CERT-UK

Lookout

Mobile Malware in the UK

A report from CERT-UK and Lookout Mobile Security

Executive Summary

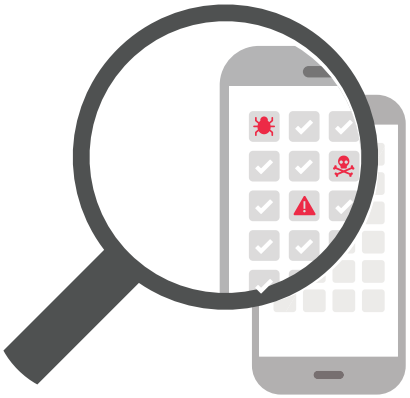
Mobile malware is increasingly sophisticated and as such presents a growing threat to organisations as well as consumers. The volume of malware targeting mobile devices in the UK quadrupled in 2015, with Q1 2016 already reaching 50% of 2015 numbers. CERT-UK assesses that the following factors should be taken into consideration when organisations review their mobile devices security policy;

- Mobile malware continues to target consumers but as the role of mobile in business grows, threat actors have identified mobile devices as a possible weak link in network security.
- Mobile devices can be targeted for a variety of reasons, including to monitor conversations, steal intellectual property and harvest financial details. However it is assessed that the greatest threat to organisations is the theft of network credentials and login details.
- Mobile malware is growing in sophistication, borrowing obfuscation and deployment techniques from traditional PC malware. This implies funding and development from advanced threat actors.
- Although mobile malware presents a risk to all sectors the majority of criminal activity is targeting the financial sector by spoofing mobile banking applications in order to steal user credentials.

It is assessed that mobile devices will become a prevalent part of the attack chain in targeted attacks, especially as a means of harvesting user credentials.

CERT-UK recommends a number of mitigation techniques including Mobile Device Management systems, Mobile Threat Protection solutions, use of mobile Virtual Private Networks and crucially, user education.

Contents



The threat to UK business

Mobile devices are now the most common means of accessing the internet in the UK. Smartphones have overtaken laptops as the most connected devices as of 2015[1] and a third of all web pages are accessed through a mobile device, making UK internet access the most mobile in Europe[2]. Mobile devices are used to connect on social media, banking, shopping online and working on the move, making them critical to UK businesses. Personal mobiles are often as important to business as corporate devices, with four in ten UK employees[3] using their personal mobile for work related tasks. As such all mobile devices have become increasingly connected to organisations networks.

Attackers follow the data, as more sensitive data is accessed by mobile devices, malware targeting this platform is also on the rise.

Lookout data reports that the number of unique samples of mobile malware in 2015 was four times that which was seen in 2014, and this rate of expansion is expected to continue. In 2016, at the time of writing, there have already been twice as many unique malware samples as the same period in 2015.

> "Four in ten UK employees use their personal mobile for work related tasks"

[1] http://media.ofcom.org.uk/news/2015/cmr-uk-2015/
[2] www.timico.co.uk/blog/2016/03/08/byod-reducing-costs-whilst-increasing-productivity-for-your-business
[3] commsbusiness.co.uk/features/byod-technology-employers-employees/#sthash.0HUK8uD8.dpuf

"The average malware infection on a mobile device costing £6,400"

The cost of a mobile infection to an organisation can be significant, with the average malware infection on a mobile device costing £6,400[4] to mitigate. However, the potential impact can be much greater in terms of cost, intellectual property theft, brand reputation and operational capability. Malicious actors now view mobile devices as a viable attack vector and the attacks have reached new heights of operational sophistication, which is likely to result in an increased security risk to UK business.

This report provides an overview of the mobile malware threat to UK businesses, outlining the threat vectors, targeted operating systems and key case studies. This report also includes advice to organisations on how to keep their devices secure and mitigate risk.

What is mobile malware?

Mobile malware is malicious software specifically designed to attack mobile devices such as phones or tablets. Whilst it often works in tandem with computer malware it can also operate entirely separately. Many of the threats are the same as might be encountered whilst browsing on a computer, however some threats such as those attacking applications, are unique to mobile devices.

Historically the majority of mobile malware targeted consumers, as they represented the largest proportion of device owners. As much of this was lower severity adware, riskware or chargeware, (the definition of which can be found in the appendix) mobile malware has been in the past, perceived to have limited impact on organisations. However this paper outlines how mobile malware can and does represent a threat to UK business.

What is the threat to UK businesses?

