



Trends for 2012

Malware Goes Mobile

ESET Latin America: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com



By:

ESET Latin America's Lab
Additional material: ESET
North America

Date:

November 2011, revised
January, 2012

Contents

| | |
|--------------------------------------------|-----------|
| Introduction | 3 |
| Malware in mobile devices | 4 |
| Massive impact | 7 |
| Android: the new XP? | 7 |
| New technologies, new threats | 9 |
| Conficker disappearance | 10 |
| Botnet takedowns | 11 |
| Simplicity: rogue and greyware..... | 12 |
| Threats in Latin America | 13 |
| Conclusion: a new era?..... | 15 |

Introduction

It has become customary for ESET Latin America's Malware Analysis Lab to analyze in its [Trend Report](#) what has happened throughout the year, and 2011 is no exception. The present document looks at trends for next year, not only with reference to malicious code, but also looking more generally at other types of computer attacks and the cybercrime world.

The ways in which people are accustomed to use technology have always influenced and determined malware development; and that trend that will continue. This being so, the significant growth in the use of mobile devices will be increasingly obvious in 2012. After all, malware developers have been working over the past few years to make these platforms a viable entry point for malicious codes infection. This document describes the way desktop-computer threats have moved to the mobile world and become increasingly widespread there.

In this context, [threats against mobile devices](#) (regarding new malicious programs as well as Internet frauds, among other types of attack) will be the most significant trend during next year, in addition to the appearance of new types of attack and of new variants of existing attacks.

At the same time, the evolution of security technologies for the current platforms will give rise to more waves of [new and technologically complex threats](#). However, at the other end of the scale, there will still be malicious programs that will impact heavily on users despite their technical.

So what will be the main trends for 2012? In the following sections, this question will be addressed. As users become more aware of these current threat trends they will be better placed to determine how to optimize protection mechanisms both at home and in corporate environments.

Malware in mobile devices

During the last few years, we have witnessed how different threats have appeared in mobile devices. Before 2011, the rise of various malicious programs for platforms such as Symbian and Windows Mobile attracted attention because they were considered a novelty.

However, during 2011, the existence and real-world impact of these threats was accelerated due to the escalating numbers of people acquiring these devices, and the appearance of Android as the dominant platform in the smartphone market. At present, there are more than **5 billion mobile devices worldwide**, more than 500 million of which are in Latin American countries. On the other side, one of each four mobile devices is a smartphone.

According to the Gartner consulting firm, by mid 2011, Android was the leader in mobile platforms (with more than 400 million mobile devices worldwide, [growing at a rate of 550 thousand devices a day](#)):

