolicited emails or shared through mobile apps, and refraining from sharing credentials or personal information with anyone via any mobile channel - even in those apps you normally trust.

Even the best and most robust education programs will not solve the problem altogether. As any IT director will attest, eventually one employee will fall for a phishing campaign, which is no act of foolishness, considering the sophistication of modern attacks.

With this in mind, it is absolutely vital that you have a security solution in place that is able to monitor and intercept any traffic directed at phishing sites. As a fundamental technique in the hacker's toolkit, phishing domains form the cornerstone of most attacks. Device-only mobile security solutions will do nothing to protect against this threat.

While Wi-Fi security systems, web gateways and mail gateways will offer some protection against phishing attacks for email and for employees working at their desks, the situation changes the moment they leave the office. Organizations are dangerously vulnerable to phishing via 3G or 4G cellular connections, and also when devices connect to unknown Wi-Fi hotspots.

Wandera has built the only technology that can automatically detect, alert and block traffic to mobile phishing sites in real-time.

There is no other solution available that can detect traffic directed towards phishing sites, let alone block it. To find out how you can protect your organization from the rising threat of mobile phishing, get in touch with us today.

wandera.com/demo

wandera

Wandera's pioneering web gateway for mobile provides organizations with Enterprise Mobile Security and Data 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 Expense Management and Policy Enforcement, helping businesses reduce data usage, lower costs and improve productivity, delivering a measurable ROI.

wandera

JULY 2017

Mobile data report

An in depth analysis of mobile data security and usage trends across Wandera's global network of enterprise mobile devices.

Our monthly Mobile Data Report is the world's first report purely focused on enterprise mobility data. It provides a complete analysis of mobile data security and usage trends along with traffic patterns across our global network of enterprise mobile devices. These are corporate liable devices (mostly corporate owned and BYOD) used domestically and whilst roaming.

Security

EMERGING THREAT: ROUGHTED

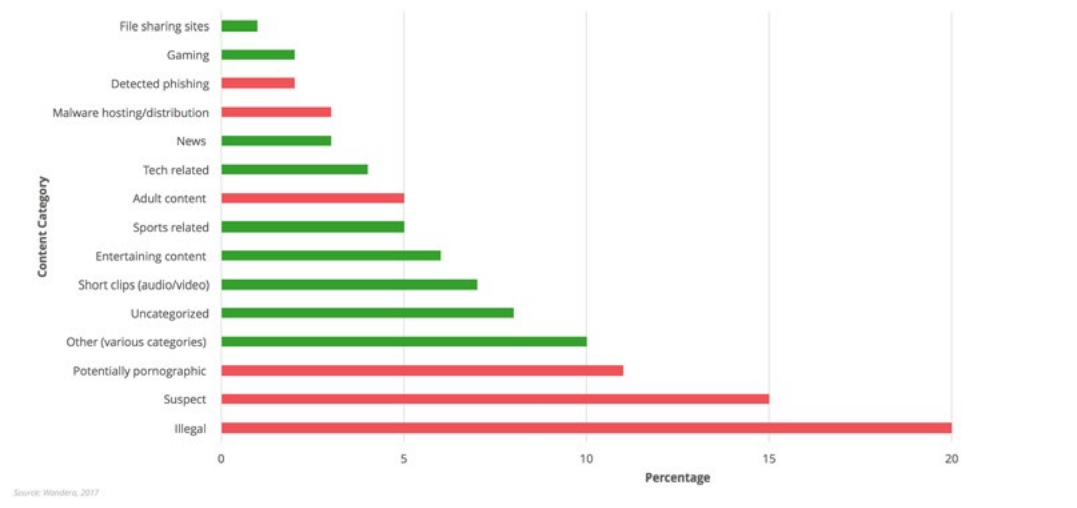
If you've been keeping up with your security news, you'll know that RoughTed is the malvertising operation that has taken the enterprise world by storm.

With thousands of webpages and apps publishing the malvertisements and an estimated half billion hits for the campaign in the last three months, it is responsible for an outlandish number of malicious software downloads on employee devices.

Here at Wandera, our machine learning intelligence engine MI:RIAM has identified 10 zero-day domains that have hosted RoughTed malvertisements that have not yet been blocked by any security nor anti-virus scanner. We also identified the content categories of each domain that was affected by RoughTed and accessed by our global network of devices.