Traditionally the threat to UK businesses was aimed at the employee's devices rather than networks. However, although end devices continue to be the target they may no longer be the ultimate goal of an attack. For example, adware, whilst continuing to target consumers has been observed exhibiting more sophisticated behaviour. Many attacks now seek to root, or gain high level privileges to the device in a trojan-like behaviour.

"Many attacks now seek to root, or gain high level privileges to the device"

This means that although the attacker may initially focus on delivering adware if the method of monetisation were to change to exploiting an individual's work emails, calls or messages, organisations could begin to be severely impacted by an attack initially directed at an individual mobile device.

The ultimate threat to an organisation is the compromise of corporate data, therefore businesses should be aware that this is likely to be the objective of some malicious actors. Employees use mobile devices and PCs in tandem, and it should be expected that threat actors will do the same, incorporating mobile devices into the attack chain, especially to target user credentials. It is important, therefore, that UK businesses are aware of the potential cyber risk to their organisations beyond traditional PC malware.

[4] The Economic Risk of Confidentia Data on Mobile Devices in the Workplace

What types of malware are targeting the UK?

The critical and evident trend is that the volume of mobile malware is increasing, with a 421% increase in unique samples in 2015 compared with 2014. This trend is set to continue, with Q1 2016 already reporting 48% of the full year 2015 numbers.

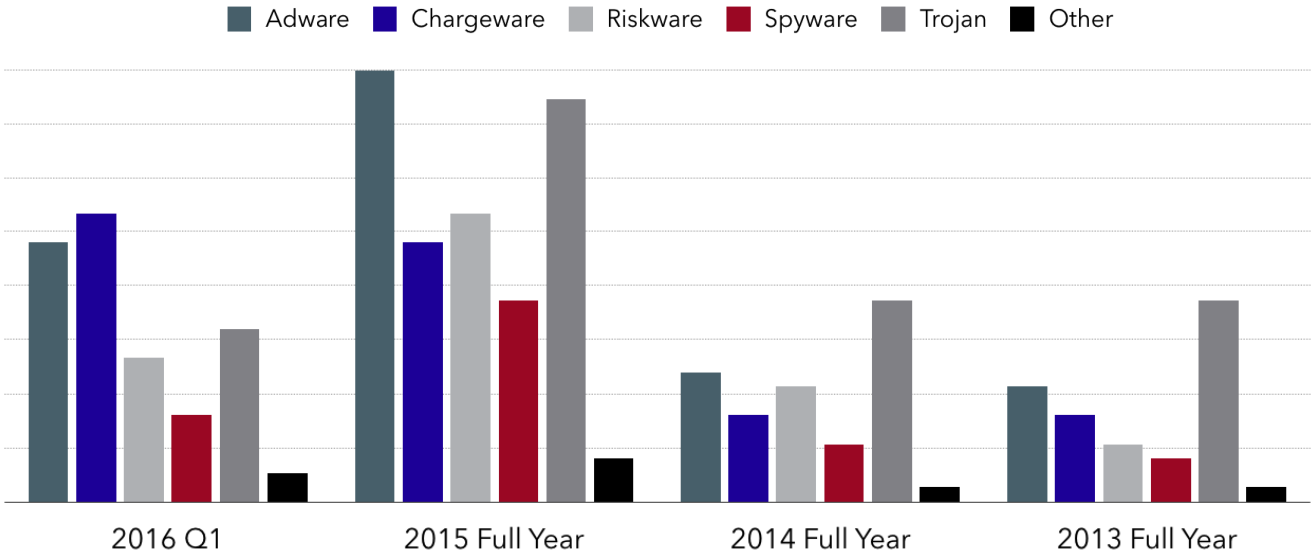
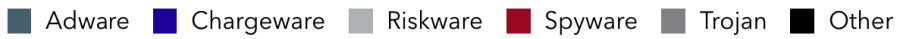


Figure 1 illustrates the growth of unique malware samples across the last three years and the first quarter of 2016.



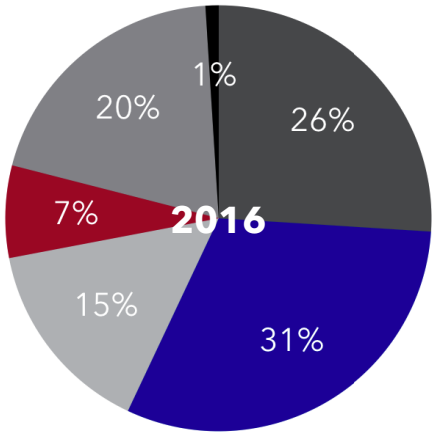


Figure 2 shows the breakdown of mobile malware seen by Lookout researchers, in Q1 2016.