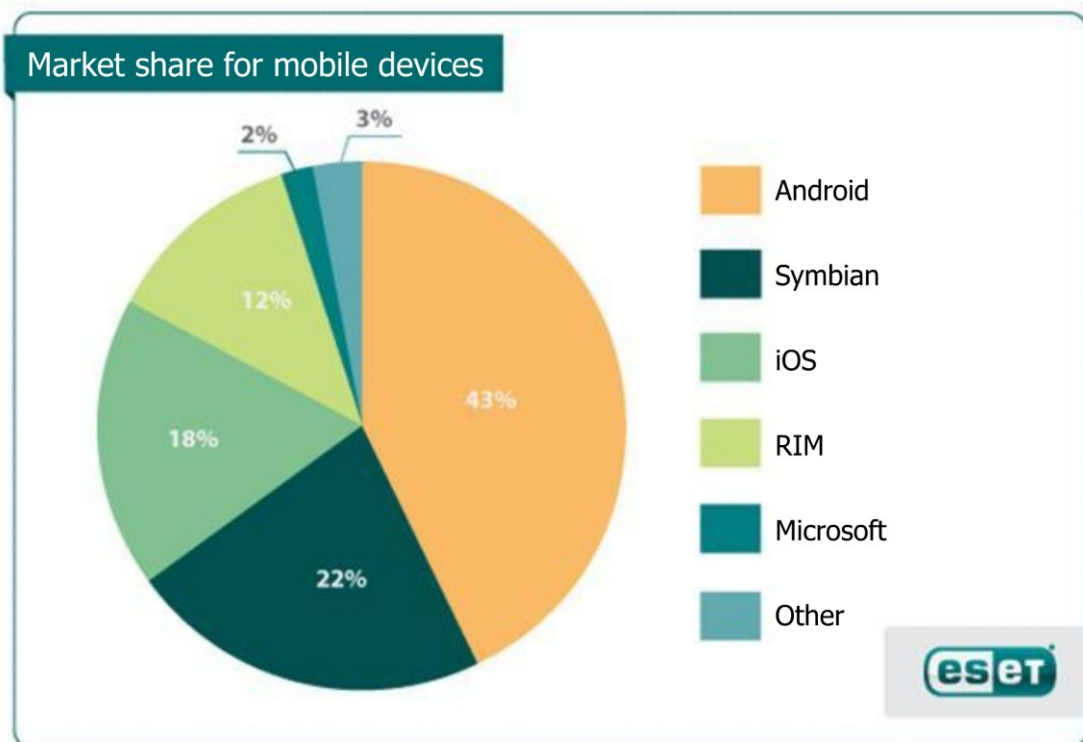


Figure 1: market share of operating systems for mobile devices

This trend was accompanied by the development of malicious code as can be seen in the following chart. This chart shows in detail the main malware variants that targeted the Android devices during the last two years, since the appearance of FakePlayer, the first malicious code for this platform (the chart can be viewed in a bigger size at the end of this document, together with its references):

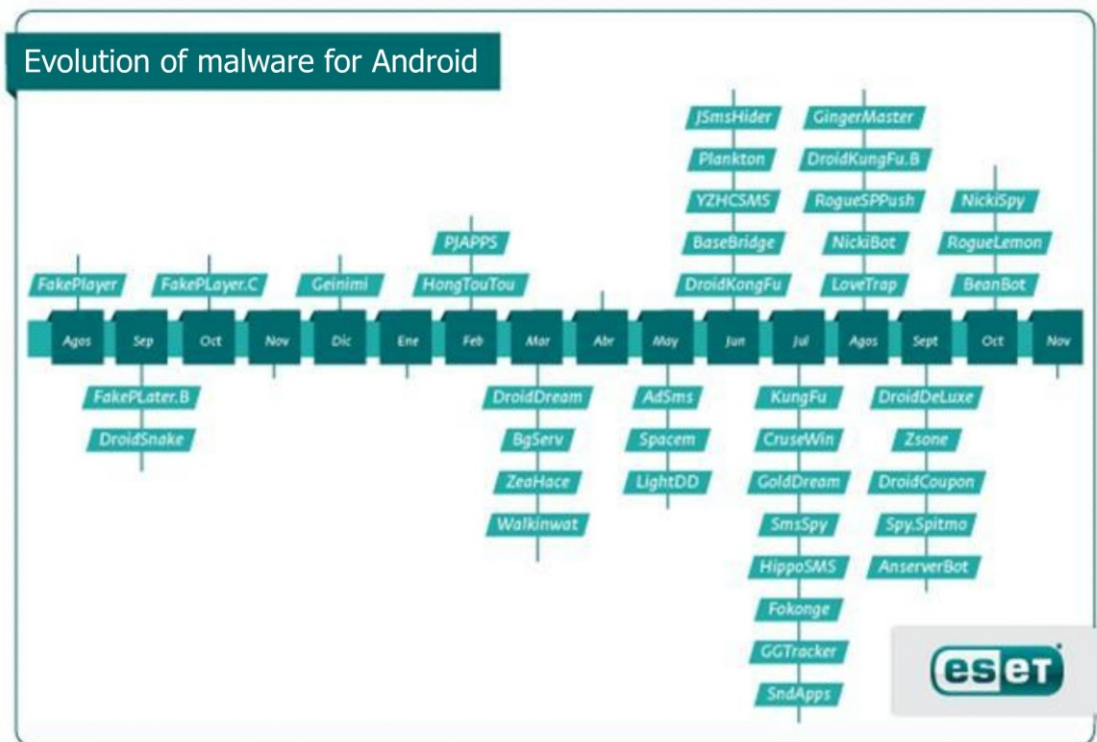


Figure 2: Growth of malware for Android

It is interesting to notice the how the number of malware variants has increased over the years taken into account for this analysis. Out of **41 malicious codes that were analyzed, only 5 appeared in 2010**, belonging only to three different malware families. This trend continued during the first two quarters of 2011 with the appearance of only 7 new variants, in contrast to a significant concentration of threats for this platform during the last six months of 2011, thus highlighting **threats for Android as the main trend for the year 2012** (its malware market share exceeded Symbian's in 2011).

