Mobile Malware Evolution:

An Overview, Part 4

by Denis Maslennikov

Contents

[Introduction 2](#_Toc288160553)

[Families and variants. Statistics and changes 2](#_Toc288160554)

[New developments 7](#_Toc288160555)

[Mobile malware money-makers 7](#_Toc288160557)

[Technologies 8](#_Toc288160558)

[Mobile threats in the wild 9](#_Toc288160559)

[Symbian 9](#_Toc288160560)

[Worm.SymbOS.Yxe 9](#_Toc288160561)

[Trojan-SMS.SymbOS.Lopsoy 11](#_Toc288160562)

[Trojan-Spy.SymbOS.Zbot 12](#_Toc288160563)

[Windows Mobile 13](#_Toc288160564)

[Trojan-SMS.WinCE.Sejweek 14](#_Toc288160565)

[Trojan.WinCE.Terdial 15](#_Toc288160566)

[iPhone 17](#_Toc288160567)

[Net-Worm.IphoneOS.Ike 17](#_Toc288160568)

[Android 18](#_Toc288160569)

[Trojan-SMS.AndroidOS.FakePlayer 18](#_Toc288160570)

[J2ME 21](#_Toc288160571)

[Trojan-PSW.J2ME.Vkonpass.a 21](#_Toc288160572)

[What’s next? 22](#_Toc288160573)

#

# Introduction

Some major events have taken place since the publication of *Mobile Malware Evolution: An Overview, Part 3*.

First of all, we have seen changes in the distribution of the different mobile device operating systems. The Android operating system is consistently winning over new users, leaving Windows Mobile a long way behind. The iOS operating system (for iPhone/iPod Touch/iPad) and BlackBerry operating system have also increased their market presence, while Symbian continues to lose ground, although it is still the global leader.

Next, the list of platforms targeted by malicious programs has expanded and now includes iOS and Android. As we predicted, the malicious programs targeting iOS are only capable of infecting jailbroken iPhones.

Malicious programs and attacks have, in general, become more complex.

Finally, the overwhelming majority of the malicious programs we have detected in the past year are designed to steal money from mobile device users.

As usual, we will begin our overview with some statistics.

# Families and variants. Statistics and changes

The popularity of smartphones and the increase in the number of new services they offer means a parallel increase in the number of malicious programs used by cybercriminals to make money from mobile device users.

By mid-August 2009, Kaspersky Lab had recorded 106 families and 514 variants of malicious programs targeting mobile devices. By the end of 2010, those numbers had grown to 153 families and over 1,000 variants. In other words, in 2010, we detected 65.12% more new malicious programs targeting mobile devices than in 2009, and over 17 months they nearly doubled in number.

At the end of 2010, the mobile malware situation was as follows:

|  |  |  |
| --- | --- | --- |
| **Platform** | **Number of Families** | **Number of Variants** |
| *J2ME* | 45 | 613 |
| *Symbian* | 74 | 311 |
| *Python* | 5 | 60 |
| *Windows Mobile* | 16 | 54 |
| *AndroidOS* | 7 | 15 |
| *Sgold* | 3 | 4 |
| *MSIL* | 2 | 4 |
| *IphoneOS* | 1 | 2 |

*The number of families and variants, by platform*

The data above is shown as a pie chart below:

*The distribution of the variants of detected threats, by platform*

Note that the creation of J2ME Trojans became incredibly common among virus writers: the number of J2ME threat variants even exceeded the number of threats targeting Symbian. Readers should bear in mind that malicious Java applications are a threat not only to smartphone users, but also to owners of basic mobile phones. These malicious programs generally attempt to send text messages to short numbers.

*The increase in the number of known variants (2004-2010)*

*Monthly fluctuations in the appearance of new variants (2004-2010)*

Below is a table of mobile malware threats that appeared between August 2009 and December 2010 (by family):

