westcoast labs

Test Report October 2011

NetQin Custom Test Test Report

NetQin Mobile Security - Test Report

WCL Corporate Offices and Test Facilities

USA Headquarters and Test Facility

West Coast Labs, 16842 Von Karman Avenue, Suite 125, Irvine, CA 92606, U.S.A. Tel: +1 (949) 870 3250, Fax: +1 (949) 251 1586

European Headquarters and Test Facility

West Coast Labs, Unit 9 Oak Tree Court, Mulberry Drive, Cardiff Gate Business Park, Cardiff, CF23 8RS, UK.
Tel: +44 (0) 29 2054 8400, Fax: +44 (0) 29 2054 8401

Asia Headquarters and Test Facility

West Coast Labs, A2/9 Lower Ground Floor, Safdarjung Enclave, Main Africa Avenue Road, New Delhi 110 029, India. Tel: +91 (0) 11 4602 0622, Fax: +91 (0) 11 4602 0633

Date: 24th October 2011 **Version:** 2.0

Authors: Michael McMenamin, Richard Thomas, Mark Thomas, Matt Garrad, Chris Thomas

NetQin Mobile Security - Test Report

Contents

NetQin Mobile Security - Test Report

Introduction

The Evolution of Mobile Security Technology – Satisfying User Needs

Mobile phones are not simply phones anymore. Increasingly people view so-called "dumb phones" as a relic, as quaintly simplistic. What use is a phone that can only allow you to hear another person's voice? Now, you can reach out and "touch" someone on your phone via voice, SMS, MMS, corporate or personal email, social networking sites, or any of a number of Internet enabled applications. Almost any functionality that is available on a PC is now available on a modern smartphone. But with this interconnectedness and unprecedented power comes increasing exposure and vulnerability to security threats.

To address this, a number of security vendors have developed applications for consumers and corporate users to protect themselves, their privacy, and their data. They are complex security suites, which allow users to block malicious software, prevent phishing or spam messaging, and often provide features such as remote data wipe (for lost or stolen phones) and firewall functionality.

Central to most of these security solutions is anti-malware technology, which is designed to deal with the most prevalent of all the mobile security threats.

Hence, an understanding of these threats, as well as the available protection technology, is central to choosing the solution best suited to one's needs – whether as a corporate user or as an individual consumer.

The Evolution of Mobile Malware

If malware authors can be relied on for one thing, it is that they will always explore the potential for taking advantage of popular new technologies. Where ever people and technologies go, so goes malware. In the past, initial forays by malware authors into new technologies have invariably been exploratory and proof-of-concept, more for bragging rights than for financial gain. In time, new malware becomes more robust, more complicated and more financially lucrative. History shows that, in the evolution of every new technology, it is at the point that malware development, distribution and exploitation is proven profitable that it experiences exponential growth.

That point seems to have arrived for mobile platforms.

NetQin Mobile Security - Test Report

Introduction

As a matter of simplicity, mobile malware began life as purely text-based, utilizing vulnerabilities within SMS and MMS protocols. Malicious URLs and Bluetooth connections were used to spread early worms. This is because, at the time, malicious URLs were also becoming a popular threat vector in the traditional PC arena and Bluetooth vulnerabilities were being widely discussed in security and hacking circles. In time, the focus of the delivery of malware shifted to downloadable applications as these had an explosion in popularity across all smartphone platforms.

Most of the early, non-financially motivated attempts at developing mobile malware occurred on Symbian's operating system. Proof of concept code, a few file-infecting viruses and quite a few static viruses and trojans were created. Because mobile malware gained momentum so slowly, a large number of variants exist in a moderately small number of malware families. For that reason, and until recently, the bulk of the existing malware was written for Symbian. As the market has evolved, focus has shifted and now other operating systems, in particular Android, are the primary focus of new malware creation.

History of Mobile Operating Systems

It is difficult to describe the path of the popularity of smartphones the world over, as it has gone in waves in different regions. NetQin reports that smartphone use in Asia and Europe was much more prevalent, as their cell phone network evolved more quickly. Symbian became the first popular mobile operating system among users in these areas, where the first mobile malware was seen years before it became a worldwide issue.

Arguably, the next popular OS was RIM’s Blackberry, which is popular primarily with corporate users, but it was also built with security in mind and to this day there are few true malware samples which are available for Blackberry. Application markets gained steam with Blackberry, but once again the model for delivery was a closed one in which new software had to be vetted before it became available for download.

With the introduction of the iPhone and iOS, smartphones hit the mainstream. Combining the new technology with a series of clever marketing campaigns, everyone from the boardroom to the classroom “had to have” an iPhone. Mobile applications became wildly popular, and Apple's advertising slogan "There's an app

NetQin Mobile Security - Test Report

Introduction

for that" has become a catch phrase to describe the incredible variety of applications available for people to use.

Android OS took this popularity a step further, addressing the still somewhat closed nature of the app markets of most other operating systems. As Android OS is not locked to any one vendor's hardware or any one (or two) cell phone network(s), smartphones became more affordable and approachable for the average home user as well as people in smaller businesses. The app market in Android is totally open and unvetted, and its developer kit is offered free of charge, which makes it an ideal target and development environment for malware authors. Indeed, this has been exactly what has occurred, with Android malware experiencing robust growth in a short timeframe. Google (the developers of the Android OS) does take down malware as it's discovered, but this does not stop malware from being created or distributed.