Continuing our analysis of the main malicious codes for Android, it is interesting to note their propagation method, since 12 of the identified variants were available for download from the Android Market. In this respect, the fact that 30% of the threats can be downloaded from the official manufacturer's repository shows the significance that this platform will have in the future as a threat vector, and the need for manufacturers to strengthen their efforts to

minimize this kind of incident. Nevertheless, it is equally significant that most threats were downloaded from non-official repositories (7 out of 10), indicating that it is still absolutely **crucial that users** are made aware of the importance of **downloading software from the official websites**.

Other data to highlight show that 15 out of the 41 applications analyzed were identified as **SMS trojans**, one of the main threats against users of mobile devices, and that 60% of the malicious codes that were analyzed had **botnet characteristics and functionality**. That is, they allowed the attacker to gain remote access to and control of the device, which, once infected, becomes a zombie.

As regards botnets in particular, it is also possible to identify a further trend in the development of malware for mobile platforms. During 2011, we noticed a marked influx of variants of mainstream botnets ported to mobile devices, years after they were first seen infecting desktop computers. For example, **Zeus** first appeared in 2007 and three years afterwards, versions for mobile devices started to appear. By 2011, there were already variants for four important mobile platforms.

The following table shows all the dates in which the Zeus and SpyEye variants were discovered, both in their desktop and mobile variants (ZITMO and SPYTMO, respectively):

| Botnets in mobile devices | | | | | |
|---------------------------|---------------|----------------|----------------|----------------|----------------|
| | Desktop | Windows Mobile | Symbian | Blackberry | Android |
| Zeus (ZITMO) | July 2007 | February 2011 | September 2010 | September 2010 | July 2011 |
| SpyEye (SPYTMO) | December 2009 | - | April 2011 | April 2011 | September 2011 |




Figure 3: Appearance of Zeus and SpyEye for desktop computers and mobile devices

It is clear from this figure that different malware variants have been migrating to mobile versions during 2011. This trend can be expected to continue and, once the first instances of one

type of specific malicious code appear, the creation of variants that can begin to spread slowly is a logical next step.

To take a more recent example, by the end of October 2011 malicious programs of the rogue type (fake security software) have also appeared for Android, as [reported by the ESET Latin America's Lab Blog](#).

Massive impact

Another indication that malicious code for mobile devices will be the main trend for next year is the increased impact of mobile malware. **DroidDream** turns out to be the best exemplar for this trend, since there were more than **250,000 downloads of this threat from the Android Market**. This attack had such an impact that Google decided to uninstall the application remotely from all the infected systems. All the users whose mobile devices had been compromised were notified by email.

Among DroidDream's main objectives is the theft of information that allows an attacker to unambiguously identify the infected device as well as the ability to install other malicious code. One of the most striking peculiarities of this malware is that, to avoid being identified by the user, it became active during the night by checking that the time is between 23:00 and 08:00, which gave it its name.

DroidDream will go down in history as the first malicious code for mobile devices with such massive impact, guaranteeing of the likelihood of finding more incidents of this kind during next year.

Android: the new XP?

For many years we have seen how the developers of malicious software for desktop operating systems focused their efforts on Windows. Although in the last few years there have been multiple threats for other platforms (such as Linux or Mac OS), the Microsoft operating system has always been the center of attention for malware writers.

Despite the current gap between the mobile and desktop computer worlds, if we take into account the amount of devices and the number of threats, it can be said that nowadays malicious software developers have found in Android that the same exploitability that Windows XP has offered for years: not only because of the characteristics inherent to the platform, but also because most users have unsafe habits.

