# Mobile Malware Implications for IT Management[1]

**Brett van Niekerk**
**Manoj S. Maharaj**

## Abstract

Since the turn of the century malicious software, called malware, has been generated to infect not only computer systems but also 'smart' mobile phones. This malicious code is designed specifically to infect the mobile devices and disrupt the operation of the device or to send messages or make calls, resulting in financial loss to the user. The paper analyses trends in mobile malware from the listings of the malware descriptions. These trends show the increasing severity of the mobile malware problem, the introduction of new malware types, and the changing focus on the malware objectives; predictions of possible future trends are made. The implications of these trends for organisational management are discussed, and possible countermeasures to the risks are suggested.

**Keywords:** malicious software, mobile malware, infection tends, trend analysis, implications for management

## 1. Introduction

Traditionally malicious software, called malware, was based on infecting personal computers (PCs) and propagating via the networks. With the ubiquitous nature of mobile devices, it was only a matter of time before malware migrated to mobile phones. Once malware had been introduced to

[1] An earlier version of this paper was presented at the Business Management Conference 2011 at the University of KwaZulu-Natal.

Electronic ISSN: 2519-5476; DOI: https://doi.org/10.29086/2519-5476/2017/sp20a12

mobile platforms, malware developers found many new communications technologies (and related vulnerabilities) to aid in the propagation and infection strategies for the malware.

The paper is organised as follows: Section 1.1 describes the various available mobile platforms that are relevant; Section 1.2 provides background to the basics of mobile malware, including the types and payloads, and the infection, propagation and distribution strategies. Section 2 discusses the past trends in mobile malware by analysing secondary data; Section 3 discusses emerging and possible future trends. Section 4 concludes the paper.

## 1.1 Mobile Platforms

As with traditional computer-based systems, mobile devices have operating systems (OS). Different device manufacturers utilise different operating systems; some have their own OS designed in-house. In addition, there are development platforms available to allow users and third parties to create applications for the mobile devices. This section describes popular platforms that are relevant to the paper.

There are two platforms for Windows Mobile: the earlier version was known as Windows CE or WinCE, and more recently the Microsoft Intermediate Language (MSIL); applications may be programmed in other languages, which are then compiled into MSIL to run on the device (Dwivedi, Clark & Thiel 2010). Siemens devices use a custom design called S/EGold (Gostev & Maslennikov 2009), and Nokia largely uses the Symbian series OS for their range of devices. Google Android is based on Linux and is programmed with the Java language (Dwivedi, Clark & Thiel 2010).

The iPhone, iPad and similar devices use the iOS developed in-house by Apple (iPhoneBlogr, 2010). The functionality of these devices is limited by the iOS; this can be circumvented by JailBreaking, which refers to escalating access privileges on the iOS versions. This gives the user better access and application control for the device, improving its functionality (iPhoneBlogr 2010). However, this may also open vulnerabilities.

Java 2 Mobile Edition (J2ME), also known as Java Mobile Edition (JME) is a popular development platform for mobile devices; however, it is not a full OS, but a set of standards, and may be run on many different devices and OS versions (Dwivedi, Clark & Thiel 2010). Python is a scripting language which has variants for Windows Mobile and Symbian OS (Dwivedi, Clark & Thiel 2010). These development platforms allow users and third parties to create custom applications for mobile devices. The created applications are transferred onto the devices, then installed as is done with conventional PC software.

## 1.2 An Introduction to Mobile Malware

The developers of the malware need to release it into the open; this is known as distribution. The released malware then initially infects the targets and begins to replicate itself and propagate. Once the device is infected, the malware may activate a portion of the code that results in the infected device being affected; this is known as the payload.

Malware is categorised into different types, according to their replication, propagation, and payload characteristics. The definitions of mobile malware types are the same as that of traditional computer-based malware; namely (Dunham 2009):

- Virus – it infects files in order to spread.
- Trojan – it masquerades as something that appears legitimate; they usually do not spread (Dwivedi, Clark & Thiel 2010).
- Worm – it makes a copy of itself as it spreads. (Dwivedi, Clark & Thiel 2010).
- Spyware – these usually install themselves without user permission, and may result in pop-up messages or report user behaviour to a remote location.
- Garbage – the malware replaces files and applications with non-functional versions or garbage, leaving the applications useless, and in some case the device if important system files are replaced.

