

Trends for 2011: Botnets and Dynamic Malware

By: ESET Latin America's Lab
Date: November 22nd, 2010

Additional material by David Harley, ESET LLC, January 6th 2011

Contents

Introduction	3
Botnets: the End of Static Malware	4
Costs.....	6
Botnet Administration.....	8
Botnet Dismantling	10
Multiplatform Malware	11
BlackHat SEO Attacks and Social Networks.....	13
The “Usual” Trends	14
Vulnerability Exploits.....	14
Social Engineering.....	16
Privacy and Social Networks	17
Latin American Attacks	17
Conclusion.....	18
References	19

Introduction

Having analysed the most relevant aspects of this year's computer attacks and the malware development industry, ESET Latin America's Research Team has created this report to summarize the **main trends for 2011** as regards malicious programs and antivirus security.

Crimeware (malware related to computer crimes committed in order to gain financial profit), which was predicted a year ago as the main trend for 2010, has proven its maturity by the increase in the number of malicious programs to which the term can be legitimately applied, as well as the increase in the proportion of this kind of malware to more traditional malicious code.

Botnets appeared in connection with both cybercrime and malware. The activities of most botnet administrators (at least the type of botnet reliant on bot Trojan malware with which ESET is usually most concerned) have always been illegal in most jurisdictions: there are few countries where there are no laws against the creation of malware for purposes of unauthorized access, unauthorized modification, the unauthorized use of system resources, and so on. So simply infecting someone else's machine in order to recruit it into a botnet is a criminal act, before we even start to consider the criminality of some of the activities carried out by botmasters (spam dissemination, Distributed Denial of Service attacks, click fraud and so on). A botmaster for hire who specializes in renting out botnets often doesn't care whether they're used for frankly criminal purposes, for hacktivism bordering on cyber-terrorism, or out of enthusiasm for hacking (in the broadest pejorative sense of the term) and even misplaced idealism. However, while botnets in this category have existed and been developing over many years, we can now make a useful distinction between such networks and other networks implemented by or on behalf of unequivocally criminal gangs with the express purpose of carrying out organized crime.

Botnets are comprised of zombie computers in a virtual network, controlled by an attacker with the intention of using them as a resource for achieving his own malicious ends. Botnets will be the major player in the crimeware arena in 2011, continuing the trend observed during 2010: an increase in numbers of this malware type, of active zombie networks and of overall volumes of zombie computers. In the same way, the profits achieved by the administrators of these networks will also increase; there will be further innovations in botnet technology, and the community will be more concerned at the need to shut down this kind of criminal network.

These and other anticipated malware trends for the year 2011 are described in detail below.

Botnets: the End of Static Malware

Several years ago, when creating malicious code, the malware developer had to decide what tasks it would perform once it had infected a system: among other things, which files it would modify, which registry keys it would alter, which pieces of information it would capture, or to which hacker's address it would send the data. With the rise of the backdoor trojan [1], the first hints of **dynamic malware** appear. By dynamic malicious code, we mean malware that first infects the system and then, by creating a covert channel between the compromised computer and the remote attacker, a variety of tasks can be carried out without the complicity of the computer's legitimate user, changing over time and continuing as long as the computer remains uncleaned.

In the last few years, the backdoor trojans have largely been superseded by bot trojans, developed to build networks of infected computers. **Botnets** [2] are the **confirmation of** the onset of **dynamic malware**, combining with organized crime to allow the botnet: administrator to exploit zombie computers anytime to carry out various computer crimes, such as stealing information, performing Internet attacks or sending spam, among other misdeeds.

What do we expect to see in 2011? A higher number of botnet networks implies an increase in the amount of the bot type of malware. Therefore, many more users are likely to be affected by this threat. Moreover, the volume of malicious programs of this kind will be significantly higher in proportion to the volume of *all* current malware. In the case of a user with a compromised computer, the chances of undergoing a botnet infection will be higher and will happen more frequently; in other words, **an infected computer will probably be a zombie computer**.