Growth in market share, the technical features of the operating system, the ability to propagate the malware via repositories (official or otherwise), and certain other characteristics, ensure that Android is becoming a priority target for any malicious code developer, and **that will be the focus of malicious code for these platforms during 2012.**

New technologies, new threats

According to the statistics [published by the Gartner consulting firm](#), by the end of 2011, Windows 7 will become the most widely used desktop operating system in the world, with 42% of market share. This event, which will displace Windows XP from the first place, also implies some changes in the threats developed by cybercriminals. The improvements in the security provided by newer operating systems lead to a corresponding development of more technologically advanced malicious code, with the purpose of evading such protection mechanisms as User Account Control (UAC). These threats will be more complex from a technological perspective: in the Windows XP era, many of the threats simply overwrote a registry entry or wrote a file in order to damage the system; however, newer malicious programs will need to implement more complex strategies in order to infect and execute a payload .

In addition to these protection mechanisms, many 64-bit systems (supplied with most modern desktop computers) have security protection that is launched along with the operating system startup in order to avoid threats such as rootkits: malicious programs that hide their activity from the operating system by working within it. However, throughout 2011, [new malware variants](#) were spreading that included features intended to evade these protection mechanisms. The appearance of new variants of the latest version of a known threat, such as [TDL4](#), proves that the development of more complex malware is a reality. These evolutions consist of a rootkit of the botnet type that is able to infect [64-bit operating systems](#) and bypass their authentication mechanisms; it was specially developed for Windows Vista and Windows 7.

In 2012, there will be more malicious programs able to breach the digital signature systems also present in the most modern operating systems. One such case was Mebroni, a malware that [infects the BIOS of the system](#), compromising it before the startup process gets going. This is a **much more persistent type of threat** because, by infecting the BIOS of the system, it can rewrite system startup code – the Master Boot Record (MBR) and Volume Boot Record (VBR), thereby compromising the computer's security.

Digitally-signed malicious codes with stolen certificates, as was the case with [Stuxnet](#) by the end of 2010, will become more frequent over the next year. In fact, in summer 2011, DigiNotar, a company that issued certificates, was hacked and its certificates were used for malicious purposes, resulting in the company's eventual **bankruptcy and increasing distrust of the [CA system](#)**.

Finally, the [Stuxnet legacy will live on](#). Just as the ESET Laboratory predicted in its report “Trends for 2011: botnets and dynamic malware”, there wasn't a massive growth of malicious code targeting SCADA systems during 2011, but there was much interest in vulnerability research: this trend will keep on growing slowly, and it is likely that next year some high-impact threats of this kind will appear.

Conficker disappearance

Another consequence of the supplanting of Windows XP by Windows 7 as the leader operating system is the reduced presence of [Conficker](#). This computer worm appeared in November 2009 and subsequently became the most important worm of recent years, placed month after month among the three most-detected threats over a three year period, according to the monthly threat reports published by ESET.

Nevertheless, the number of instances of this malicious code detected is decreasing, as shown by statistics from ThreatSense.Net®, ESET's early warning system:

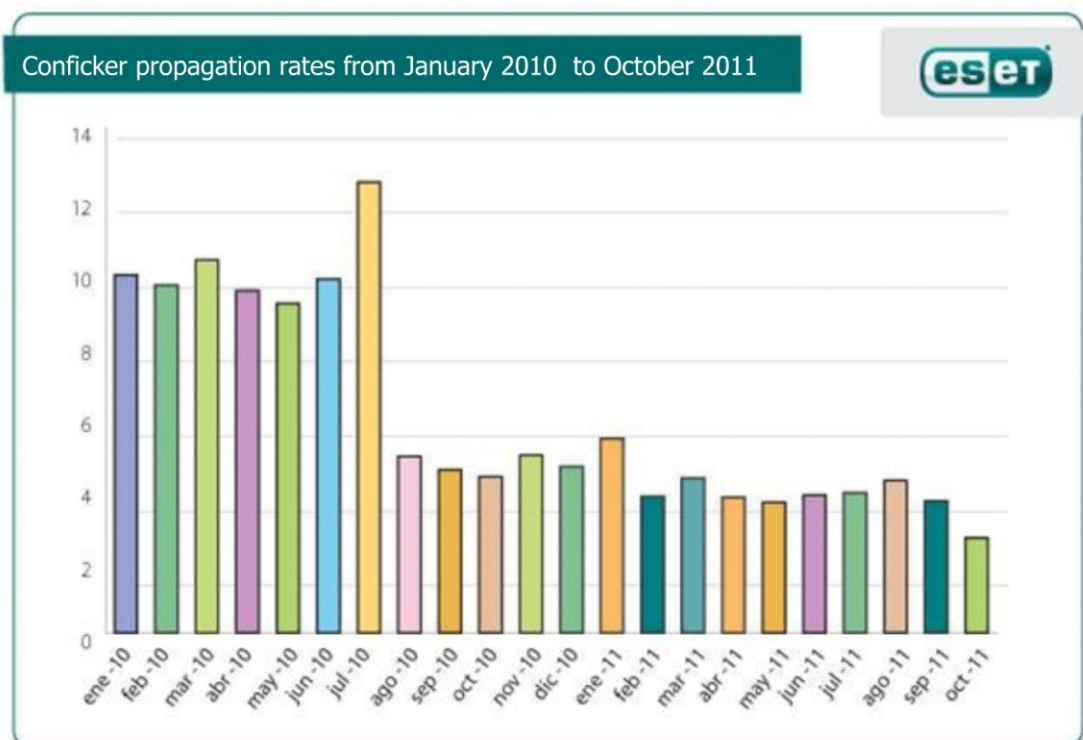


Figure 4: Conficker propagation rates from January 2010 to October 2011

As can be seen, the worm detection rates are diminishing month after month, with an average of **3.9% in 2011** (up to the end of October), a quite remarkable decrease as compared to the previous year, where the average was 7.83%. During 2010, Conficker was ranked by ESET as the most detected malicious code in 7 of the 12 months of the year; whereas in 2011 it only reached top place in January (with 5.38% of the detections). That percentage had considerably decreased by October of this year (third, with 2.63%; the lowest detection rate since its appearance).

What is the reason for the decrease in Conficker detection rates? Two important factors affect these detection rates. Firstly, the natural decline in spread and impact over the life cycle of any malicious code (which in the case of Conficker was [very long indeed](#)), as a result of the users who installed security patches in order to cut off the propagation paths, or users who installed and/or updated antivirus solutions to improve detection.

However, in the case of Conficker, the variants that continued to have a high impact on users were the ones that spread through USB. Nevertheless, during 2011 there were some noteworthy events: on the one hand, the growth of Windows 7, a platform where default settings do not allow Conficker to spread automatically through USB devices. On the other, in February 2011, Microsoft issued an update to enforce disabling of Autorun on USB devices in computers with Windows XP operating systems (a patch that had already been available for users in previous years, but as an optional update). In this way, propagation paths for the Conficker worm were blocked for more and more users.

Therefore, we can expect for 2012 that infection/detection levels will continue to decrease, and that this threat, (which affected so many users over so many years and broke so many records due to its impact and speed of propagation) **will slowly disappear from the global malware scene**.

Botnet takedowns

As ESET Latin America had predicted the year before, during 2011 security companies, ISP companies and public organizations collaborated to dismantle networks of zombie computers, also known as botnets.

This procedure, known as [takedown](#), consists of cutting off some operating network node and, if possible, trace the people responsible for its administration. During 2011 the takedown of important networks such as [Kelihos](#) (dismantled by Microsoft in September), Coreflood and Koobface, among others, became known to the public. The [Bredolab case](#) is quite interesting, since it was dismantled with the total support of the Dutch government, a key factor for the success of this operation.

Bearing in mind the significant growth of the botnets during 2011 (according to ShadowServer, there are almost [six thousand active networks as of October 2011](#)), these efforts will need to be maintained and significantly increased, not only to prevent the operation of large-scale zombie networks, but also in order to take down the botnets receiving less media exposure which nevertheless manage to infect thousands of computers.

Consequently, during next year, botnet takedowns will continue to be frequent (though some have expressed doubt as to their long-term efficacy), and many of them will be made public when the extent of the takedown is sufficient to make a significant difference to botnet impact.

Simplicity: rogue applications and greyware

Apart from the growth – as expected – of increasingly technically complex threats, during 2011 there was a significant parallel growth in other malicious codes representing the other end of the scale: **technically and programmatically, they are very simple**. However, due to the effectiveness of the Social Engineering behind them, they manage to spread very efficiently.