After the malware has been developed and distributed, some types attempt to replicate themselves and propagate through various means. Mobile malware has a number of communication technologies that may be used to propagate, which are described below (Morales 2009b; Dunham 2009):

- Short messaging service (SMS) – this could be a vector to entice users to download Trojans. The SMS services may also be used as an infection vector as the SMS contains a section which instructs mobile devices to perform certain actions, vulnerabilities in this may be exploited to install malicious code;

- Multimedia messaging service (MMS) – the MMS is used to carry the malware in order to propagate, and code in the MMS may exploit vulnerabilities on the device in order to install the malicious code. Some MMS malware requires users to install the infected file, which is a Trojan masquerading as a legitimate application such as a game;
- Email – as with traditional computer-based malware, emails can be a propagation method;
- Multimedia-card (MMC) – these cards form the removable storage media for many digital devices, most notably digital cameras and mobile devices, and therefore would make an ideal method for distributing and propagating malware;
- Bluetooth – malware can attempt to propagate using the Bluetooth services, and exploit vulnerabilities to infect devices. A disadvantage of this method is the relatively short range of Bluetooth, therefore this method is suited to heavily populated areas;
- Wireless networking – it may be possible to use the wireless network services on mobile devices to propagate or distribute malicious code, which may infect other devices and possibly wireless routers;
- Operating system (OS) vulnerabilities – traditional computer-based malware often exploits vulnerabilities in the OS, which appears also to be the case for mobile devices. These vulnerabilities allow the malware to infect the device;
- User installation – often the user is tricked into installing the malware;
- Device-to-PC synchronisation – the ability to synchronise data between a PC and a mobile device may allow malware to be propagated between the two.

Once the malware has infected the device, replicates itself and attempts to propagate, the payload is triggered. The payload it the portion of the mobile malware that consists of malicious code which may result in the device performing unauthorised or unexpected manner. Common payloads include (Morales 2009b):

- Sending SMS messages – the malware may attempt to propagate via

SMS, flood a specific phone or service provider by transmitting large quantities of messages, or send messages to premium-rated services which allow criminals to receive money. As this is often done without the user's knowledge, it may result in a large phone bill;

- Calls to premium-rate services – the malware makes calls to premium-rate services, which allows criminals to receive money, and may result in large phone bills for the user. The criminals receive their money as the calls are charged as if it is an international call, however the call is not routed all the way (called short-stopping), and the criminals get the difference in charges (Hyppönen 2010);
- Infect files – the malware infects files in order to replicate, and usually destroys the original contents of the file;
- Overwriting files – the malware replaces existing files with garbage, which may have additional consequences if they are system files for the device or applications;
- Deleting files – the malware deletes files, which may have additional consequences if they are system files for the device or applications.
- Stealing information – information about the device, such as the international mobile equipment identifier (IMEI) number, contacts or other information, such as location, may be retrieved from the phone, or the calls and messages may be monitored.

The next section discusses the trends in the characteristics of mobile malware.

## 2. Mobile Malware Trends

This section discusses trends of mobile malware since their first appearance, which is derived at from analysis of secondary data. Morales (2009b), Gostev (2006), and Gostev and Maslennikov (2009) list the descriptions of mobile malware families and variants for specific time periods; the trends of those descriptions are presented here. Trends in the following are discussed: the number of malware families and variants (Section 2.1); the popular platforms for mobile malware (Section 2.2); the common types of mobile malware (Section 2.3); the common payloads (Section 2.4); and the common propagation vectors (Section 2.5).

## *2.1 Mobile Malware Numbers*

Table 1 shows the number of malware families that were detected in the period of two reports. Whilst the time periods are not exactly the same, by 'normalising' the time frames to one year it can be approximated that there was a 78% increase in the number of new malware families detected in the second period, and a 15% increase in new malware variants.

**Table 1: Detected Malware Numbers per Report Release**

| | 2004 - Aug 2006 | Sept 2006 - Aug 2009 |
|---|---|---|
| Families | 31 | 75 |
| Variants | 170 | 302 |

**Source (Gostev 2006; Gostev & Maslennikov 2009)**

Figure 1 shows the newly detected malware families per year according to Morales (2009a), Gostev (2006), and Gostev and Maslennikov (2009). As these two sources are not perfectly consistent, the total family plot combines the two sets if figures by taking the larger of the two figures for each year to give an approximation.

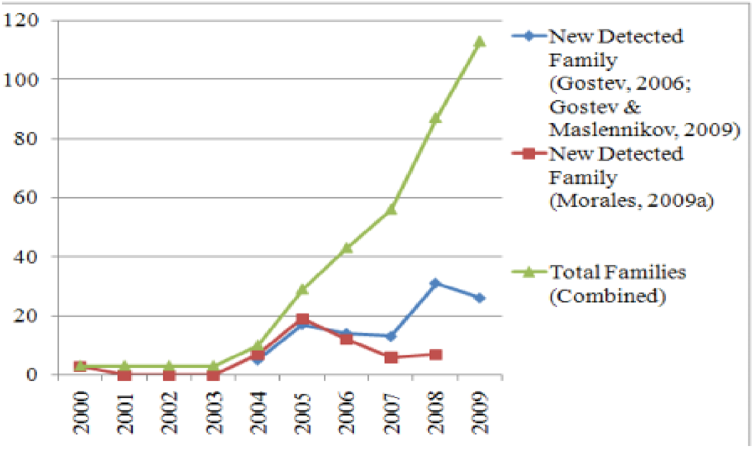

**Figure 1: Trends in Mobile Malware Family Numbers Source (Morales 2009a; Gostev 2006; Gostev & Maslennikov 2009)**

As can be seen both sources show similar trends. Gostev and Maslennikov (2009) show a more pronounced increase than Morales (2009a) as Morales' listing ends in July 2008, whereas there was a significant spike towards the end of 2008 which is accounted for by Gostev and Maslennikov. The two plots of new detected families show a general increase in the numbers of new malware families. The approximation of the total numbers of malware families is exhibiting an exponential growth rate; this is due to the ever-increasing new malware that is being developed each year.