Chargeware, adware and riskware account for 72% of the mobile malware seen and mainly impact consumers rather than organisations. However, in many cases these malware are now exhibiting root capabilities and as such are capable of surviving a factory reset. Root capabilities should give organisations pause, as a malicious actor could use them to install key-loggers, capture sensitive information and even circumvent a Mobile Device Management (MDM) container, retrieving a user's corporate username and password in the process[5].

These capabilities have the potential to significantly impact end users and the organisational infrastructure that they're connected to. Techniques typically seen only in PC malware are being steadily incorporated into their mobile counterparts; evasion techniques have recently been joined by modular malware consisting of multiple stages. This increase in complexity suggests more technically skilled, well-funded adversaries are operating in the mobile space. These actors will target existing rooted devices (the 72% affected by adware, chargeware and riskware) and seek to exploit them beyond installation of adware.

[5] https://www.linkedin.com/pulse/byod-security-illusion-finding-corporate-credentials-mdm-flossman Lookout

"Mobile trojans account for 20% of mobile malware"

Mobile trojans account for 20% of mobile malware so far this year and perform malicious actions other than those advertised. Trojans can vary in impact on the user depending on the sophistication and intent on the malicious actor who deployed it.

Spyware applications harvest information from a large number of devices, and account for 7% of mobile malware seen. They hide on devices and forward information about device activities to a third party. Information forwarded may include contacts, calls, SMS messages, current or previous locations, and browsing history. This can have obvious implications for information security for organisations, in particular in relation to intellectual property or M&A details and organisations should be aware that cyber criminals will often work in tandem with traditional criminal networks to commit fraud.

The "Other" category is the smallest seen in the UK, accounting for only 1%, but contains some of the most dangerous threats to organisations such as mobile exploit kits, high level surveillance activity and bot deployment.

An example of this would be NotCompatibleC, a threat to Android devices, discovered by Lookout. Disguised as a system update that contains a proxy functionality, it allows attackers to infiltrate secure enterprise networks via compromised devices[6].

The method of distribution is a relatively simple spam campaign which is not reflective of the complexity of the back end of the attack, but clearly represents how simple infiltration methods can still deliver sophisticated malware. Mobile devices that operate outside of the traditional security perimeter are often the targeted weak link, and this is not limited to mobile phones; organisations should ensure they consider all connected mobile devices.

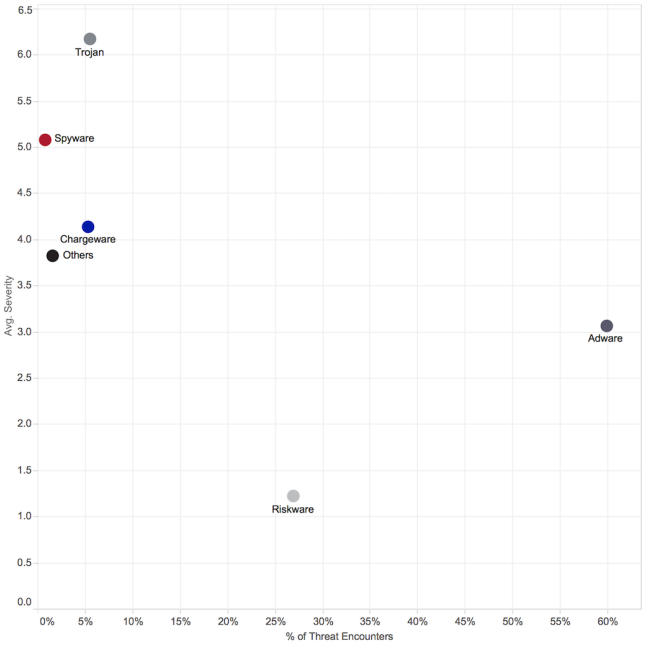


Figure 3 illustrates mobile malware recorded by Lookout in 2016

As with any threat analysis it is important to weigh the impact of the threat against the likelihood that it will attack your organisation. Figure 3 shows threats by risk, with risk being the likelihood of a threat (prevalence) paired with its severity (impact). Some threats may be common but are less severe. Conversely, even if some threats are present on just a small number of mobile devices, their severity is high, presenting a high risk to the organisation. It can take just one compromised device to provide an attack vector into an organisation.

In 2015 the three most prevalent mobile malware threats detected by Lookout in the UK were all Android ransomware trojans. Whilst these trojans may be targeting individuals and consumers it is worth noting that PC ransomware is now successfully targeting organisations, and it is therefore not unreasonable to expect malicious actors to attempt to emulate this success on corporate mobiles devices.