|  |  |  |
| --- | --- | --- |
| **Family** | **Date of Detection** | **Platform** |
| *Trojan-SMS.Kipla* | Aug 09 | J2ME |
| *Trojan-SMS.Jifake* | Aug 09 | J2ME |
| *Trojan-SMS.Vkofk* | Sep 09 | J2ME |
| *Trojan-SMS.Cyppy* | Sep 09 | WinCE |
| *Trojan-SMS.Lopsoy* | Oct 09 | Symbian |
| *Trojan-SMS.BadAssist* | Nov 09 | Symbian |
| *Net-Worm.Ike* | Nov 09 | IphoneOS |
| *Trojan-SMS.VScreener* | Nov 09 | J2ME |
| *Trojan-SMS.Levar* | Nov 09 | WinCE |
| *Trojan-SMS.Druleg* | Dec 09 | J2ME |
| *not-a-virus:Monitor.Flesp* | Dec 09 | Symbian |
| *not-a-virus:Monitor.Dadsey* | Dec 09 | Symbian |
| *Trojan-SMS.Sejweek* | Dec 09 | WinCE |
| *Trojan-SMS.Luanch* | Feb 10 | WinCE |
| *Trojan-Spy.Cripper* | Feb10 | WinCE |
| *Trojan-SMS.Picong* | Mar 10 | J2ME |
| *Worm.Megoro* | Mar 10 | Symbian |
| *Trojan.Terdial* | Apr 10 | WinCE |
| *not-a-virus:Montior.Mobspy* | Apr 10 | WinCE |
| *Trojan-SMS.Smmer* | Apr 10 | J2ME |
| *Trojan-Spy.Mijispy* | Apr 10 | J2ME |
| *Trojan-PSW.Vkonpass* | May 10 | J2ME |
| *Trojan-SMS.Slishow* | May 10 | J2ME |
| *not-a-virus:Monitor.Bond006* | June 10 | WinCE |
| *not-a-virus:Monitor.Bond006* | June 10 | Symbian |
| *Trojan-PSW.Facekob* | June 10 | Python |
| *not-a-virus:Monitor.RedGoldEye* | June 10 | WinCE |
| *SMS-Flooder.Spammo* | June 10 | J2ME |
| *Trojan-SMS.Zonagal* | June 10 | J2ME |
| *Trojan-PSW.Liamgpass* | June 10 | Python |
| *Worm.Sagasi* | June 10 | Symbian |
| *Trojan-Spy.Reples* | June 10 | Symbian |
| *Trojan-SMS.FakePlayer* | Aug 10 | AndroidOS |
| *not-a-virus:Monitor.Tapsnake* | Aug 10 | AndroidOS |
| *Trojan-SMS.Abcmag* | Aug 10 | WinCE |
| *Trojan-Spy.Zbot* | Sep 10 | Symbian |
| *Worm.Nmplug* | Nov 10 | Symbian |
| *Trojan-Spy.GPSpy* | Nov 10 | AndroidOS |
| *Trojan-Spy.Fakeview* | Nov 10 | AndroidOS |
| *Trojan-SMS.Pocha* | Nov 10 | WinCE |
| *Trojan-PSW.FakeLogin* | Dec 10 | J2ME |
| *Trojan-Downloader.Minplay* | Dec 10 | Symbian |
| *not-a-virus:Monitor.Replicator* | Dec 10 | AndroidOS |

*Total: 46 new families*

The number of new variants and new families of malicious programs targeting various platforms, detected between August 2009 and December 2010, inclusive:

|  |  |  |
| --- | --- | --- |
| **Platform** | **Number of New Families** | **Number of New Variants** |
| *J2ME* | 13 | 431 |
| *Symbian* | 12 | 58 |
| *Python* | 2 | 15 |
| *Windows Mobile* | 11 | 28 |
| *AndroidOS* | 7 | 15 |
| *IphoneOS* | 1 | 2 |
| **Total New Threats:** | **46** | **549** |

# New developments

## Mobile malware money-makers

As usual, the world of mobile malware is dominated by programs that send text messages to fee-based short numbers. The use of SMS Trojans is still the easiest and most effective means for malicious users to earn money. The reason is relatively simple: any mobile device, be it a smartphone or just a basic handset, has a direct connection to its owner’s money in the form of their mobile account. It is this ‘direct access’ that cybercriminals actively exploit.

One of these SMS Trojans has even started using adult content resources — smartphones infected with Trojan-SMS.AndroidOS.FakePlayer will immediately send four text messages to a number used to pay for access to adult content material.

However, since 2010, sending fee-based text messages ceased to be the only illegal money-making scheme for virus writers developing threats targeting different platforms.

In 2010, for the first time in the 6-year history of mobile malware, Kaspersky Lab detected a Trojan (Trojan.WinCE.Terdial.a) that makes *calls* to international fee-based numbers.