Among the most simple malicious software, we find the banking trojans of the Qhost type which, when executed in the system, modify a text file allowing the attacker to steal the users' banking credentials.

Within this same category, two threats stand out due to the high impact they are starting to have on the users' systems: [rogue applications](#) and [greyware](#).

The first of these, also known in some of its incarnations as fake antivirus, is characterized by being a malicious code whose functions, in many cases do not extend beyond a simple animation. Its only purpose is to deceive the user, frighten him and charge a fee for a nonexistent service. The rogue app is a hoax in malware format. However, regardless of its technical simplicity, they offer very large profits since, despite the rudimentary nature of many of these attacks, such false security “solutions” are charged for at rates well above the prices charged to consumers in the real security industry. Indeed, their profitability is increased by the minimal development and maintenance costs of the more basic examples of this type of malware, though there have been instances of fake security software showing more sophisticated and adaptive behavior and interface, enhanced by a “support”, marketing, administrative and “legal” infrastructure that to some extent mimics the real thing. Of course, this level of sophistication is infinitely less expensive and resource-intensive to maintain than real security software, since it doesn't have to maintain highly-pressured product maintenance labs and other facilities.

While rogue applications are mostly seen in English, it is to be expected that the rogue software localized in the Spanish language will start appearing in Latin America during 2012, and it is

likely that other widely used languages will be used more in regions that offer sufficient potential profits

Finally, **greyware** is another growing threat trend: these are files whose malicious features are so subtle that are difficult for malware analysis labs to detect accurately and appropriately. This is the case because the degree of "malice" entailed is not simply defined in terms of direct damage (or even by the harder-to-ascertain motivation of the programmer), but also by the perception and intent of the user. Within this category there are many applications which may, for example, send the user's personal information to the attacker by acceding to the usage policy. In this way, many of these malware developers anticipate that the antivirus companies will not be able to generate these signatures to protect the computer (or will detect them optionally rather than by default, in anticipation of [legal harassment](#) from greyware and [PUA](#) developers). It is more and more commonplace to find these threats, which are specifically **focused on acquiring potentially sensitive information**.

This kind of threat, so simple from a technological point of view, will keep on growing due to its relevance in both the global and Latin American malware contexts.

Threats in Latin America

Finally, what will happen with cybercriminals in Latin America? As we already know, for many years now, computer threats are not only "imported to the region from other countries: there are also local malware developers. They take advantage of the most important events in Latin America in order to use Social Engineering techniques and infect thousands of users.

In this context, the threats generated in the region that will stand out most are the following:

- **Hacktivism:** the use of computer attacks with ideological intent is growing considerably in the region. Since the Wikileaks case and the immense popularity of some of the actions attributed to Anonymous, many people in the region have identified or aligned themselves with these movements and many organizations are starting to suffer these types of computer attacks, especially governmental organizations or persons related to politics. During 2011, many governments in the region were affected by these attacks, among which were Argentina, Chile, Colombia, Guatemala and El Salvador.
- **Privacy and social networks:** Latin America is a region where usage of social networks is high. Out of the 200 million web-surfers in the region, 162 million have a [Facebook](#) account. Therefore, Trojan propagation by these means (through [Social Engineering](#)) and particularly the growth of scams such as clickjacking (misuse of the pay-per-[click](#)

[business](#) by cybercriminals), and the use of fraudulent or [false applications to steal information](#), will be significantly high during 2012.

- **Banking trojans and phishing:** Among malware, banking Trojans are beyond any doubt the most characteristic type of malware developed in Latin America. Phishing, as an associated threat, has also spread massively during the last year and, due to its effectiveness (ESET studies confirm that a criminal in the region can get **data from seven credit cards an hour with an active attack**), will continue to operate next year. The monitoring of Brazilian attackers who spread banking trojans, carried out by the ESET Latin America's Lab team, indicates that during 2011, more than 60 propagation campaigns were launched and in those months they obtained at least 200 thousand email accounts to use for spam dissemination, for the purpose of perpetuating the infection cycle.