Figure 2 shows the same trend for the newly detected variants of malware. There is a significant jump from the total numbers calculated from Morales (2009a) and McAfee (2011) in 2011.

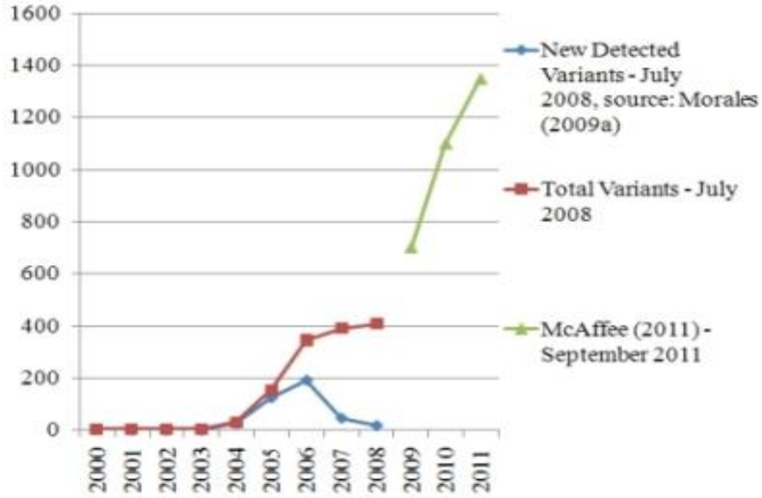

**Figure 2: Trends in Mobile Malware Variant Numbers, 2000 - July 2008 Source (McAfee 2011; Morales 2009a)**

As Morales' data is up to July 2008, the increase of new malware families detected in the latter part of 2008 mentioned above accounts for this to some degree. The plot for the total number of detected malware variants exhibits the same exponential growth as that of the total number of detected families in Figure 1. These growths in mobile malware numbers is to be expected due to the increasing 'intelligence' of the devices and their prevalence in society.

## *2.2 Mobile Malware Platforms*

Malware are usually developed to target a specific OS. Usually, the most common or popular OS will exhibit much more malware activity. As such, mobile malware is developed on various platforms: Figures 3 and 4 show breakdowns of mobile malware by platform for the period 2004 to August 2009 for the detected families and variants, respectively. As can be seen, the Symbian platforms receive the majority of malware activity, probably due to the fact that Nokia phones are so widespread. The J2ME platforms also exhibit significantly more malware activity than the other platforms.

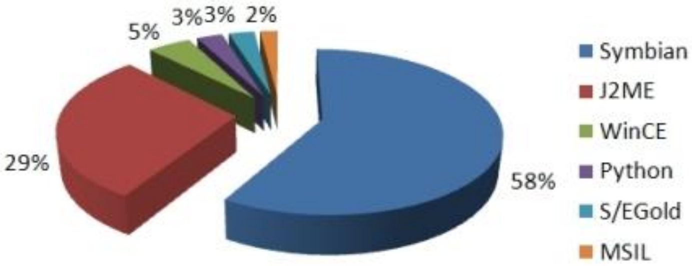

**Figure 3: Mobile Malware Families by Platform Source: (Gostev & Maslennikov 2009)**

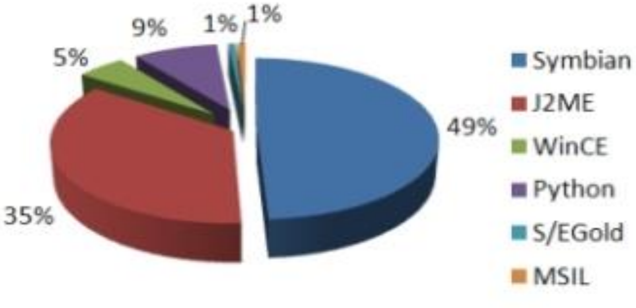

**Figure 4: Mobile Malware Variants by Platform Source: (Gostev & Maslennikov 2009)**

There is a recent shift towards malware for other popular systems not covered by the study by Gostev and Maslennikov (2009): Google's Android and the IPhone and IPad are experiencing new malware activity, whereas the majority of Symbian malware is from 2004 to 2006 (Hyppönen 2010). The malware for the iPhone is still restricted to phones that have been jailbroken (Hyppönen & Sullivan, 2010). Seriot (2010) lists four malware variants for the iPhone. The McAfee (2011) threat report also shows rapidly increasing malware numbers for the Android platform.

## *2.3 Mobile Malware Types*

Figure 5 shows a breakdown of the mobile malware variants detected from 2000 to July 2008 by type. As can be seen, the majority of variants are Trojans, which implies that most of the malware is distributed as another application which appears legitimate. Viruses are the second most common, which indicates those that are distributed and propagate by infecting files. Some malware families may have variants that are different types; for instance CommWarrior variants are primarily viruses, however variant B is a Trojan, and there are variants that are worms or are classed as garbage (Morales 2009a). Due to this, it is difficult to provide similar visual representation that is accurate for malware families.