When one has completed programming an Android application, its code does not need to go through any approval process in order to be available to the public, unlike the varying levels of approval used in the Windows Mobile, Blackberry or iPhone markets. This has led to the popular practice of repackaging Android applications. This repackaging can be strictly malicious in intent (e.g. including damaging or spying modules in a popular existing package) or it can be more “grey” in intent. For instance, some developers have begun including adware modules within existing packages, viewing this as an easy way to make money off the efforts of others.

Windows Mobile has little market share at this point, but this may change as Nokia has moved their handsets to this operating system from Symbian. However, it remains to be seen whether or not the joint forces of Microsoft and Nokia can make this a successful, widely accepted platform and thus a prime target for malware authors. That said, some financially motivated malware has already been discovered for this OS, so time will tell whether or not their numbers increase.

As far as overall OS market share is concerned, much is dictated by the volumes of smartphones shipped by the major manufacturers – it’s a very fluid market. Strategy Analytics recently confirmed that despite the switch in OS, Nokia have suffered what they describe as a dramatic collapse in their smartphone market share with the

NetQin Mobile Security - Test Report

Introduction

Finnish company falling to third place behind Apple (20.3 million) and Samsung (19.2 million) for handsets shipped during Q2 2011 out of a total shipped globally of 110 million units. For Nokia, that represents a drop from 23.8 million in Q2 2010 to 16.7 million in Q2 2011 and less than half of what its market share was in 2010. Statistics aside, there is no question that the Android platform will soon take the dominant share of the global smart phone market.

China – The Origins of Threats and Technologies

"Mobile" security is unique, in that one specific region of the world has had tremendous influence to date on not only growth of security threats, but also the prevention of these threats. A large number of mobile threats and products alike originate in China.

Over the last five to ten years, traditional PCs and laptops have been too expensive for the average Chinese consumer. Because of this, China's users have turned to the smart phone not only for voice communication, but also to replace, or to act in lieu of, the functionality of traditional PCs. With hundreds of millions of smartphone users comprising their target user base, China has become the world's ripest breeding ground for malware authors creating mobile threats. NetQin have stated that their figures show, even today, nearly 65% of all new mobile security threats originate in China.

Due to China's user base and the increasingly sophisticated risk profile which this generates, it is important to note particular differences in malware and in anti-malware products in China.

Given this "head start" brought on by sheer demand, anti-malware products researched, developed and engineered in China are some of the most full-featured and technologically advanced products in the burgeoning mobile security market. For instance, some Chinese vendors are already taking advantage of Cloud Technology to analyze and identify malware code, prior to users even executing the Trojan application in which it is embedded in. This sophistication can be likened to providing a vaccination to prevent disease as opposed to medicating a patient after they have been infected.

NetQin Mobile Security - Test Report

Introduction

Predictions – The Future Evolution of Mobile Security

No mobile phone OS has been ignored by malware authors in recent months. A variant of the prolific Zeus botnet family has targeted all major mobile phone OSes, stealing bank passwords and checking in to a command and control channel.

Each OS has its own malware behavioural trends to be aware of. Based on the structure of the operating system, its target market and its application market policies, different types of malware become specific concerns for each operating system.

Blackberry and iPhone apps are both vetted restrictively, but this does not stop people from creating programs which could also be considered 'potentially unwanted' tools or software. Both OSes have spyware-type applications which are available for purchase, which allow a remote user to gather data or listen to calls on an affected phone.

"Jailbreaking" iPhones is a popular way to get around restrictive app markets, for those who wish to customize their phone more than is allowed by default. But with this power comes danger – many proof of concept pieces of malware have been created which target jailbroken (or jailbreak'd) iPhones. Many of these are pranks rather than destructive attacks. However, now that financial motives have come to all mobile platforms, this is likely to change rapidly.

While most new malware threats are found on Android, Symbian OS still has its share of new malware like Zitmo, trojanized apps such as those popular on Android can also be found on Symbian. Windows Mobile was also recently targeted with a trojanized app which makes calls to premium-rate phone numbers.

Choosing a security solution

As mobile malware is a relatively new issue to new smart phone adopters, and therefore only recently the subject of awareness by the broader consumers market about mobile security products, how should one go about choosing a product which meets one's needs? There are a number of potential options to consider, similar to choosing a security product for a PC.

NetQin Mobile Security - Test Report

Introduction

In order to adequately assess risk on a user's smartphone, each individual or company must assess how they use their handsets. Is personal or corporate privacy important? Is there sensitive or proprietary data on the phone? Is the device used for online banking or shopping? What kinds of apps are, or might be, used or downloaded? Will a child have access to the phone? Once these questions are answered and any specific needs identified, the examination of results of neutral and independent third party tests is essential in determining which products make best use of the existing technologies. The two key areas for users to examine are: 1) the effectiveness (e.g. ability to detect malware, speed, data consumption, and reliability) of the scan engine, and 2) the robustness of the feature set of the overall offering.

Industry leading mobile security products, rather than being simple virus signature scanners or application behaviour monitors (e.g. identifying a virus just by its code or its action after installation), are now feature rich suites, providing users with the ability to block threats before they are installed, or stop malicious URLs before they are opened.