A worm designed for the iPhone (Net-Worm.IphoneOS.Ike.b) was used by cybercriminals to launch a targeted phishing attack against users of one Dutch bank. When an attempt was made to visit the bank’s website from a smartphone infected with the worm, the user was redirected to a phishing website.

Another new malicious program (Trojan-Spy.SymbOS.Zbot.a) appeared on the scene and was used by the cybercriminals to bypass SMS authentication for online banking customers. This mobile Trojan was used in a complex attack in combination with the dangerous Zbot (ZeuS) Trojan.

These malicious programs are discussed in more detail below.

## Technologies

Since the publication of our most recent *Overview*, mobile malware evolution has not seen the development of any new technologies. However, new malicious programs are actively using known technologies in combinations that pose formidable threats.

For example, malicious users have started to control and combine their malicious programs from remote servers, allowing them to:

* Quickly obtain stolen user data
* Update malware performance parameters
* Integrate infected mobile devices into botnets

This means that attacks launched by mobile threats have reached a completely new level.

# Mobile threats in the wild

We will take a look at the most significant malware for different platforms that existed between August 2009 and December 2010.

## Symbian

### Worm.SymbOS.Yxe

At the start of the summer of 2009, a fourth new variant of the Worm.SymbOS.Yxe worm was detected.

You may remember that when the Yxe worm first appeared in early 2009, it was the first malicious program for smartphones running on Symbian’s S60 3rd edition platform. This threat, in addition to its ability to self-replicate via text messages and collect data about the phone and its owner, also had another distinguishing trait: all of its variants had a Symbian digital signature and were able to execute on just about any smartphone running Symbian S60 3rd edition.

The worm’s fourth variant, Yxe.d, not only sent out text messages, but also updated the text message template linked to a remote server. Yxe.d showed us that mobile malware is capable of operating from remote servers run by malicious users, in addition to receiving updates and commands from them. Unfortunately, the system runs all too smoothly — which means that the capability to build mobile botnets now exists!

Incidentally, the first malicious program for mobile devices capable of receiving commands from malicious users (Backdoor.WinCE.Brador) appeared back in August 2004. However, it never posed much of a threat until now, as smartphones were not continuously connected to the Internet at the time. In contrast, wireless technologies are very widespread today and the mobile Internet has become much more affordable — a precondition for the inevitable development of a mobile threat that would, one way or another, interact with a malicious user-controlled remote server.

Things quietened down after the emergence of the .d version. In early 2010, the Chinese virus writers behind Worm.SymbOS.Yxe once again updated their creation. The new features in the most recent variant of the worm are:

- The worm makes attempts to connect with a Chinese social networking site

- The worm is capable of downloading files

The text message that the worm sent in order to self-replicate offered recipients the chance to find out more about the private life of the famous Chinese actress Zhang Ziyi. If the user clicked on the link via the mobile Internet, they would be asked to download and install the file LanPackage.sisx. If the user visited the site through a regular computer-based browser, then the page would display a ‘404 Error’ page.

In other words, the remote server verified the User-Agent, which contains information about the application, the operating system, language settings, etc, and if the user arrived via anything but the mobile Internet, it simply displayed an error message.

The added file download function worked correctly when the worm was detected, although there were no files on the malicious user’s remote server ready for downloading.

### Trojan-SMS.SymbOS.Lopsoy

Prior to autumn 2009, Worm.SymbOS.Yxe was the only threat of its kind targeting mobile devices running on the Symbian S60 3rd edition platform — and with a Symbian digital signature. In October 2009, Kaspersky Lab detected a new SMS Trojan for smartphones running on Symbian S60 3rd edition: Trojan-SMS.SymbOS.Lopsoy, which also had a Symbian digital signature.

*The Trojan’s digital signature data*

The Trojan was planted on a number of file hosting resources disguised as a variety of mobile apps and games, including those with adult content. After penetrating a user’s smartphone, the malicious program would:

1. Use autorun
2. Hide itself in the process list
3. Run a search for an Internet access point in order to connect with the malicious user’s remote server
4. Once connected to the server, it would receive a premium-rate number that it subsequently sent text messages to. The text for the outgoing messages was also provided.