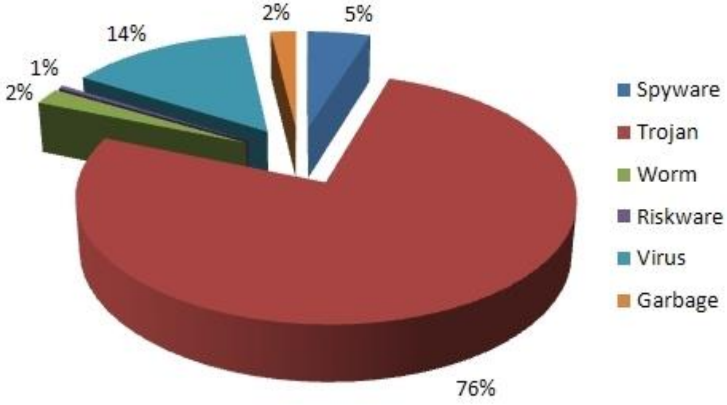

**Figure 5: Mobile Malware Variants by Type Source (Morales 2009a)**

As can be seen in Table 2, earlier forms of mobile malware variants were restricted to viruses and Trojans. In 2006-2007 new types were being introduced, in particular worms and spyware. As spyware attempts to compromise confidential information, it may be being used to attempt to compromise logon information for mobile banking accounts. Worms have also been detected for the iPhone and related devices (Seriot 2010).

**Table 2: Annual Trends for the Number of Malware Variations by Type**

| Malware Type | 2000 | 2004 | 2005 | 2006 | 2007 | 2008 | Total |
|---|---|---|---|---|---|---|---|
| Virus | 1 | 15 | 19 | 17 | 6 | 0 | 58 |
| Trojan | 2 | 11 | 105 | 160 | 23 | 10 | 311 |
| Worm | 0 | 0 | 0 | 0 | 2 | 7 | 9 |
| Spyware | 0 | 0 | 0 | 5 | 15 | 0 | 20 |
| Garbage | 0 | 0 | 0 | 8 | 0 | 0 | 8 |
| Riskware | 0 | 0 | 0 | 1 | 0 | 1 | 2 |
| Total | 3 | 26 | 124 | 191 | 46 | 18 | 408 |

**Source: (Morales 2009a)**

## *2.4 Mobile Malware Payloads*

Table 3 lists the number of detected malware families and variants with a given payload for the period 2004 to August 2006. As can be seen, the most common payload is to send SMS and replace, delete, or infect files. Morales (2009b) confirms these trends, and also adds that an 'indirect' payload is that the infected mobile device's battery is drained due to the increased activity of the Bluetooth and SMS services as the malware attempts to propagate. The SMS are usually sent to premium numbers, as discussed in Section 1.2. The majority of malware payloads is to provide financial benefit to the criminals (Hyppönen & Sullivan, 2010), hence the relatively large percentage malware that sends SMS. Similar payloads have been seen where the device makes calls to premium rate numbers; experts believe that these types of attacks are likely to get worse (Hyppönen 2010). Of those that send SMS, only one family (with four variants) propagates by SMS, and two families (with one variant each) are classed as SMS flooders. There is also the introduction of spyware, which can compromise information stored on the device; these may develop to target mobile banking applications. Of the four iPhone malware variants discussed by Seriot (2010), three stole data off the phone, and one behaved like a 'botnet' (Porras, Saidi, & Yegneswaran, 2009).

**Table 3: The Effects of Mobile Malware Payloads**

| Action | Families (%) | Variants (%) |
|---|---|---|
| Infects files | 4 (3.8) | 11 (2.1) |
| Sends SMS | 42 (39.6) | 237 (46.1) |
| Replaces files, icons, fonts, system apps | 15 (14.2) | 172 (33.5) |
| Installs additional malware/corrupted apps | 8 (7.5) | 44 (8.6) |
| Interferes with anti-virus | 5 (4.7) | 36 (7) |
| Disables or blocks functions, storage | 5 (4.7) | 9 (1.8) |
| Steals data, monitors calls & SMS | 9 (8.5) | 87 (16.9) |
| Deletes files, fonts, folders, contacts, messages etc | 8 (7.5) | 8 (1.6) |
| Interferes with phone booting/restarting | 3 (2.8) | 7 (1.4) |
| Nuisance (changes settings etc, fake system messages, fake anti-virus etc) | 7 (6.6) | 15 (2.9) |
| Makes calls to paid services | 2 (1.9) | 3 (0.6) |
| Other/unknown | 11 (10.4) | 13 (2.5) |

**Source (Gostev 2006; Gostev & Maslennikov 2009)**

## *2.5 Technology Used for Infection and Propagation*

Table 4 shows the technology used for malware detected between 2004 and August 2006. As can be see a very large proportion exploits OS vulnerabilities, file application programming interfaces (APIs), and Bluetooth.