We are already beginning to see vendors taking holistic approaches to mobile security, and incorporating such features as remote lock/track and contact backup/restore. Privacy controls are being integrated, which alert users as to which applications have access to their personal contacts, can automatically send SMSs, or can track their location. No doubt as more parents give their children phones, you may find security suites incorporating more parental controls and behaviour logging functionalities.

Mobile security products will undoubtedly be an exciting space to watch, providing innovative and creative solutions to both personal and corporate users.

NetQin Mobile Security - Test Report

Test Objectives

NetQin commissioned West Coast Labs to carry out the following testing:

- Checkmark Certification testing on NetQin Mobile Security.
- Comparative testing of the selected NetQin products against a range of competitor products in a “static” test environment (see following page).
- A comparison of product feature sets using publicly available information on vendor websites and marketing collateral.

The NetQin applications included in the test program are:

- NetQin Mobile Security
- NetQin Mobile Manager (for feature comparison only)

A list of all NetQin Checkmark Certifications can be found on page 30.

NetQin Mobile Security - Test Report

Test Objectives

For the *Comparative Testing* and the *Comparison of Product Feature Sets*, a number of tests and a selection of comparable competitor products were identified by NetQin. These were purchased in the way that any ordinary user would buy them – from the Google Market, and directly from vendor websites. They are detailed below.

Product	Version	Obtained via	Date
NetQin Mobile Security	5.0.02.02	Email	14/07/11
BullGuard Mobile Security 10	10.0.21	Download	22/07/11
Kaspersky Mobile Security 9	9	Download	19/07/11
AVG Mobilation	2.8.1	Download from Google Market	18/07/11
F-Secure Mobile Security	7.1.6762	Download	19/07/11
Norton Mobile Security	2.1.0.272	Download from Google Market	18/07/11
Lookout Mobile Security	6.2	Download from Google Market	19/07/11
McAfee WaveSecure	4.2.0.4	Download from Google Market	18/07/11

Testing was conducted between 19/07/11 and 10/08/11.

NetQin Mobile Security - Test Report

Comparative Product Testing – Test Overview

The comparative testing comprised a basic evaluation of malware detection comprising of two test suites: a suite of 75 samples built from WCL's own collection and based on the Mobile Anti-Malware Checkmark test suite, and a suite of 129 infected, or otherwise potentially unwanted programs, and 33 clean samples sourced from WCL's various industry resources.

Further collections were also built at NetQin's request; 5 samples for SMS URL malware scanning, and 5 for the real time installation testing. A manual installation test was also carried out, with 50 malicious or potentially unwanted applications being tested against each solution.

Each solution was installed to a HTC Desire Z handset running Android 2.2. During installation, WCL noted how the installation was performed, as well as whether or not the licence agreement displayed.

Each solution was updated to the latest available definition, engine, and signature releases before testing began on 19/07/11. Static scans were run against two of the collections built for the purpose, as well as a scan using any Cloud Scanning components, where available.

Each solution's Anti-Loss and Remote Wipe features were tested where available. The former was tested for time to locate, as well as location accuracy, time to sound the alarm, and time to lock the handset. The latter was tested for time to wipe the handset, and the handset was forensically inspected afterwards for any remaining data such as Contacts, SMS messages, and user data on the SD card.

Each solution's Account Backup features were also tested for the ability to back up contacts to different locations such as a server or SD card. The restore abilities were also tested to ensure complete restoration of contact data to the handset.

NetQin Mobile Security - Test Report

Comparative Product Testing – Test Overview

Further testing comprised of SMS URL scans, in which engineers would send an SMS containing a link to a suspect application and then proceed to download the application and install it from that link. This test was combined with the real-time protection scanning portion of the testing as suggested by NetQin to replicate as closely as possible a "real-world" scenario. A collection of 10 samples was used, split evenly between the two tests, as well as a further 50 samples for manual installation.

The final part of the main comparative testing was the un-install tests, where engineers noted the result of each solution's uninstallation.

Comparative Product Testing – Test Network

Testing was carried out on mobile handsets within a secure environment at WCL's European Headquarters.

In order to provide a balanced reporting process, West Coast Labs recommended that all handsets should be of the same brand and be running the same Android OS version. The OS version was Android 2.2 and the handsets were all HTC Desire Z.

In some cases this meant that they may not have been running on the latest version of a particular operating system, but this method meant that any testing carried out was directly comparable. Each handset was also equipped with a SIM card from the same UK-based mobile carrier (O2).

NetQin Mobile Security - Test Report

Comparative Product Testing – Test Methodology

In each test case, the function of each solution most likely to be used was employed to test the solutions – these are detailed as below.

Installation: WCL installed each application in an appropriate manner, and where possible, obtained .apk files. Specifics are documented in the test results section.

Licence Agreement: WCL noted which solutions displayed a licence agreement, and whether or not, when selected, the licence agreement only displayed once.

Account Backup: WCL created a custom list of fake contacts to use for this test. This list was then duplicated to all handsets. The contacts were backed up to any available location (server, SD card etc,) then deleted from the handset. A restore action was then performed to check that details were restored accurately in their given locations.

Uninstall: WCL uninstalled each solution and checked to see the ease with which this occurred, and also to ascertain if any remnants were left behind.