*The URL of a malicious user’s server in the body of a Trojan*

Unlike the primitive SMS Trojans designed for the J2ME platform, Lopsoy provided malicious users with considerably more capabilities. Once infected with the malicious program, the phone would constantly connect to the remote server, while the malicious user would in turn regularly change the text of the outgoing messages and the number to which the messages would be sent.

Finally, there was one more digitally signed malicious program for the Symbian S60 3rd edition platform that was capable of connecting to a remote server in order to receive operational parameters.

### Trojan-Spy.SymbOS.Zbot

In late September 2010, specialists at S21Sec detected a malicious program capable of forwarding incoming text messages to a specific number. At first, it appeared to be of no particular interest. However, it turned out that this threat was, first of all, connected to the well known Zbot (ZeuS) Trojan, and furthermore, malicious users weren’t interested in all of the text messages — just the ones that contained authentication codes for online banking transactions. Kaspersky Lab labeled this threat Trojan-Spy.SymbOS.Zbot.a.

The attack was set up as follows:

1. Zbot steals online banking access data from an infected computer.
2. After confirming the victim’s telephone number, the malicious user sends a text message with a link to a malicious program for smartphones.
3. When a user clicks on the malicious link, they are asked to download an app and can either install it, which launches the Trojan, or decline it.
4. The malicious user then attempts to conduct a transaction via online banking services that require text message confirmation.
5. The bank sends a text message with the authentication code to the victim’s phone number.
6. The malicious program then forwards the incoming message to the malicious user’s phone number.
7. The malicious user obtains the authentication code and completes the online banking transactions.

This malicious program also had a legitimate digital signature.

Such a complex plan of attack just goes to show that malicious users are constantly broadening their interests. Prior to the detection of this particular threat, text message authentication was one of the last reliable means of protection when conducting banking transactions on the Internet. Now, malicious users have found a way to bypass even this level of security.

## Windows Mobile

Today, the Windows Mobile operating system is losing its foothold on the mobile market for a number of reasons:

1. Microsoft is launching a new operating system for smartphones — Windows Phone — and is abandoning any further development of Windows Mobile.
2. The number of new smartphone models with preinstalled versions of Windows Mobile is falling.
3. The operating system has not been updated for quite some time.

However, even with the falling popularity of this operating system, virus writers are still as active as ever.

### Trojan-SMS.WinCE.Sejweek

In late 2009, a new SMS Trojan targeting the Windows Mobile platform appeared: Trojan-SMS.WinCE.Sejweek. In many ways it was similar to Lopsoy, but there were some differences as well.

Firstly, as with Lopsoy, Sejweek made attempts to connect with a remote server. If the attempts were successful, the Trojan would download an XML file like the one below:

*The XML file downloaded by Sejweek*

Clearly, the information between some of the tags has been encrypted. The following table is stored in the Trojan’s code and is used for deciphering the encryption:

*The table used for deciphering encrypted code*

When the data between the <phone> and <interval> tags is deciphered, it looks like this:

*The deciphered XML file*

As you can see from the contents of the <phone> and <interval> tags, the malicious program sends fee-based text messages from the infected phone to the short number 1151, and does so every 11 minutes. If you consider that the Trojan also regularly updates the XML file — i.e., it downloads new data to send short messages — then it is easy to see how it is capable of reducing a user’s mobile account balance to zero very quickly.

This is not, unfortunately, the only example of monetizing malware that targets this particular operating system.

### Trojan.WinCE.Terdial

In 2010 and for the first time, a Trojan that makes calls to toll numbers was detected. In late March, a new game called 3D Anti-Terrorist appeared on a variety of international websites offering free software for smartphones running Windows Mobile. In addition to the game itself, the 1.5MB zipped folder also contained a file named reg.exe, which was actually Trojan.WinCE.Terdial.a, a Trojan that makes international fee-based calls.

After the antiterrorist3d.cab file was installed and launched, the game would install in the Program Files directory and a copy of the 5,632-byte malicious reg.exe file was installed in the system directory under the name smart32.exe.