Dunham (2009) shows that the majority of malware infections is due to the user allowing the malware to install, followed by Bluetooth, MMS and MMC, however it is also shown that users report a significantly higher rate of

Bluetooth and MMS infections, and a lower rate of user installation as a vector. A reason for this is that users do not want to accept responsibility for installing the malware, and therefore report the vector that was used to propagate it. Therefore the majority of malware reported from 2004 to August 2006 probably exploited the file APIs and OS vulnerabilities, but also relied on the gullibility or ignorance of many users to aid with the installation and infection. Files that have been infected may be shared amongst users, allowing viruses to propagate to additional devices. However, with the introduction of the mobile worms, there may be a shift to the malware spreading autonomously without user interaction.

**Table 4: Technology Used 2004 – August 2006**

| | **Families (%)** | **Variants (%)** |
|---|---|---|
| Bluetooth | 5 (16.1) | 33 (19.4) |
| File API | 8 (25.8) | 24 (14.1) |
| Network API | 2 (6.5) | 3 (1.8) |
| SMS | 2 (6.5) | 3 (1.8) |
| OS Vulnerability | 18 (58.1) | 124 (72.9) |
| MMS | 2 (6.5) | 12 (7.1) |
| Java | 1 (3.2) | 2 (1.2) |
| Email | 1 (3.2) | 3 (1.8) |
| Other/Unknown | 2 (6.5) | 3 (1.8) |

**Source (Gostev 2006)**

## *2.6 Summary*

The numbers of mobile malware are increasing exponentially; this is to be expected due to their prevalence in modern society. The malware targets popular devices; therefore Nokia's Symbian OS was initially the primary target. There has been a shift towards targeting Google's Android and the Apple iPhone and related devices. The vast majority of malware types is the Trojan; however there was an increase in the number of worms and spyware towards the period of study. The payload of the malware is mainly to send SMS messages to premium rate numbers to generate cash for criminal organisations, however there is a large number that are malicious and infect, delete, or destroy files on the device, which may leave it inoperable. The malware considered generally exploits vulnerabilities in the OS and file APIs, and the most commonly reported propagation vector is Bluetooth.

## 3. Emerging and Potential Future Trends

Recent malware attacks are beginning to closely follow PC-based malware; the Ikee.B iPhone worm formed a 'botnet', as is found in many PC-based malware (Porras, Saidi & Yegneswaran 2009). There is also a case where PC-based malware has migrated to mobile phones; the Zeus malware, which targeted internet banking, migrated to mobiles to target mobile banking (Kitten 2010). CNN hosted a war game called Cyber Shockwave to simulate how senior government in the United States would handle a major malware attack; the scenario was that malware was propagating through the mobile networks, disrupting service, and then migrated to the computer networks (Cable News Network 2010). This simulation was interesting in that a dual mobile/PC malware type could possibly be used in an information warfare attack, which will be very difficult to attribute to any single nation or organisation.

A case of mobile devices being used to distribute PC-based malware has already been seen in the United Kingdom; the malware installed itself on the PC when the device was connected, and stole the user's account passwords (Charette 2010). India has banned the import of Chinese-manufactured cell phone devices and infrastructure components over the concern of pre-installed malware (StrategyPage.com, 2010).

The application store for Android was found to have been used to distribute malware, where Trojans or other malware was uploaded in games and applications (Mitchell 2010). There is also an application store for the Apple iPhone and related devices, however Apple tests the applications prior to posting, whereas the Android application store posts the content, and withdraws it if there are any problems (Hyppönen & Sullivan 2010); this leaves Android platforms more vulnerable. A concern was raised where a new feature of the Android market allowed users to remotely install applications onto devices; this could potentially be put to malicious use (Maslennikov 2011). By August 2011, a number of malware variants had been discovered targeting

Android devices (Fisher 2001a; 2011b; 2011c; Roberts 2011; Westervelt, 2011). Nokia has also opened an application store, and there are a number of online stores for mobile content; these may provide a perfect method of distributing malware.

Another method of malware distribution which has not yet appeared is through the social networks. Many mobile devices have integrated applications for social networking; whilst PC-based malware has been developed for these websites, nothing has been seen for mobile devices. Due to the popularity of both the social networking websites and mobile devices, it may not be too long before the mobile malware uses social networks to propagate.

Security experts are concerned that an aggressive mobile worm will spread rapidly and disrupt cellular networks globally (Hyppönen 2010); a mobile equivalent of the SQL Slammer and Sasser worms that disrupted computer networks worldwide in 2003 and 2004, respectively. Even though there has been no major mobile-based pandemic, numerous nations, including South Africa, have had infections cases of notable malware, namely the Cabir and ComWar families (Gostev 2006b).