According to statistics extracted from ThreatSense.Net®, ESET's scanner-based Early Warning System, malicious code of this type has increased in 2010, and we believe that this trend will continue and will become more established during 2011. For instance, when comparing October 2009 with the same month in 2010, we can see how the malware family identified as *IRC/SdBot*, which represented 0.24% of all malware detections by ESET products during October 2009, represented 0.49% a year later. In other words, while in a particular month in 2009, up to 1 in 400 users had systems compromised by that threat, in 2010 up to **1 in 200 users may have found that same botnet variant** in their systems, as the following table explains how the detection percentage of different signatures has increased between 2009 and 2010, according to detection statistics provided by ThreatSense.Net:

Signatures	Malware detection	
	2009	2010
IRC/SdBot	0,24%	0,49%
Win32/IRCBot *	0,15%	0,24%
Win32/Zbot	0,09%	0,23%
Win32/AutoRun.IRCBot *	0,03 %	0,18 %

* All the associated variants

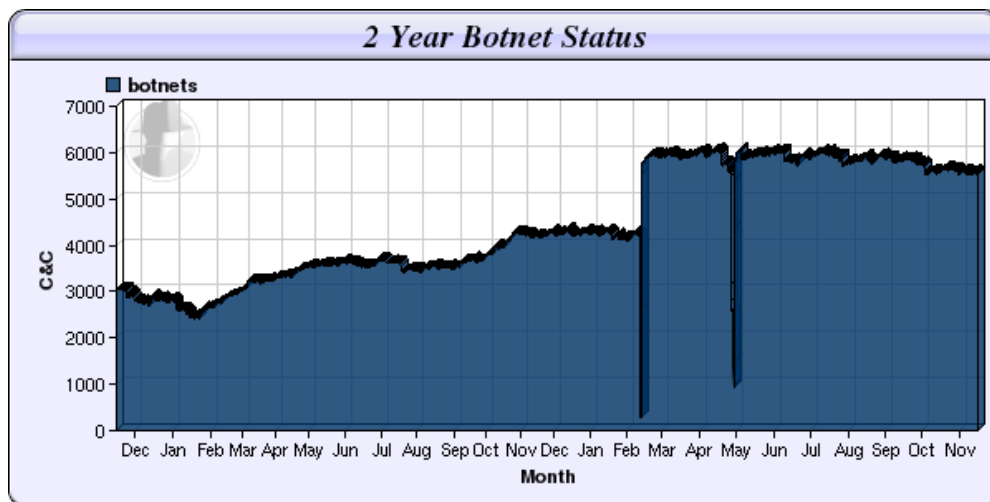
As a result, these data show that among users of ESET security solutions, there was also an increase in the amount of times that certain threats were detected throughout the year. The following chart shows the increase percentage from one year to the next:

Signatures	Increase from 2009 to 2010
IRC/SdBot	98%
Win32/IRCBot *	66%
Win32/Zbot	130%
Win32/AutoRun.IRCBot *	139%

* All the associated variants

The malware data correspond to the statistics published by Shadow Server [3], a foundation dedicated to the analysis of digital threats, which tracks down botnet networks and publishes periodic statistics for the community.

These data indicate that by November 2010 **5,500 botnets** were detected (having peaked at six thousand during the year, in months such as May or July). This is a significant rise compared to the end of the previous year, where just over four thousand botnets had been detected. The growth of active botnet networks detected by Shadowserver in the last two years can be observed in the following chart:



If we take into account these 24 months, the increase in the amount of active botnets is estimated at approximately 85%. From these figures, **it is possible to anticipate a rise to more than seven thousand active botnet network in 2011**.

The graph shows that millions of users are affected by this threat. This figure is estimated on the basis that only three of these botnets have been taken down in 2010 (read next section): Waledac (80 thousand affected users), Mariposa (13 million) and Bredolab (30 million).

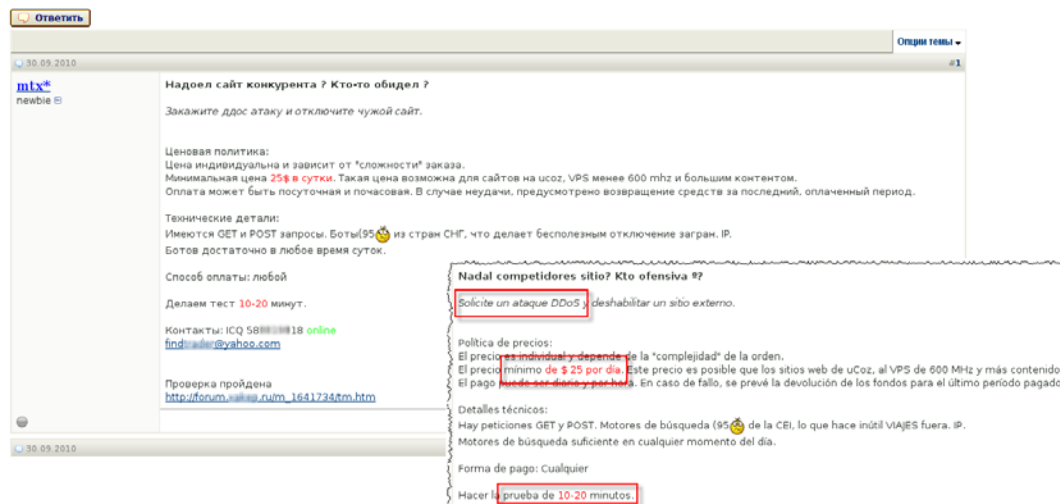
Costs

What is the cause of such a high number of botnets and compromised systems? Basically, money: the low outlay required for criminals to get administration panels or bot malware, and the disproportionately large sums they can obtain by exploiting the criminal services offered by these networks.