Malware Scanning: WCL tested each solution's ability to detect malicious and potentially unwanted applications in their raw formats. Each suite was comprised of apk files, jar files, and infected mobile applications embedded in zip files. Clean files were also included for false positive checks. The scan was run in three stages. The first stage was scanning the suite based on Checkmark samples. The next was scanning an expanded suite that contained samples from WCL's Checkmark suite as well as a selection of samples from WCL's industry sources. Finally, both collections were scanned with a Cloud component enabled where available.

NetQin Mobile Security - Test Report

Comparative Product Testing – Test Methodology

SMS URL Scanning: For this, WCL selected a small subset of 5 samples from the above collections and hosted them on a web server. A URL link to each of the samples was then sent via SMS message to each handset in turn. Each link was then selected, and the file downloaded and installed to check the solution's ability to detect threats over this infection vector.

Real-Time Protection: Each solution's real-time protection features were tested using a small subset of samples from the main collections. Each sample was installed manually onto the handset via the SDK.

Anti-Loss: To test the anti-loss features of each solution, WCL removed the handset (which was free from malware at this point) to a location at a minimum distance of 100 metres from the laboratory, and then activated a “locate” command. This was performed via SMS and via a website when available. The time taken, and accuracy of the data returned to the handset were then recorded. These figures have some margin of error due to different factors such as network signal strength and connection speeds. The next portion of this test involved WCL sending an “alarm” command, and results were recorded for speed of activation as well as functionality. The final test for this section involved activating the “lock” command. This was tested for speed of activation, as well as security of the locking feature.

Remote-Wipe: WCL tested this feature by building a collection of common files. These included MP3s, jpgs, xls, docs, and some zip files. WCL also sent SMS messages, and used the custom contact list created for the Account Backup testing, as well as Google Account login details. A remote wipe command was then sent to each solution, and WCL tested for speed of time to wipe, as well as the thoroughness of the action. SMS, contacts, Google accounts details, and the SD card were then all forensically inspected, and the results recorded.

NetQin Mobile Security - Test Report

Comparative Product Testing – Test Results

The following section contains the results for all testing conducted as part of this report. Although anonymised within the results tables, the product versions used in this test were as follows:

- NetQin Mobile Security version 5.0.02.02
- BullGuard Mobile Security 10 version 10.0.21
- Kaspersky Mobile Security 9 version 9
- AVG Mobilation version 2.8.1
- F-Secure Mobile Security version 7.1.6762
- Norton Mobile Security version 2.1.0.272
- Lookout Mobile Security version 6.2
- McAfee WaveSecure version 4.2.0.4
- McAfee Mobile Security version 1.0.0.31

Please note that the product list order above does not correlate to the following results tables.

NetQin Mobile Security - Test Report

Comparative Testing – Test Results – General Use

Installation

Solution	**NetQin Mobile Security**	**Product A**	**Product B**	**Product C**
Purchased via	N/a	Company website	Company website	Google Market
Download from	N/a	Company Website	Company Website	Google Market
Install method	Local apk file	Local apk file	Local apk file	Automatic
Also available	Google Market	Google Market	Google Market	N/a
	Product D	**Product E**	**Product F**	**Product G**
Purchased via	Company Website	Google Market	Company Website	Company Website
Download from	Company Website	Google Market	Google Market	Google Market
Install method	Local apk file	Automatic	Automatic	Automatic
Also available	Google Market	N/a	N/a	N/a

A review of the solution provision and installation methods showed that the security vendors would all follow one of three methods. Either the product is purchased and downloaded directly from the vendor's website, purchased and thus installed automatically using Google Market, or purchased from the vendor's website with a link enabling the download from Google Market.

Those vendors, such as NetQin, that provide multiple options for purchase or download should be of extra help to prospective customers.

Comparative Testing – Test Results – General Use

License Agreement

Solution	NetQin Mobile Security	Product A	Product B	Product C
Displayed on first user	Yes	Yes	Yes	Yes
Display on first-run only	Yes	Yes	Yes	Yes
	Product D	**Product E**	**Product F**	**Product G**
Displayed on first user	Yes	Yes	Yes	Yes
Display can be disabled	Yes	Yes	Yes	Yes

There are a few interesting approaches to the "first-run" scenario. Most solutions under test favour the quicker approach of selecting an agreement box and continuing into the main area of the product. Other applications allow first time users to see everything the application is intended for without having to navigate through menus themselves.

NetQin Mobile Security - Test Report

Comparative Testing – Test Results – General Use

Account Backup

Solution	NetQin Mobile Security	Product A	Product B	Product C
Can backup data	Yes	Yes	No	Yes
Backup location	SD or server	Server	n/a	Server
Activate restore from	Handset	Website	n/a	Website
Restore successful	Yes	Yes	n/a	No
	Product D	**Product E**	**Product F**	**Product G**
Can backup data	No	No	Yes	Yes
Backup location	n/a	n/a	Server	Server
Activate restore from	n/a	n/a	Website	Website
Restore successful	n/a	n/a	Yes	Yes

Testing has shown that there is a variety of ways this particular technology is employed by each solution. For those that contain such a technology, most were able to provide a means of accurately backing up and restoring contacts lists. The most notable exceptions were products C and G.