A recent development by Intel allows processors to be disabled remotely via SMS should the notebook or computer be stolen, known as a 'kill switch' (Roberts 2010). This may open an opportunity for a malicious attack where mobile malware intentionally attempts to trigger the kill switch by transmitting SMS; this may be used to launch an attack on computer infrastructure from mobile devices. The same 'kill switch' concept allows Google to remotely remove malicious applications off infected devices; this remote cleaning has been put into affect twice (Keizer 2011). Should any vulnerabilities in the technical implementation of the kill switch exist, future malware may be able to exploit this and maliciously wipe the contents of the phone. Research in Motion, who manufacture the Blackberry devices, provide a central enterprise server which has the ability to control and automatically update end-user devices; a vulnerability was discovered which may have resulted in the servers being ‘commandeered when handset users received images containing booby-trapped images’ (Goodin 2011). By taking control of the server, attackers could potentially 'push' malicious code to all end-user devices connected to the server.

Possible future evolution of smart mobile devices may see a common operating system between mobile, tablets, and PCs. Such an evolution could result in malware being developed which could easily migrate between and attack the full range of systems as the common operating system will result in common vulnerabilities.

## 4. Implications for Management

The potential impact of mobile malware on an organisation is as follows:

- Malware that disrupts the mobile device communication modules or floods the network will result in contact with mobile workforce being lost;
- Payloads that generate calls or SMS to premium rate numbers will result in direct financial loss to an organisation;
- Malware that provides backdoor access or steals information from the device could result in a breach of sensitive organisational data;
- Compromised enterprise servers for the mobile devices could potentially result in all of the above, as malicious applications could be 'pushed' onto the phones, the communications could be blocked, and sensitive data retrieved;
- An infected mobile device that is connected to a computer inside the organisational network may result in the computers becoming infected (as discussed under the emerging trends).

As mobile devices are 'outside' of the traditional computer-based network, it is difficult to control the user's actions on the mobile devices, and difficult to ensure the relevant security measures are in place. Whilst the use of mobile devices may be restricted and controlled through the use of the enterprise servers (such as the Blackberry Enterprise Servers), this does not aid in controlling personal devices that may be introduced into an organisational environment. Lopez (2010) indicates that policies usually prohibit organisational data being accessed on personal devices; however employees may find many workarounds to these restrictions, such as forwarding company emails to their personal email addresses.

A possible method of ensuring personal mobile devices are prevented from accessing the corporate network is to employ IP address filtering; when users wish to gain access they are required to register their devices, and demonstrate basic security measures are in place, such as a mobile anti-virus application, and a pin code or passwords to lock the device (van Niekerk 2011). For organisation-provided devices, access should be restricted to social media, application stores, and entertainment websites as these may be used to distribute mobile malware. These devices may be 'pre-loaded' with anti-malware and firewall applications and restrictions prior to them being distributed to the employees.

A number of legal concerns may arise from allowing personal mobile phones onto the corporate network. If malware results in a data breach of corporate information from a personal device, it may be difficult to determine responsibility and accountability; however the organisation may be held liable if there are insufficient policies or measures in place to prevent employees from accessing the information. Privacy legislation, such as the Protection of Personal Information Act (POPI 2009) in South Africa, require certain measures to be in place

The organisation may be prevented from checking personal devices due to privacy concerns, as many laws prohibit accessing or jamming of electronic communications, such as the Electronic Communications and Transactions Act (ECT 2002) and the Regulation of Interceptions of Communications Act (RICA 2002) of South Africa and the Electronic Communications Privacy Act (ECPA 1986) in the United States. Checking devices provided by the organisation may also be limited in that features may not be used that could compromise the employee's privacy. In 2010 a suit was filed against a school in the United States when they remotely activated the webcams on laptops they had provided to students and captured images of the students in their bedrooms (Staglin 2010). Similarly, remotely activating features on laptops or other mobile devices may infringe on the employee's privacy.

Awareness training directed towards informing employees about the malware and security risks of 'smart' mobile devices will empower them to secure both organisation-owned and their personal devices. Senior executives should not be exempt from this awareness training; they are most likely to be using 'smart' mobile devices, and they have greater access to sensitive organisational information. The training should aid employees in identifying malicious application or messages that may contain malware, and create awareness of the mobile anti-virus applications that are available. This can be encompassed in a general information security training session, were awareness of the risks of using the Internet, email, social networks, and mobiles is explained. This will enable employer's to illustrate the legal ramifications to the employees; and in doing so this may reduce the organisation's liability regarding breaches, but increase the liability of the employee as an individual.

## 5. Conclusion

Due to the pervasiveness of mobile devices in society, malware developers began targeting these platforms. This paper presented trends in the listing of malware characteristics for the period of 2000 to August 2009, and describes possible future trends. During this period, the number of detected mobile families and variants was seen to increase exponentially. Popular platforms were targeted by malware developers, therefore the Symbian OS has seen the majority of malware activity; however, there is a shift towards Android and iPhone platforms. The most common malware type is the Trojan, with worms and spyware making an appearance from 2006.

The malware typically either is intended to be a source of profit for criminal organisations by sending SMS messages to premium rate numbers, or is malicious and interferes with files and applications on the mobile device. There is a rise in malware where information is stolen and messages and calls can be monitored. Bluetooth, file APIs, and OS vulnerabilities are the primary methods that malware employs to infect devices; however, there seems to be some reliance on user's to install the malware. With the introduction of mobile worms, there may be a rise in 'self-propagating' mobile malware.