[6] Lookout publication, "Notcompatible.C a sophisticated Mobile Threat that puts protected networks at risk" P.1

Case study : the Triada malware family

The Triada malware family is a perfect example of mobile malware continuing to increase in sophistication by borrowing techniques from desktop malware. Emulator detection, polymorphic code, packers and code obfuscation have gradually been incorporated into the toolkit of mobile malware developers resulting in a serious increase in sophistication over the past few years. The Triada family has taken this a step further by implementing a very modular, multistage approach.

As the name suggests, multistage malware consists of multiple components that are downloaded and run on a device at different times. The first stage is often a seemingly benign app that doesn't contain any overtly malicious functionality. It's designed to have a small footprint on the device and its purpose is simply to gather device information and report it to the command and control infrastructure.

A second stage that contains the core functionality of the malware can then be downloaded later. This is the approach Triada takes and it can be an effective way to evade anti-malware solutions. A threat actor can build up their user base before launching their attack, as was the case with Brain Test[7] game app, which was live on the Play Store for months before receiving a malicious update. Updates are a critical part of mobile security but familiarity with the process can provide an opportunity for social engineering. An attacker can also determine if an infected device is of high value before choosing to deploy their second stage.

By limiting the spread of their second stage to high value targets an attacker is able to reduce the chance that their core capabilities are found, analysed and detected by security researchers.

Who is behind the threats to UK business?

As with PC malware, the threat actors in mobile malware are numerous and diverse with varying motivations. However the most significant threats can be categorised as criminal groups and APT.

Criminal

Initially considered the domain of the amateur cyber-criminal, the increasing sophistication and prevalence of mobile malware indicates that professional cyber-criminal groups are investing in this sphere. The motivation is profit generation through; directly removing money from victim accounts, extortion, stealing information and even by generating income through premium SMS and advertising revenue.

Often criminal networks will employ adware and chargeware which may seemingly target individual users rather than organisations. However, much of this malware comes with rootkit capability, allowing the criminal heightened permission on the device. If the method of monetisation of the criminal were to pivot, organisations could be exposed to extortion through ransomware, corporate espionage through monitoring of emails, calls or messages or even by using the compromised mobile device as a means to access the main corporate network as was seen in the NotCompatibleC example.

APT

Mobile malware presents an obvious opportunity to Advanced Persistent Threat (APT) groups who seek to gain access to conversations, data, passwords, geolocations and the myriad of personal information that mobile devices can hold. This presents a risk to the intellectual property of UK businesses. The potential for mobile malware to be used in espionage has been much discussed in the media following Google's removal of an App from its play store after allegations that it was being used by an APT group to monitor Indian Military personnel[8], recording their phone calls and locations. One of the most ubiquitous forms of mobile malware in the wild is AndroRAT, identified as far back as 2012 and still persists today, it is a remote access tool for Android, published online and thus available to anyone.

[7] https://blog.lookout.com/blog/2016/01/06/brain-test-re-emerges/
[8] https://www.hackread.com/google-removes-smeshapp-india-pakistan-spying/

It allows attackers to monitor calls and messages, establish device co-ordinates, and activate camera and microphone as well as access files and documents. Organisations which allow employees to use their personal mobile for work should be particularly aware of this threat. In 2015 the Italian spyware company Hacking Team, who provide software targeting user communications, were hacked. This revealed not only the data which they had collected for their clients, which were often state governments, but also that there was significant interest in compromising mobile devices and the capabilities available to do so. This included the ability to monitor non-jailbroken iPhones using an app which had been signed with an Apple enterprise certificate, allowing it to be side-loaded and operated on a non-jailbroken device[9].

Case study : Operation Pawn Storm

Operation Pawn Storm is a well-known and active APT targeting primarily military and political organisations. They are known to be using mobile devices as one of their attack vectors, in particular iOS. The malicious app, identified by Trend Micro as IOS_XAGENT, is found masquerading as a legitimate game (Madcap). The malware steals information from any mobile device it infects including SMS messages, contact lists, geo-location, pictures and voice recordings.

Whilst Pawn Storm may be targeting governments, this example illustrates that the capability exists to monitor potentially sensitive conversations. This presents a threat to UK businesses as it has been seen that, as with PC malware, hackers are willing to work in tandem with other elements of the criminal and fraud community. An example of this was the string of Wall Street banks targeted by a combination of hackers and insider traders, monitored private M&A discussions over a 5 year period to illicit over $100 million.