To sum up, Latin American criminals are still focused on threats that, in spite of being a little bit dated technologically speaking, continue to work extremely efficiently as a means of infecting users in the region.

Conclusion: a new era?

For many years, users witnessed a certain stability regarding the nature of malicious code: primarily these were worms and Trojans, distributed by email and social networks, which infected users and focused on information theft.

Today, the mobile world and the new platforms draw forth a wider diversity of malicious programs since these devices generate new usage patterns and habits in users. Not only because they have a greater amount of sensitive information available online, but also because modern mobile devices allow access to systems that previously were normally accessed through desktop computers. Information theft from smartphones now not only represents access to a contact list, but also to confidential files, private images or even passwords for sensitive systems.

This opens the door to new attack vectors and modes, where mobile platforms have a greater significance, though the continued existence of threats for desktop computers shouldn't be forgotten. Users will have to be aware of the value of the information they transport in their mobile devices day after day, and to understand that they not only can compromise their confidentiality while using web services but also by the loss or physical theft of mobile devices.

This does not necessarily represent a complete migration of malware to mobile devices, nor the rise of a new era; however, it does imply a series of changes in the malware scenario towards unequivocal cybercriminality.

In addition to the greater take-up and sophistication of mobile devices, one of the phenomena behind these changes is the resurgence of old acquaintances in the malware methodology arena, such as the [Induc case](#) towards the end of 2011, or the upsurge of [BIOS rootkits](#). In this way, we will witness the rise of a greater range and complexity in malicious codes that are becoming more frankly cybercriminal.

Furthermore, we will still see major growth in technologically unsophisticated threats. Therefore, during 2012, the most important malware cases will certainly be at both extremes of the technological complexity threat continuum.

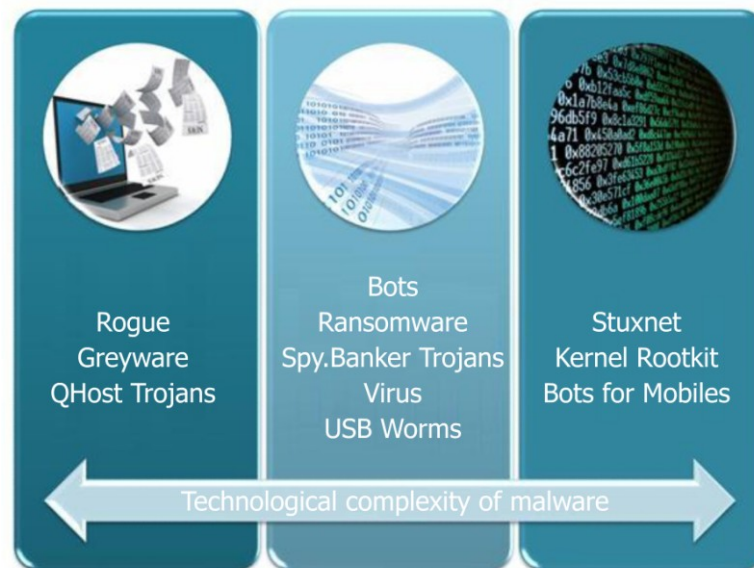


Image 5: Threat complexity spectrum

This polarization of threat sophistication implies a greater challenge for the final user because:

- The most complex threats appear less frequently but their impact can be very high.
- The simplest threats are easily accessible to developers with malicious purposes and their use can also have a massive impact.

This second point is quite relevant: there will be no botnet or rogue in particular that represents a high infection rate, or at least they will become more unusual. Instead, we will witness the massification of botnets all around the world and of fake antivirus programs that infect the users. However, this will be paralleled by a complementary diversification; this implies that each one of them will propagate in low numbers, which will be enough to generate profitability for criminals while reducing the attack surface.

Therefore, this trend will represent a risk for the user, since the lack of threats that stand out can induce a **sense of false security** when, in fact, statistics will show that the users are still being infected. In 2011, 80% of the users surveyed by ESET Latin America reported having suffered from an infection, almost as many as in 2010 (84%).

In this way, we can conclude that the ease with which attackers can multiply and diversify threats and threat variants will represent a new challenge for 2012: trying to achieve holistic protection from all kinds of malicious codes, regardless of technical complexity.