The future may see an increase in malware distribution through online applications stores, and possibly a shift towards mobile malware on social networking websites and applications. Mobile devices may also be used to distribute PC-based malware, and there may be increased migration between PC-based and mobile malware. Security experts are concerned that a mobile worm could spread rapidly and disrupt cellular communications globally. Should such a pandemic occur, it is likely that South Africa will be affected, as two of the most notable mobile malware families have been found in the country. The advent of the remote 'kill switch' technology, which Google uses to remove infected applications from devices, may result in additional vulnerabilities which could be exploited to maliciously wipe legitimate functionality off the mobiles. Future evolutions of operating systems may result in coders producing malware with the capability of infecting the full range of computer and mobile systems.

In the management of information security, mobile malware is still a new and developing threat. This threat has a number of implications from the management of network access control to legal liabilities. Employers are required to ensure that private or sensitive information is not breached due to mobile devices, and the networks are now more vulnerable to malware infection from the inside. Awareness training, device registration, and filtering may be employed to restrict access and limit infections and subsequent data breaches.

**Acknowledgements**

The first author has received grants from the South African Department of Defence and Armscor Ledger Program through the Cyber Defence Research Group at the Council for Scientific and Industrial Research, Defence, Peace, Safety and Security (CSIR-DPSS), and the University of KwaZulu-Natal for his PhD research, from which this paper originates. This paper is part of the requirements for the Postdoctoral Scholarship awarded by the University of KwaZulu-Natal.

## References

Cable News Network 2010. We Were Warned. Cyber Shockwave. February 20 2010. Available at: http://transcripts.cnn.com/TRANSCRIPTS/1002/20/se.01.html. (Accessed on 01 October 2010.)

Charette, R. 2010. First Energizer, Now Vodaphone: More Malware Found in Store Bought Consumer Electronic Products. IEEE Spectrum Riskfactor Blog, March 10 2010. Available at: http://spectrum.ieee.org/riskfactor/computing/it/malware-found-in-store-bought-consumer-electronics. (Accessed on 03 May 2010.)

Dunham, K. 2009. Introduction to Mobile Malware. In Dunham, K. (ed.): *Mobile Malware Attacks and Defense*. Burlington: Syngress Publishing.

Dwivedi, H., C. Clark & D. Thiel 2010. *Mobile Application Security*. New-York: McGraw-Hill.

ECPA 1986. *Electronic Communications Privacy Act. 18 U.S.C. §2510-2522*. Washington, D.C.: United States Congress.

ECT 2002. *Electronic Communications and Transactions Act. Act 25 of 2002*. Pretoria: Government of South Africa.

Fisher, D. 2011a. Malware-Infected Apps Yanked from Android Market. Threatpost.com, 2 March 2011. Available at: http://threatpost.com/en_us/ blogs/malware-infected-apps-yanked-android-market-030211. (Accessed on 03 March 2011.)

Fisher, D. 2011b. SMS Trojan Found in Several Android Apps. Threat-post. com, 12 May 2011. Available at: http://threatpost.com/en_us/blogs/ sms-trojan-found-several-android-apps-051211. (Accessed on 16 May 2011.)

Fisher, D. 2011c. New SMS Trojan Targeting Android Users. Threatpost.com, 11 July 2011. Available at: http://threatpost.com/en_us/blogs/new-sms-trojan-targeting-android-users-071111. (Accessed on 12 July 2011.)

Goodin, D. 2011. Smartphone Images can Hijack BlackBerry Servers. The Register, 11 August 2011. Available at: http://www.theregister.co.uk/ 2011/ 08/11/blackberry_high_severity_bug/. (Accessed on 12 August 2011.)

Gostev, A. 2006a. Mobile Malware Evolution: An Overview, Part 1. SecureList, 29 September 2006. Available at: http://www.securelist.com/ en/analysis/200119916/Mobile_Malware_Evolution_An_Overview_Part _1. (Accessed on 07 December 2010.)

Gostev, A. 2006b. Mobile Malware Evolution: An Overview, Part 2. SecureList, 26 October 2006. Available at: http://www.securelist.com/en/ analysis/201225789/Mobile_Malware_Evolution_An_Overview_Part_2. (Accessed on 07 December 2010.)

Gostev, A. & D. Maslennikov 2009. Mobile Malware Evolution: An Overview, Part 3. SecureList, 29 September 2009. Available at: http://www. securelist.com/en/analysis?pubid=204792080. (Accessed on 07 December 2010).

Hyppönen, M. 2010. F-Secure Mobile Security Review September 2010. FSecure News You Tube Channel, 11 October 2010. Available at: http://www.youtube.com/watch?v=fJMLr8BDQq8. (Accessed on 13 December 2010.)