How can mobile malware infect your device?

Mobile malware can be delivered through several different vectors; these include compromised websites, infected applications, or by users jailbreaking their devices or side loading apps.

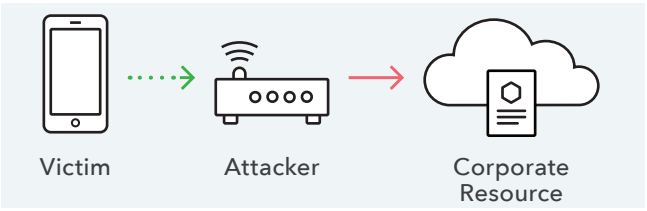
Drive-by-downloads

This infection vector, which takes advantage of vulnerabilities in a web browser by exploits hosted on web sites visited by the user has long been used in PC malware delivery and works in much the same way across mobile. Infection can occur when a user browses the web and lands upon a compromised website or if they are directed there by clicking on a link sent by email or, increasingly, in an SMS message. SMS phishing campaigns (SMishising) are considerably more effective than PC email campaigns due to lack of awareness and implicit trust in the personal nature of SMS messages.

UK organisations should look to raise user awareness of the problem and have device level controls to validate app or file downloads, whilst also ensuring devices operating systems are routinely updated to reduce the number of vulnerabilities on devices available for exploit.

Man in the Middle attacks

Whereby a user's traffic is intercepted and decrypted by an attacker. The user may be tricked into connecting to a rogue hotspot in a location such as a cafe, airport or hotel, allowing an attacker to intercept the traffic. From the user's point of view this process may be transparent. Limiting access to Wi-Fi networks completely may be impractical, so organisations should consider the use of device level security to detect network tampering in progress. In addition, network and app level transport encryption can help mitigate the threat.



[9] https://www.washingtonpost.com/news/the-switch/wp/2015/08/11/hackers-who-breached-corporate-wires-made-millions-off-insider-trading/

Mobile Applications

Lookout researchers assessed the total amount of malware ever seen in the official Android Play Store to be just 2.02% of all apps published on it. This is in contrast to 34.55% of apps sourced from unofficial sites or third party app stores being identified as malware. As such UK businesses should consider restricting app downloads on corporate devices to official stores only, in order to reduce the risk of downloading infected apps.

This will be even more important as mobile and PC applications converge, with mobile devices gaining functionality typically associated with PCs and PCs are being architected more like mobile devices. Windows 10 for phones and tablets can run "Universal" apps that also run on PCs.

This increases the likelihood of a mobile device being used as a means of entry to an organisation's central network, as universal or platform agnostic apps will act as a bridge between mobile devices and PCs.

Side-loaded apps and Jailbroken devices

Increasingly phones do not have to be jailbroken in order to download apps from unofficial stores, instead we are seeing a rise in the number of side loaded apps which are often legitimate but provide an easier avenue of approach for malware compared with official stores. For a $299 subscription, Apple's Enterprise Developer Program allows organisations to create and deploy their own in-house apps, a process which may be abused by third parties looking to distribute apps outside of the official App Store.

Case study : gaining access to official app stores

There have been several recent incidents which indicate an escalation of effort by bad actors to gain access to official app stores and their users. XCodeGhost was the first large scale attack that deceived the review process on Apple App Store, successfully infecting millions of users with malicious code. Adopting a previously unseen infection vector, it targeted the Software Development Kit (SDK) used to write iOS apps directly, the compromised SDK then infected legitimate applications with injected code.

The infected apps had the capability to collect device information and open web pages from the app and redirect users to sites which could contain adware or further malware. CERT-UK data showed a huge spike in the latter half of 2015 (Figure 4) , demonstrating that while traditionally Android devices have been the most targeted, iOS is far from immune. Xcodeghost, YouMi and MobiSage were all examples of malware which exploited the SDK, demonstrating the creativity of malicious actors to work around, rather than attempt to break through security processes.