A more in-depth analysis of the threat’s code revealed that:

* The malicious program was created by Russian-speaking virus writers
* The threat used the CeRunAPpAtTime autorun function
* After launching for the first time, the Trojan would make calls to 6 different premium-rate numbers each month

*A list of numbers to which calls were made*

+882\*\*\*\*\*\*7 - International Networks

+1767\*\*\*\*\*\*1 - The Dominican Republic

+882\*\*\*\*\*\*\*4 - International Networks

+252\*\*\*\*\*\*\*1 - Somalia

+239\*\*\*\*\*\*1 - San Tomé and Príncipe

+881\*\*\*\*\*\*\*\*3 - Global Mobile Satellite System

To spread the virus, the author responsible for creating this Trojan used the relatively popular and legitimate game, 3D Anti-Terrorist, which was developed by the Chinese company Huike. As we all know, many Internet users install free or cracked software and cybercriminals use sites offering cracked software as a place to plant their malicious programs, disguising them as legitimate files — and that is exactly what happened in this case. Unfortunately, this will continue to happen in the future.

## iPhone

In the conclusion of Mobile Malware Evolution: An Overview, Part 3, we predicted that iPhones would become infected only if they had been jailbroken and if the user had installed apps from non-official sources. Our predictions turned out to be true.

### Net-Worm.IphoneOS.Ike

In early November 2010, the first worm for iPhone was detected and named Net-Worm.IphoneOS.Ike.a. The users at risk of infection were those who had jailbroken their iPhones or iPod Touches without changing the default SSH password. The worm replicated using this special feature of the iPhone. It did not however cause any major damage to its victims: Ike changed the background on users’ smartphones to a picture of 80s singer Rick Astley, but did not do anything else.

However, just a few weeks later a new worm targeting the iPhone was detected: Net-Worm.IphoneOS.Ike.b. This time, the worm stole user data and let malicious users remotely control infected smartphones. This variant also attacked users of jailbroken iPhones and iPod Touches where the default SSH password was not changed.

*The ‘vulnerability’ exploited by Ike.b*

People who used the online services of the Dutch bank ING Direct also became victims. When users attempted to go to the bank’s website from an iPhone infected with the worm, it redirected them to a phishing site. If the user entered their data on the phishing webpage, then it fell into the hands of malicious users.

The Ike worm is a truly ‘monetizing’ malicious program that targets jailbroken iPhones and iPod Touch devices.

## Android

The Android platform, which has managed to win substantial market share, was not of particular interest to virus writers for a while. However, that all changed in August 2010, when the first malicious program targeting the operating system was detected. Since then, we have seen both new variants of the original threat and other malicious programs targeting Android, the current total standing at seven families.

### Trojan-SMS.AndroidOS.FakePlayer

As was noted above, the first malicious program for Android smartphones found in the wild was Trojan-SMS.AndroidOS.FakePlayer, which was detected in early August 2010.

Unfortunately, there is nothing specific that can be said about the means used to spread the first variant of this Trojan. It can only be said that FakePlayer was not spread via the official Android Market.

If a user’s phone became infected with this malicious program, the Trojan sent three text messages to two Russian short numbers immediately after launching.

The second variant of Trojan-SMS.AndroidOS.FakePlayer appeared in early September 2010, or approximately a month after the first one. Its primary function had not changed much at all. The detection of the second variant of FakePlayer did shed some light as to how it spread. As we know, virus writers often take advantage of those users with a penchant for adult content material in order to spread malicious programs, and it was adult content material that played a substantial role in the spread of FakePlayer.

These days, on the Russian Internet, owners of fee-based adult content websites offer visitors the opportunity to gain rapid access to the website’s content by using their mobile devices: the user sends an SMS message (or messages) containing specific text to a premium-rate number, and the user then receives an access code that they enter on the website’s homepage.

The message that provided payment for the adult content material was sent out by Trojan-SMS.AndroidOS.FakePlayer not just once, but four times in rapid succession. So how did the Trojan get onto peoples’ mobile phones?

Clearly, many users end up on adult content websites via web searches. The owners of adult content resources that use Trojan-SMS.AndroidOS.FakePlayer also used SEO methods to bring the links to their websites as close to the top of search results as possible for common adult content related search requests.

If a user was on their personal computer, the following scenario might have taken place:

The user performs a search for something related to adult content and is led to an adult content website; the user sends a text message to receive an access code and views the website’s contents.

So what happens when someone is using a mobile device for browsing, such as a smartphone running on the Android platform?

The first three steps in the process are the same, but later, it gets more interesting. After clicking on one of the links ‘promoted’ by a website owner in search results, a remote server managed by malicious users transfers an HTTP request containing, among other things, a User-Agent string (i.e., it contains information about the application, the operating system and language, etc.).