Whilst both were able to restore the contacts data, the format of the telephone numbers were altered to xxx-xxx-xxxx, no matter how the user had entered them. In the case of Product C, while the telephone numbers for standard contacts were still operational in this new format, the built-in carrier contacts (e.g. MMI code for checking account balances, etc.) no longer worked.

Online the NetQin Mobile Security solution appeared to offer a choice of backup locations and maintained 100% accuracy in the backup and restoration of contact data.

Comparative Testing – Test Results – General Use

Uninstallation

Solution	NetQin Mobile Security	Product A	Product B	Product C
Successful removal	Yes	Yes	Yes	Yes
	Product D	**Product E**	**Product F**	**Product G**
Successful removal	Yes	Yes	Yes	Yes

Although a very minor, and arguably trivial, matter when dealing with the security of a user's mobile handset, it is important that any installed application can be completely removed from the device without leaving any remnants.

All of the solutions included in this report were found to provide an acceptable method of uninstallation. Further analysis of each mobile device displayed no immediate signs of any remnant, benign or otherwise.

NetQin Mobile Security - Test Report

Comparative Testing – Test Results – Anti-Malware

Malware Scanning

The following is the result of the static scans against Suite 1, comprising of 75 samples:

Product	Update Date	Percentage Detected
NetQin Mobile Security	02/08/11	100.00%
Product A	02/08/11	42.66%
Product B	02/08/11	28.00%
Product C	02/08/11	0.00%
Product D	02/08/11	4.00%
Product E	02/08/11	1.33%
Product F	N/A	0.00%
Product G	02/08/11	2.66%

Product B did not manage to complete a scan, as the application kept freezing and being forced to close. The above result is the best result that engineers managed to get from the product over multiple attempts. Product C and Product F detected no samples. WCL believe this to be because they do not actually look for infected raw apk files during a regular scan, instead focusing on the detection of running/live malicious applications. Product F does not update in the normal way as it relies on a Cloud component in place of signature updates fed to the handset.

NetQin Mobile Security - Test Report

Comparative Testing – Test Results – Anti-Malware

The following is the result of the static scans against Suite 2, comprising of 129 malicious or potentially unwanted and 33 clean samples:

Product	Updated Version	Percentage Detected
NetQin Mobile Security	04/08/11	96.12%
Product A	04/08/11	31.01%
Product B	04/08/11	12.40%
Product C	04/08/11	0.00%
Product D	04/08/11	41.08%
Product E	04/08/11	21.70%
Product F	N/A	0.00%
Product G	04/08/11	21.70%

NOTE: Cloud scanning was included in these results.

These test results show that, with the additional cloud components enabled, some of the competitor solutions do begin providing a relatively higher degree of protection against malware and potentially unwanted apps.

Testing conducted after the activation of the cloud components offers a more realistic picture of overall functionality for those products in which it is incorporated. Whilst cloud necessarily increases the amount of data usage on the user’s tariff, it certainly appears that the scope of protection has a tendency to be wider when such technologies are both available and used.

NetQin Mobile Security - Test Report

Comparative Testing – Test Results – Anti-Malware

SMS URL Scans and Real-Time Protection

Solution	NetQin Mobile Security	Product A	Product B	Product C	Product D	Product E	Product F	Product G
Detect with auto install	Yes 5/5	No 0/5	Yes 4/5	Yes 4/5	Yes 4/5	No 0/5	Yes 4/5	Yes 4/5
Detect with manual install	Yes 5/5	Yes 4/5	Yes 2/5	Yes 3/5	Yes 3/5	Yes 2/5	Yes 2/5	No 0/5

Many of the solutions were able to protect against both the automatic installation, performed by accessing the URLs, and the manual installation of such applications. However, these results do show that the level of protection a user receives can sometimes depend on the delivery method of the application.

A follow-up test was then performed, against Suite 3, comprising of 50 malicious and potentially unwanted applications. This time, the focus was solely on each solution's ability to detect the presence of such applications on the handset.

Solution	NetQin Mobile Security	Product A	Product B	Product C	Product D	Product E	Product F	Product G
Detection	84%	10%	52%	50%	62%	40%	52%	38%

Comparative Testing – Test Results – Anti-Loss

Anti-Loss

Each subsection of this test has been broken down into Locate, Alarm, and Lock features. The following is for the Locate functionality:

Product	Activate via Web	Activate via SMS	Time - Web	Time - SMS	Accuracy
NetQin MS	Yes	Yes	Around 2 minutes	Under 1 minute	within 200 meters
Product A	Yes	No	Under 2 minutes	N/A	within 200 meters
Product B	No	Yes	N/A	Over 6 minutes	Unable to locate
Product C	Yes	No	N/A	N/A	N/A
Product D	No	Yes	N/A	Under 1 minute	within 200 meters
Product E	No	Yes	N/A	4 to 5 minutes	within 30 meters
Product F	Yes	No	Around 3 minutes	N/A	within 200 meters
Product G	Yes	Yes	Around 7 minutes	Around 4 minutes	within 250 meters

Some of the solutions automatically turned on GPS when receiving a command to Locate via SMS. Product B was unable to detect any location coordinates for the handset, and after 6 minutes returned an SMS saying it was unable to locate the handset. Engineers were unable to get the website manager for Product C to work correctly.