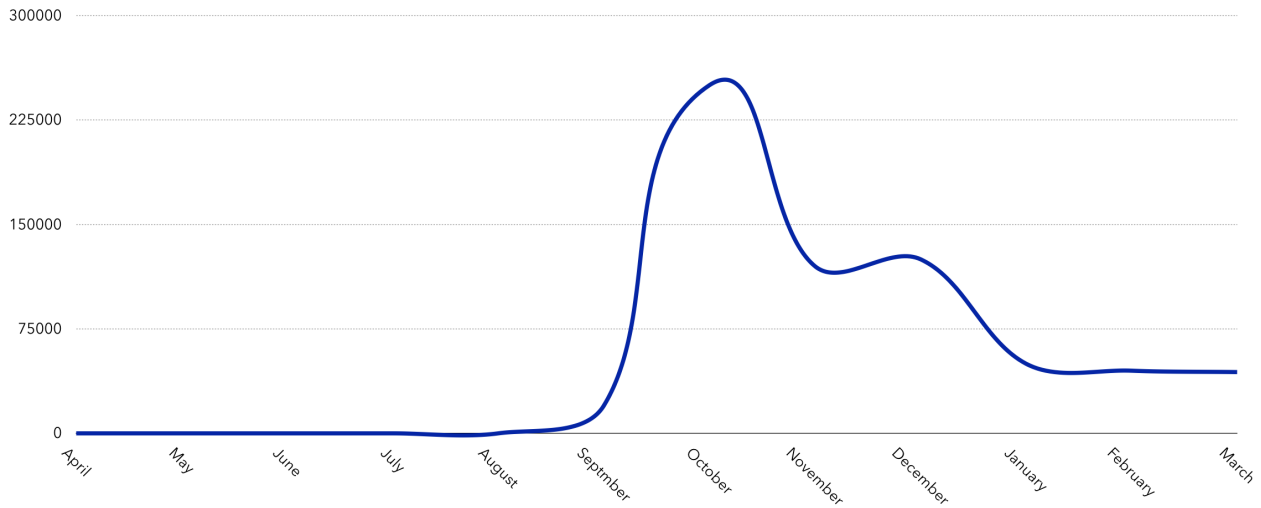


Figure 4 illustrates the spike in malicious activity on iOS seen by CERT UK

What are the main mobile malware vulnerabilities, and to which platforms do these apply?

Google has made efforts to reform the Google Play store in order to reduce the amount of malware targeting its operating platform, despite this the majority of reported mobile malware is seen targeting Android.

This is driven by Android's domination of the global market[11], functionality allowing side loaded apps and by the complex update and patching process. At the time of writing, only 4.6%[12] of Android users were running Marshmallow, the latest updated version of Android released in October 2015.

However, Google continues to make security improvements such as full disk encryption and granular app permission control, forcing mobile malware authors to evolve and adapt which is likely to include targeting other operating systems.

Targeting iOS is more complex, often requiring the threat actor to chain together multiple exploits in order to gain root. This requires a high degree of complexity and is highlighted by the fact that no jailbreak is currently available for the latest version of iOS and that the security company Zerodium offered a reward of one million dollars for an iOS 9 remote code exploit[13].

This reward was allegedly paid indicating that iOS is clearly a target for well-funded sophisticated threat actors. Therefore although most low level malware is targeting Android, more sophisticated threats, particularly from APT groups, will focus on the platforms where their desired target victims operate. State actors and well-funded criminal networks are known to sponsor corporate espionage, and it is highly likely that malware monitoring the mobile activity of C-level employees is targeting UK businesses. A lack of visibility of malware on other operating systems does not necessarily mean they don't exist. As figure 5 illustrates, the Android platform is the most exposed to vulnerabilities.

The Android landscape is heavily fragmented with a multitude of devices running different versions of this operating system. Each device will typically have an Android OS that has been modified by the device manufacturer as well as the regional telecommunications provider. This introduces a significant lag in the update cycle, as any patches that Google releases need to be approved and modified by both the device manufacturer and telecommunications carrier.