Hyppönen, M. & S. Sullivan 2010. Security Review May 2010: Mobile Phone Security. FSecureNews YouTube Channel, 12 May 2010. Available at: http://www.youtube.com/watch?v=4xi9SdSXIl8. (Accessed on 13 December 2010.)

iPhoneBlogr 2010. Greenpois0n Tutorial – How To Jailbreak iPhone 4, 3GS, iPod Touch 4G, 3G, 2G and iPad. iPhoneBlogr, 12 October 2010. Available at: http://iphoneblogr.com/2010/10/how-to-jailbreak-4-1-with-greenpois0n-tutorial/. (Accessed on 14 December 2010.)

Keizer, G. 2011. Google Throws ‘Kill Switch’ on Android Phones. Computerworld, 7 March 2011. Available at: http://www.computerworld. com/s/ article/9213641/Google_throws_kill_switch_on_Android_phones. (Accessed on 10 August 2011.)

Kitten, T. 2010. Zeus Strikes Mobile Banking. BankInfoSecurity.com, 13 October 2010. Available at: http://www.bankinfosecurity.com/articles. php?art_id=3005&rf=2010-10-16-eb. (Accessed on 18 October 2010.)

Lopez, M. 2010. IT Best Practices: Mobile Policies and Processes for Employee-owned Smartphones. Lopez Research. April 2010. Available at: http://us.blackberry.com/business/leading/IT_Best_Practices-_Mobile _Policies_and_Processes_for_Employee-owned_Smartphones.pdf. (Accessed on 10 February 2012.)

Maslennikov, D. 2011. The Dark Side of the New Android Market. Threatpost.com, 4 February 2011. Available at: http://threatpost.com/ en_us/blogs/dark-side-new-android-market-020411. (Accessed on 07 February 2011.)

McAfee Labs 2011. McAfee Threats Report: Third Quarter 2011. Available at: http://www.mcafee.com/uk/resources/reports/rp-sda-cyber-security.pdf? cid=WBB048. (Accessed 09 February 2012.)

Mitchell, S. 2010. Spy Tool Highlights Android App Store Security Issues. PC Pro, 17 August 2010. Available at: http://www.pcpro.co.uk/ news/ security/360370/spy-tool-highlights-android-app-store-security-issues# ixzz0x20ZTgJK. (Accessed on 19 August 2010.)

Morales, J.A. 2009a. Timeline of Mobile Malicious Code, Hoaxes, and Threats. In Dunham, K. (ed.): *Mobile Malware Attacks and Defense*. Burlington: Syngress Publishing.

Morales, J.A. 2009b. Taxonomy of Mobile Malware. In Dunham, K. (ed.): *Mobile Malware Attacks and Defense.* Burlington: Syngress Publishing.

POPI 2009. *Protection of Personal Information Bill. Bill 9 of 2009.* Pretoria: Government of South Africa.

Porras, P., H. Saidi & V. Yegneswaran 2009. An Analysis of the iKee.B (Duh) iPhone Botnet. SRI International, 21 December 2009. Available at: http://mtc.sri.com/iPhone/. (Accessed on 15 November 2010.)

RICA 2002. *Regulation of Interception of Communications and Provision of Communication-Related Information Act. Act 70 of 2002.* Pretoria: Government of South Africa.

Roberts, P. 2010. New Intel Chips Support SMS Kill Switch. ThreatPost.com, 20 December 2010. Available at: http://threatpost.com/en_us/blogs/new-intel-chips-support-sms-kill-switch-122010. (Accessed on 23 December 2010.)

Roberts, P. 2011. Google: Spyware Found, Removed from Android Market. ThreatPost.com, 13 June 2011. Available at: http://threatpost.com/en_us/blogs/google-spyware-found-removed-android-market-061311. (Accessed 21 June 2011.)

Seriot, N. 2010. iPhone Privacy. Black Hat DC 2010 Conference, Arlington. Available at: http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives. Html. (Accessed on 26 June 2010.)

Staglin, D. 2010. School District Accused of Spying on Kids via Laptop Webcams. USA Today. 18 February. Available at: http://content.usatoday.com/communities/ondeadline/post/2010/02/school-district-accused-of-issuing-webcam-laptops-to-spy-on-students/1. (Accessed on 20 February 2012.)

StrategyPage.com 2010. India Bans Chinese Cell Phones. StategyPage.com, 2 May. Available at: http://www.strategypage.com/htmw/htiw/articles/20100502.aspx. (Accessed on 03 May 2010.)

van Niekerk, B. 2011. *Vulnerability Assessment of Modern ICT Infrastructure from and Information Warfare Perspective.* PhD Thesis. Durban: University of KwaZulu-Natal.

Westervelt, R. 2011. New Android Phone Malware Indicates Transition to Mobile Platform Attacks. SearchSecurity, 12 July. Available at: http://searchsecurity.techtarget.com/news/2240037695/New-Android-phone-malware-indicates-transition-to-mobile-platform-attacks. (Accessed on 14 July 2011.)

Brett van Niekerk
School of Management, IT and Governance
University of KwaZulu-Natal
Durban, South Africa
vanniekerkb@ukzn.ac.za

Manoj S Maharaj
School of Management, IT and Governance
University of KwaZulu-Natal
Durban, South Africa
maharajms@ukzn.ac.za