Comparative Testing – Test Results – Anti-Loss

Remote Alarm

Product	Activate via Web	Activate via SMS	Time to Activate
NetQin MS	Yes	Yes	Under 1 minute
Product A	Yes	No	Under 1 minute
Product B	No	No	N/A
Product C	No	No	N/A
Product D	No	Yes	Under 1 minute
Product E	No	No	N/A
Product F	Yes	No	Under 30 seconds
Product G	Yes	Yes	Around 3 minutes

Product B’s alarm feature can only be disabled through the website, while three of the solutions do not have an alarm feature. One solution’s alarm comes with the ability to set how many times you want the alarm to sound, however it is the engineers’ opinion that the Alarm could potentially be mistaken for a ringtone. For Product F, the alarm feature can be stopped without the need for a code, which potentially lessens the value of the security feature.

Comparative Testing – Test Results – Anti-Loss

Remote Lock

Product	Activate via Web	Activate via SMS	Time to Activate
NetQin MS	Yes	Yes	Under 1 minute
Product A	Yes	No	Under 1 minute
Product B	No	Yes	Under 1 minute
Product C	Yes	No	N/A
Product D	No	Yes	Under 1 minute
Product E	No	Yes	Under 20 seconds
Product F	Yes	No	Under 30 seconds
Product G	Yes	Yes	Around 2 minutes

Product B requires users to set it as the default Home screen to enable a total lock when the command is received. This same feature is used in Product D with the added ability to set a pin, pattern, or password. A feature of Product E is that the app will wipe the handset after 10 unsuccessful password attempts at the lock screen. If an SMS is used to trigger a remote lock, Product G displays the number from which it was sent.

Comparative Testing – Test Results – Anti-Loss

Remote-Wipe

The following table displays the results for the Remote-Wipe feature testing. More information is available in the Engineers Comments section:

Product	Web	SMS	Time to activate	Total Wipe
NetQin MS	Yes	Yes	Under 1 minute	Yes
Product A	Yes	No	Under 1 minute	No
Product B	No	Yes	Around 2 minutes	Yes
Product C	Yes	No	N/A	N/A
Product D	No	Yes	Under 1 minute	Yes
Product E	No	Yes	Around 3 minutes	No
Product F	Yes	No	Around 4 minutes	Yes
Product G	Yes	Yes	Around 2 minutes	No

Product A left the Google Account details logged in after a wipe. Contacts could be obtained by re-synchronising this account. For Product C there are tools within the app to delete data, but these are not remotely triggered via SMS. As such, the tools were run, and the app wiped the SD card, and SMS and Contact details. Product D actually restarts the phone to perform the functions. With Product E, all handset details were wiped. However, no data was wiped from the SD card which could well present a security risk. Product E locks the handset after a wipe. Product G also leaves the Google Account logged in.

Checkmark Product Testing and Certification

Checkmark is the world's fastest growing certification system for information security products and services. It is a highly regarded accreditation program, recognized globally by vendors, end users and by government agencies as providing end users with effective confirmation of a product's or service's effectiveness in an ever-changing threat landscape.

NetQin have been tested against, and awarded certification for, the following Checkmark certifications:

- Mobile Security Anti-Malware
- Mobile Security Loss-Control

West Coast Labs' Conclusion

In conclusion, the testing carried out by West Coast Labs has revealed a number of interesting results and has shown a variance in the ways that some vendors have chosen to deal with mobile security threats. To give just one example, Product F and Product C appear to focus on installed and installing files rather than the actual .apk installation packages. Other Mobile Security vendors take the wider approach that all files are potentially malicious to handsets.

One thing has become clear from the testing - that some mobile security products still have a way to go to achieve the effectiveness of more traditional desktop-type solutions. Mobile threats are becoming more commonplace as the market and technology expands, and it seems that taking an all-encompassing approach would be an advisable way for vendors in this market area to proceed.

We see from this testing that NetQin Mobile Security has taken the approach that all files are potentially malicious. Cloud scanning functionality, also a part of NetQin's offering, appears to be a must have feature in a time when mobile data storage and processing capacities are relatively restricted due to being on a low powered piece of hardware. When considering Cloud technologies, data bandwidth could become an issue but this is a resource that is expanding all the time, and so it is expected that this will become normal for products in a very short space of time.

WCL's comparative testing reveals that some major companies in the more traditional desktop and server-based Anti Malware space are missing features in their solutions or have decided to go down slightly different paths for their protection offerings, favouring one set of technologies over others.

NetQin Mobile Security - Test Report

West Coast Labs' Conclusion

Considering the other technologies looked at here, theft is clearly a big risk to mobile users, and Anti-Loss and Remote-Wipe technologies are an effective way to counter this threat, if they are implemented properly. The testing shows that a combination of SMS Anti-Loss features and an ability to manage a handset through a website may well be the best approach to allow for full flexibility when a handset is discovered or reported as missing.

Finally, looking at the features and functionality examined herein, the results seem to show that NetQin Mobile Security is currently one of the more feature-packed offers in the mobile security arena, and is well placed to deal with the emergence of new threats in this constantly evolving arena.

Product Feature Set Comparisons

West Coast Labs were asked to compile a comparative feature list for each of the products included in this test. This information has been gathered from freely available marketing literature of those companies included in this test.

As this information is gathered from marketing and other such materials, the information contained within the following tables should be taken as a high level overview and does not constitute a comparison of those features that were examined as part of the testing.