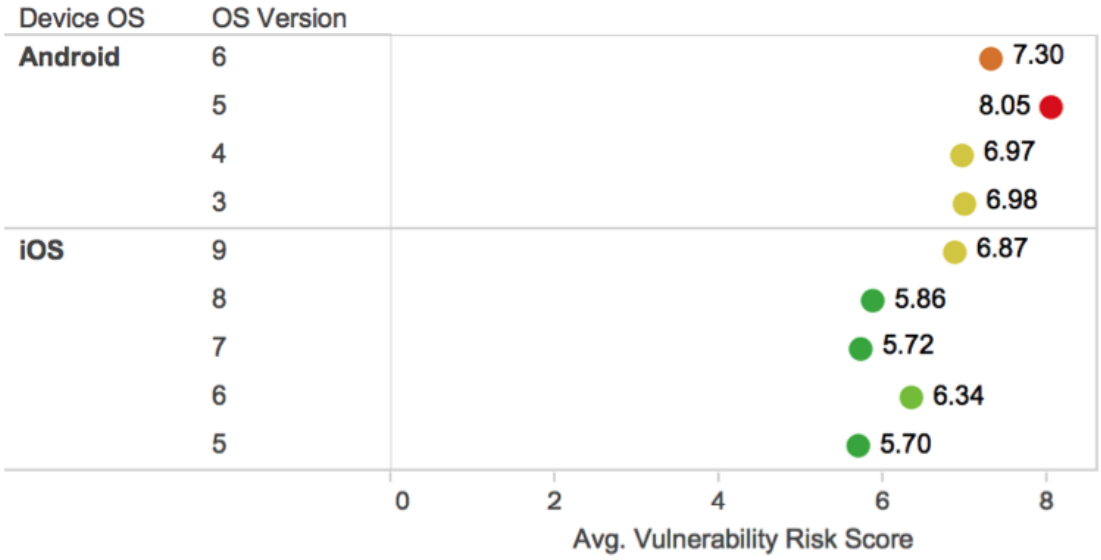


Figure 5 illustrates the most exposed OS versions on Android and iOS

[11] 80% of smartphones worldwide operate on the Android platform (http://www.idc.com/prodserv/smartphone-os-market-share.jsp)
[12] http://developer.android.com/about/dashboards/index.html
[13] https://www.zerodium.com/ios9.html

This introduces complexity and overhead and consequently it isn't uncommon for updates to never be released to customers. This has a major impact on Android users as the majority of them are running a version with known vulnerabilities that trails well behind the latest release. The Apple update cycle gives this operating system a major security advantage. Updates can be pushed out as needed and its clear end users are actively upgrading with 84% of iOS devices running the latest version[14].

When selecting a mobile platform UK businesses should consider the available features and controls including device lifecycle, updates and patching. For iOS this process is driven by Apple and requires minimal user interaction especially if organisational MDM policy requires users to be running the latest OS version. Selecting a device for Android will require ensuring it supports the latest version and will receive long term support as well as user education on the importance of running updates.

Mobile malware as a threat to an organisation's relationship with consumers

In 2015 mobile banking apps became the leading way in which customers manage their finances[15], overtaking both branch and internet banking. As money is often the motivation behind malware, this places the finance sector directly in the sights of the criminals who are seeking a profit. In 2015 Kaspersky included two mobile malware families in their top 10 malicious financial programmes[16] for the first time and the number of mobile banker Trojans increased four-fold in a single quarter[17], making it the fastest growing category of mobile threats. CERT-UK anticipates that this trend will continue in line with the growth of app and online banking. Whilst this will not present a direct threat to a financial organisation's internal network, it presents a significant risk to customers and can impact on brand and reputation.

Case study : Marcher malware

Marcher malware, one of the most prolific password stealers seen in the wild targeting mobile banking app credentials from Android platform users. Marcher waits for a user to launch a legitimate app which they may associate with payments, such as the Google Play store or a mobile banking app, it will then overlay the app's screen with a phishing window designed to look like a login screen, requesting the user's card credentials or mTAN (mobile transaction Authentication Number). Once credentials are entered they are collected and uploaded to the malicious actor. When it was first seen in 2013 Marcher was limited to Russian devices launching the Play Store, by 2014 it began targeting financial institutions in Europe and has continued to add an increasing number of global financial institutions to its repertoire.

14 https://developer.apple.com/support/app-store/
15 https://www.bba.org.uk/news/press-releases/mobile-phone-apps-become-the-uks-number-one-way-to-bank/#.VxYIvfkrLVY
16 http://www.kaspersky.com/about/news/virus/2015/Kaspersky-Lab-mobile-banking-threats-among-the-top-10-malicious-financial-programs-for-the-first-time
17 http://www.darkreading.com/vulnerabilities---threats/mobile-malware-makes-mobile-banking-treacherous/d/d-id/1322957

How can your organisation protect itself from mobile malware?

As mobile working is an extension of the connected enterprise, businesses should ensure they follow guidance published by the UK government such as 10 Steps to Home and Mobile Working. Whilst there is no such thing as 100% protection, there are certainly best practices that business can follow.

As a first step you should consider deploying a MDM (Mobile Device Management) or EMM (Enterprise Mobility Management) solution. These allow greater enforcement and control of employee devices and allow an organisation to spot endpoints that are running outdated OS versions and may be more vulnerable. MDM solutions allow organisations to have a more meaningful degree of control over employee devices via separate containers for corporate and personal apps.

If an employee leaves, or their device is lost or stolen, an organisation can remotely wipe this corporate container, significantly limiting what a malicious actor could do if they had physical access to the device.