Read more about RoughTed on our blog ›

ROUGHTED DETECTION CONTENT CATEGORIES



THREAT ADVISORY

The threat research team at Wandera, with the help of MI:RIAM, discovered a problematic data leak in Lycos's webmail service (yes, it still exists). The uncovered vulnerability puts individuals' usernames and passwords at risk of exposure, due to the transfer of said information unencrypted over-the-air during the login process.

Read more about this and other advisories on our threat research page >

OPERATING SYSTEMS

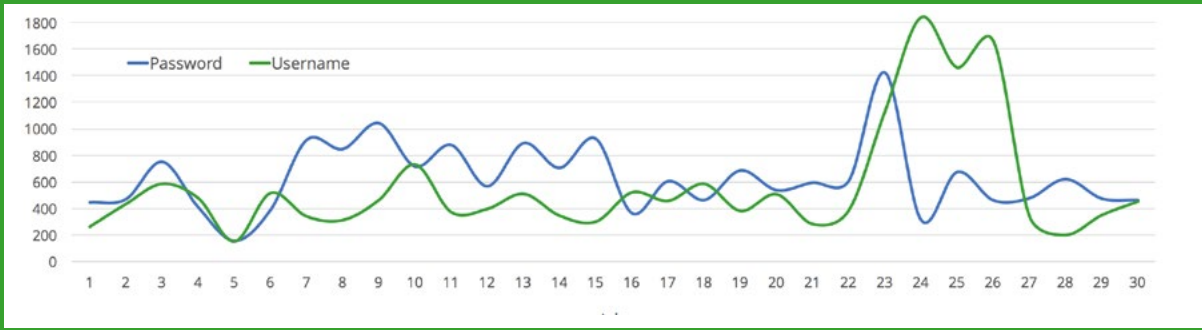
IT teams have been busy in July. Adoption of Android version 7 on Samsung devices has jumped from just 20% to more than 27%. Still a very long way to go, but some progress. Adoption of iOS 10.3 has risen by the same amount, rising to 70% of all iOS devices. We strongly recommend that mobility leaders ensure their entire fleet is upgraded to the latest versions of relevant operating systems.

	June 2017	July 2017
iOS 10.3	63%	70%
Samsung Android 7	20%	27%

DATA LEAKS

Data continues to be leaked - being transmitted unencrypted - while users access a number of different services. Location leaks continue to be more prevalent than email leaks, as we detected almost 800k such incidents in July. Username leaks peaked in late July, which related to a misconfiguration of Microsoft Active Sync Exchange accounts inside some organizations.

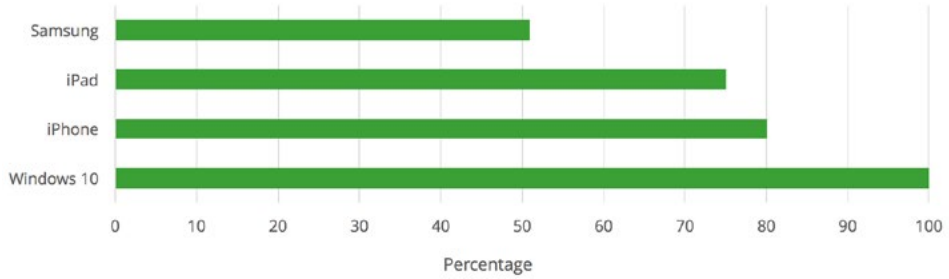
DATA LEAKS: USERNAME & PASSWORD



Usage

DATA USAGE PATTERNS

Remarkably, employees used their phones less intensively in July as they did in June. This might be the result of stricter policies, or simply a case of a vacationing workforce. Once more, Samsung users consumed the least data, with Windows 10 users eating up almost double the daily amount.



TOP APP USAGE

Was there any change in the most popular apps? No, the top ten remains the same - social media apps feature prominently once more in the kinds of services employees are using most frequently.

1. Browser	2. Facebook	3. Mail	4. Instagram	5. App Store
6. SnapChat	7. Youtube	8. WhatsApp	9. Twitter	10. Spotify

ROAMING - **UP 14%**

The amount of data used while employees were overseas rose by 14%, most likely due to the popularity of July as a holiday period. Popularity of navigation apps like Google Maps rose to reach the top five, perhaps as employees struggle to find their hotels upon arrival. Employers are reminded that, as this data suggests, many employees will use their work phones while on leisure trips. This may be no bad or unexpected thing, but it's certainly something worth considering as you develop your corporate mobility policies.

TOP USAGE CATEGORIES WHEN ROAMING

1. Social	19%
2. Technology	13%
3. Video & Photo	10%
4. App Stores	7%
5. Navigation	6%