A description of each feature technology can be found in Appendix A on page 38.

Product names have been shortened, full versions are as follows:

Product	Version
NetQin Mobile Security	NetQinAV
NetQin Mobile Manager	NetQinMM
BullGuard Mobile Security 10	BullGuard
Kaspersky Mobile Security 9	Kaspersky
AVG Mobilation	AVG
F-Secure Mobile Security	F-Secure
Norton Mobile Security	Norton
Lookout Mobile Security	LookOut
McAfee WaveSecure	McAfeeWS
McAfee MobileSecurity	McAfeeMS

NetQin Mobile Security - Test Report

Product Feature Set Comparisons

Category: Background										
	NetQinAV	NetQinMM	LookOut	McAfeeWS	McAfeeMS	Norton	F-Secure	Kaspersky	AVG	BullGuard
Supported OS										
Android	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Symbian	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
Windows Mobile	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes
BlackBerryOS	Yes	No	Yes	Yes	Yes	No	No	Yes	No	Yes
iOS	No	No	No	No	No	No	No	No	No	No
Pricing Model										
Free version available	Yes	Yes	Yes	Trial	Trial	Yes	Trial	Trial	Yes	No
Price, if at cost	£1.50	-	$29.99	$19.99	$29.99	€ 29.95	€ 29.95	£19.99	£6.09	£19.95
Length of subscription	Monthly	-	Yearly	Yealy	Yearly	Yearly	Yearly	Single	Yearly	Single
Requirements										
Filesize on download	2.2Mb	3.5Mb	2.4Mb	2Mb	3.5Mb	1.1Mb	2.9Mb	866Kb	1.4Mb	374Kb
Filesize after install	3.92Mb	4.58Mb	3.94Mb	2.77Mb	5.52Mb	1.94Mb	3.73Mb	1.33Mb	1.95Mb	712Kb

Product Feature Set Comparisons

Category: Anti-Loss										
	NetQinAV	NetQinMM	LookOut	McAfeeWS	McAfeeMS	Norton	F-Secure	Kaspersky	AVG	BullGuard
Theft Protection										
GPS Locate	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audible Alarm	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes
SIM Replacement Alarm	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No
Data Protection										
Remote Wipe - SD	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Remote Wipe - Phone	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote Block/Lock	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Protected Local Storage	Yes	Yes	No	No	No	No	Yes	Yes	No	No
Category: Privacy Protection										
	NetQinAV	NetQinMM	LookOut	McAfeeWS	McAfeeMS	Norton	F-Secure	Kaspersky	AVG	BullGuard
Privacy Protection										
Hide Selected Contacts	No	Yes	Yes	No	No	No	Yes	Yes	Yes	No
View app data access	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	No

Product Feature Set Comparisons

Category: Communication Control										
	NetQinAV	NetQinMM	LookOut	McAfeeWS	McAfeeMS	Norton	F-Secure	Kaspersky	AVG	BullGuard
Contact Control										
Black/whitelist - Calls	No	Yes	No	No	No	Yes	Yes	Yes	Yes	No
Black/whitelist SMS	No	Yes	No	No	No	Yes	Yes	Yes	Yes	No
Data Protection										
Parental control - Calls	No	No	No	No	No	No	Yes	Yes	Yes	No
Parental control - SMS	No	No	No	No	No	Yes	Yes	Yes	No	Yes
Network connect control	No	No	Yes	No	No	No	No	Yes	Yes	No
Anti-spam	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes
Web content filtering	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes

Category: Anti-Malware										
	NetQinAV	NetQinMM	LookOut	McAfeeWS	McAfeeMS	Norton	F-Secure	Kaspersky	AVG	BullGuard
Updates										
Automatic Updates	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Manual Updates	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes
Scanning										
On-Demand Scanning	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
On-Access Scanning	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Custom Scanning	Yes	No	No	No	No	No	Yes	No	No	No
Real-Time Alerts	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Automatic Scans	Yes	No	Yes	No	No	No	Yes	Yes	Yes	No

Product Feature Set Comparisons

Category: Additional Features	NetQinAV	NetQinMM	LookOut	McAfeeWS	McAfeeMS	Norton	F-Secure	Kaspersky	AVG	BullGuard
Backups										
Online Backups - Photos	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Online Backups - Contacts	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Backup Restore	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Application Control										
Remote Management	No	No	No	No	No	No	No	No	Yes	No
Local Management	Yes	No	Yes	No	No	No	No	No	Yes	No
View Running Applications	Yes	No	Yes	No	No	No	Yes	Yes	No	No
Application Review	Yes	No	Yes	No	No	No	Yes	Yes	No	No
Traffic Monitoring	Yes	No	Yes	No	No	No	Yes	Yes	No	No