> "MDM solutions are not a silver bullet when it comes to securing mobile devices"

MDM solutions are not a silver bullet when it comes to securing mobile devices. It is recommended they are complemented by a mobile threat defence solution. These provide enhanced visibility and contextual awareness of app, network and OS level threats. In addition, they can be more accommodating to BYOD deployments where deploying a management agent to a device may not be feasible.

Such tools are useful not only to corporations but also to individuals, who may benefit from being alerted to the presence of malware on a mobile device before carrying out activities such as mobile banking. When it comes to publishing in-house apps, app scanning tools can be used to review app code and to ensure they are vulnerable free, thus reducing exposure to malware and other attacks.

Ensuring a secure connection is important to improving mobile protection. Solutions may be used to detect when network attacks or eavesdropping are in progress and care should be taken to assess the inherent security of apps in use. The use of mobile VPN (Virtual Private Network) can also be used to access corporate data when a user is on the move.

Mobile working blurs the lines between corporate and personal, hence employee education can be effective in an organisation's mobile security program. This includes; awareness of the risks associated with downloading from third party app stores, risks associated with downloading unofficial apps, jailbreaking or overriding a device's security protocols, connection to unsecured Wi-Fi networks in places such as coffee shops and a general awareness of SMS Phishing and the risk of following links from unverified sources.

Correct implementation of the above recommendations will help UK organisations stay ahead of the mobile malware threat. However mobile devices will become increasingly attractive targets to actors as they become more ubiquitous and critical to business function. Mobile malware is no longer the domain of amateurs, it is increasingly being pursued by well-funded and technically proficient criminal networks and APTs.

The threat is constantly evolving and being driven to innovation and increasing sophistications. Organisations can counter this by introducing proactive user education and technical controls and most critically by remaining open minded and aware of the threat.

CERT-UK

Lookout

Threat Taxonomy

Malware Group	Threat Subclass	Description
Trojan	Trojan	Trojans perform actions other than those advertised in order to perform malicious actions such as fraudulently charging a device's wireless bill or stealing information from devices.
Adware	Adware	Adware contains code from an advertising network to collect personal information or engage in intrusive presentations of advertising without providing proper notification. This functionality can include adding shortcuts to the desktop or displaying ads in the notification tray.
Chargeware	Chargeware	Chargeware will charge a device's wireless bill for services without providing adequate information about the charges or giving users an opportunity to accept the charges.
	Click Fraud	Click fraud applications use devices to defraud pay-per-click or pay-per-download advertising, which may result in data overage charges on a device's wireless bill.
	Toll Fraud	Toll fraud applications send premium SMS or make calls to premium rate numbers that charge a device's wireless bill, often with little or no indication to the device user.
Spyware	Spyware	Spyware is software that spies, that is broadly distributed and whose end-game is typically spam and/or phishing enablement. The motive here is monetary.
	Surveillance	Surveillance applications are generally commercial software designed to monitor a specific, targeted device. They hide on devices and record or forward information about user activities to the installer of the software. Forwarded information may include contacts, call history, SMS messages, current or previous locations, and browsing history.
Riskware	Riskware	Riskware includes code, libraries, or network services that pose a risk to devices due to known vulnerabilities in the code or the low reputation of service providers used by the code. This type of application is not known to be malicious, but may subject devices to more risk than a typical application.
Worm	Worm	Worms exploit a software flaw to remotely attack devices. They will attempt to replicate themselves from device to device, and may also steal information from devices and cause unpredictable behaviour.
Others	App Dropper	App droppers download applications to devices without user consent. They may suggest that the user install the downloaded application and the downloaded application itself may be malicious.
	Backdoor	Backdoors leave a file or program on a device that will allow other programs to access protected areas of the device's operating system.
	Bot	Bots place significant device functionality under the remote control of a third party. This functionality may include accessing the network, sending SMS, making phone calls, or downloading applications.
	Data leak	Data leaking applications send information about users and/or their devices to a third party without user knowledge or consent. Forwarded information may include contacts, calls, SMS messages, current or previous location data, and browsing history. The information may or may not be used for malicious purposes.
	Exploit	Exploits utilize a flaw in software or a component of a device's operating system, usually to gain root privileges on a device and perform privileged actions on the device, including potentially malicious actions.
	Root Enabler	Root enablers give users access to privileged functionality on their devices and are commonly used in phone modification communities to enable full access and control over the device
	Spam	Spam applications send SMS or make calls from devices to enable spam campaigns, which may result in fraudulent charges on a device's wireless bill.
	Virus	A class of test applications (such as the EICAR test file) designed to test the efficacy of anti-malware detection.