Next, the remote server verifies the User-Agent. In the event that the user visited the site via a desktop browser, they will see the adult content website as expected. However, if the user visited the site from their mobile browser on an Android phone, then they will be asked to download pornoplayer.apk, also known as Trojan-SMS.AndroidOS.FakePlayer.

The sequence of events goes something like this:

The user performs a search related to adult content and is led to an adult content website. They are then asked to download pornoplayer.apk. The user downloads the program and the Trojan launches and sends four text messages to fee-based short numbers, with some of that money going to the owner of the adult content website.

Thus, the owner of the adult content website also makes a little extra money — but there’s a catch: the income is illegal.

After examining the websites used to spread FakePlayer, something unusual came to light: the cybercriminals were using geo-targeting, which let them filter visitors and only offer pornoplayer.apk for download if the user arrived from a Russian IP address.

## J2ME

Since the publication of Mobile Malware Evolution: An Overview, Part 3, J2ME has been targeted more frequently by virus writers than any other platform. The overwhelming majority of threats designed for J2ME are SMS Trojans, although no major changes have been made to their basic functions or means of infection. So instead of discussing SMS Trojans, let us instead take a closer look at an example of a malicious program that targets the J2ME platform in order to steal users’ login credentials for a commonly used Russian social network.

### Trojan-PSW.J2ME.Vkonpass.a

May 2010 saw the appearance of a malicious program that attempts to steal users’ logins and passwords to the Russian social networking site VKontake. The threat was designed for the J2ME platform, which until recently was plagued exclusively by SMS Trojans. Before Vkonpass, no other threats attempted to steal logins or passwords to social networks.

Kaspersky Lab detected Trojan-PSW.J2ME.Vkonpass.a when it was designed as a program used to access VKontakte. After the Trojan launches on the mobile device’s screen, a window appeared asking the user to enter their login and password for the social networking site, allegedly in order to access their homepage.

If the user entered their credentials, the malicious program would attempt to send the data via an SMTP protocol to the malicious user’s email address. If the attempt to send the data was unsuccessful, then the user would see a ‘connection error’; if the attempt was successful, then the user was shown an ‘Error 401’ page.

# What’s next?

In the next year, mobile threats will evolve in the following way:

1. Regarding SMS Trojans. For now, unfortunately, no preconditions are in place that would facilitate a downturn in the number of SMS Trojans. The law in some countries still needs improvements and cybercrimnals can still use short numbers with complete anonymity.
2. Concerning the number of threats targeting Android. This platform is gaining popularity among users and cybercriminals will show increased interest in it as a result.
3. There will be an increase in the number of vulnerabilities detected in a variety of smartphone platforms, and possibly the launch of attacks using these vulnerabilities. Until recently, no major attack that has exploited a vulnerability has been recorded. But one such vulnerability exists in iOS and was detected on August 4 (an update was released on August 11); it could be used to execute arbitrary code in the system. If a user tried to open a specially formatted PDF file, then it could result in a stack overflow and arbitrary code execution in the system, with the highest privileges. Was this vulnerability used in attacks against smartphones? We do not have any information about any such incidents. We do know for certain, however, that the vulnerability was only used to simplify the iPhone jailbreaking process.
4. There will be an increase in the quantity of commercial espionage software (spyware). This type of software can be used to monitor third-party activities, which could include, for example, industrial espionage or obtaining confidential information such as confidential correspondence.

Additionally, we should not forget about tablet PCs — these devices will be the rising stars of 2011. In 2010, Apple released the iPad, which uses the same OS as the iPhone. There are plans to release tablets that run on Android, with some manufacturers having already announced their intentions to produce such devices. RIM will soon launch sales of its own BlackBerry tablet.

These devices provide considerably more than typical smartphones, offering users: word processing, convenient web surfing and high-definition video and gaming capability, etc, making them a hit with consumers.

In terms of operating systems, it’s the same story. Essentially, we will have streamlined devices with larger screens running iOS, Android, BlackBerry, etc. That means malware will be able to run on smartphones and tablets.

There is one more ‘but’: smartphones and tablets are not interchangeable for one simple reason — tablets do not function as telephones. That means that most people who own tablets will also own a smartphone, driving up the number of potential victims and an increasing the number of threats targeting them.

#