Appendix A – Feature Table Descriptions

Supported OS	
Android	Supports any publicly available version of the Android OS
Symbian	Supports any publicly available version of the Symbian OS
Windows Mobile	Supports any publicly available version of the Windows Mobile OS
BlackBerryOS	Supports any publicly available version of the BlackBerry OS
iOS	Supports any publicly available version of the Applie iPhone OS
Pricing Model	
Free version available	A free version of the application is available, designating where this a trial only version
Price, if at cost	If available for purchase, this lists the currently available price
Length of subscription	If available for purchase, this lists the length of the subscription or whether it's a single, on-off purchase
Requirements	
Filesize on download	Filesize as downloaded by a user
Filesize after install	Filesize of the application once installed to the handset
Theft Protection	
GPS Locate	Ability to provide the current location of the registered handset using GPS technology
Audible Alarm	User can remotely enable an audible alarm on the registered handset as either an anti-theft feature or to aid in its location
SIM Replacement Alarm	An alarm is sounded should someone attempt to swap SIM cards in an attempt to bypass anti-theft security
Data Protection	
Remote Wipe - SD	User can enable a full wipe of the contents of the SD card from a remote location
Remote Wipe - Phone	User can enable a full wipe of the contents of the mobile handset from a

	remote location
Remote Block/Lock	User can remotely enable the locking of the handset to prevent unauthorised access
Encrypted Local Storage	User can opt to encrypt any data kept on the handset
Privacy Protection	
Hide Selected Contacts	Either a selection, or all of the contacts on the handset can be hidden from view in order protect user information
View app data access	User can view a record of what, if any, data is being accessed by given apps
Contact Control	
Black/whitelist - Calls	A list of telephone numbers can be entered into a black or whitelist in order to specifically block or allow incoming calls
Black/whitelist SMS	A list of telephone numbers can be entered into a black or whitelist in order to specifically block or allow incoming SMS messages
Data Protection	
Parental control - Calls	Parents can opt to block calls to specific numbers e.g. premium rate numbers on their child's mobile handset
Parental control - SMS	Parents can opt to block SMS messages to specific numbers e.g. premium rate numbers on their child's mobile handset
Network connect control	The ability of a solution to inform a user of the trustworthiness or availability of an available network connection
Anti-spam	Ability to block incoming SMS messages/emails that are either spam or from a blacklisted or unknown source
Web content filtering	Access to specific URLs from the mobile handset can be blocked
Updates	
Automatic Updates	Malware updates can be configured to run automatically
Manual Updates	Malware updates can be run manually from within the app
Scanning	
On-Demand Scanning	A malware scan can be launched, by the user, from within the app

On-Access Scanning	The security app can scan raw apk files as they attempt to install or are already installed
Custom Scanning	User can launch a scan of a specific location/directory on the handset
Anti-spam	Ability to block incoming SMS messages/emails that are either spam or from a blacklisted or unknown source
Real-Time Alerts	The user is alerted to threats as they appear, regardless of source
Automatic Scans	A malware scan of the mobile handset can either be scheduled or triggered to run on a specific event e.g. at startup of handset
Backups	
Online Backups - Photos	Backups of a user's photos can be taken and stored on a remote server
Online Backups - Contacts	Backups of a user's contacts list can be taken and stored on a remote server
Backup Restore	The restoration of backed up data can be activated from a remote location
Application Control	
Remote Management	Apps can be removed using remote software
Local Management	Apps can be review, removed, etc from within the mobile security application
View Running Applications	All applications currently running on the handset can be viewed from within the mobile security application
Application Review	All applications currently installed on the handset can be viewed from within the mobile security application
Traffic Monitoring	All current network traffic can be monitored from within the mobile security application

Appendix B - Test Suites

Suite 1

Number of samples: 75

Description: All samples used in this suite were selected from the larger Checkmark Mobile Security Anti-Malware certification suite.

Suite 2

Number of samples: 129 infected or potentially unwanted, 33 clean

Description: The malicious samples used in this suite were taken from both the larger Checkmark Mobile Security Anti-Malware suite and from external industry sources.

Suite 3

Number of samples: 50

Description: All samples used in this suite were selected from the larger Checkmark Mobile Security Anti-Malware certification suite and were distinct from those used in Suite 1.

NetQin Mobile Security - Test Report

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose.Therefore, the test results published within any given report should not be taken and accepted in isolation.

Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations.All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability.

West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

NetQin Mobile Security - Test Report

Revision History

Issue	Description of Changes	Date Issued
0.9	Initial draft of Test Report Version	10/08/11
1.0	Final Test Report – First Draft	05/09/2011
1.1	Final Test Report – Second Draft	05/09/2011
2.0	Removal of confidentiality and public release	24/10/2011

USA SALES

T +1 (949) 870 3250

EUROPE SALES

T +44 (0) 2920 548400

CHINA, KOREA, JAPAN, TAIWAN SALES

T +86 1 343 921 7464

REST OF THE WORLD SALES

T +44 (0) 2920 548400

CORPORATE OFFICES AND TEST FACILITIES

US Headquarters and Test Facility

West Coast Labs
16842 Von Karman Avenue, Suite 125,
Irvine, California, CA92606, USA
T +1 (949) 870 3250, **F** +1 (949) 251 1586

European Headquarters and Test Facility

West Coast Labs
Unit 9, Oak Tree Court, Mulberry Drive
Cardiff Gate Business Park, Cardiff CF23 8RS, UK
T +44 (0) 2920 548400, **F** +44 (0) 2920 548401

Asia Headquarters and Test Facility

A2/9 Lower Ground floor, Safdarjung Enclave,
Main Africa Avenue Road, New Delhi 110 029, India.
T +91 (0) 11 4602 0622, **F** +44 (0) 11 4602 0633

E info@westcoast.com

W www.westcoastlabs.com