The marketing cycle explained in the report published by ESET Latin America in April 2010 [4] summarized some of the costs associated with these malicious technologies:

- A hacker could rent a server on which to store malware, exploit kits or botnet components, among other threats, for only **USD 80 to USD 200** a month.
- The botnet administration pack known as the Eleonore Exploit Pack has a value of **USD 1,000** (version 1.3). Hiring a botnet of between 10 and 20 computers, administered using the pack mentioned above costs an average of **USD 40 on a daily basis** (which means that an administrator could recoup the investment in only 25 days!)
- Other botnet administration kits have different costs, according to their attributes and popularity:
 - Zeus kit v1.3: USD 3,000 / 4,000
 - YES Exploit System v3.0: USD 1,150
 - Fragus v1.0 : USD 980

The following image shows starkly how a **denial of service attack** is commercialized on a Russian forum, with **costs ranging from 25 dollars upwards**, and it's possible to **try it out for 10-20 minutes for free** :



More costs of this kind are revealed in the complete report "Costos del negocio delictivo encabezado por el crimeware" (*Costs of the criminal business led by crimeware*) [4].

At the same time, the profits botnet administrators can expect increase daily, encouraging hackers to create and make use of them. For example, a recent study revealed that the **Koobface botnet reaped a**

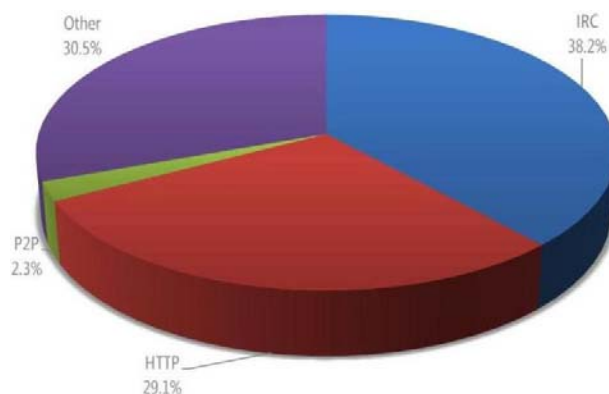
profit of more than two million dollars between June 2009 and June 2010. In countries like Russia, where botnets propagate faster than in the rest of the world, various studies indicate that even a small bot network has managed to gain **profits that exceed a million dollars in one month**. In other words, not only are the costs to use these networks relatively low, but also the potential profits are extremely high compared to any current legitimate business.

If we picture what goes on in the mind of a malware developer, whether he's a hacker for hire or working within organized crime, and considering the presented figures: what is the sense of developing new variants of static malware when it is possible to use malicious code of the bot type already available in the marketplace, at affordable cost and with extraordinary profitability? The answer to that question is the main reason why botnets will continue to increase during next year and infections of this kind will be progressively more frequent compared to other forms of malware infection.

Botnet Administration

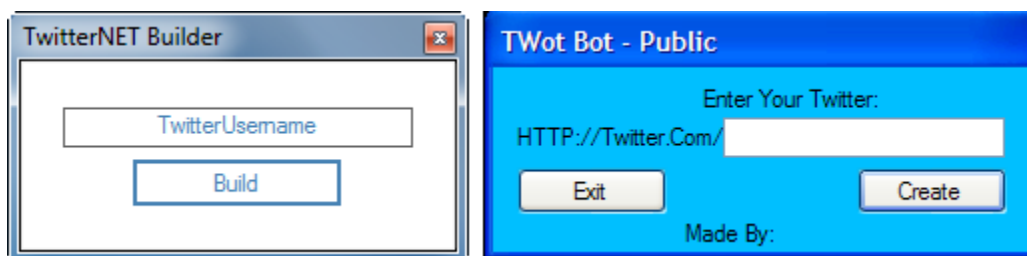
During 2010, new ways to administer botnet networks appeared, apart from the traditional use of protocols such as IRC and P2P, or more modern ones, through HTTP. While earlier administrative methodologies continued to survive, we have observed a clear tendency to make use of the web protocol, alongside newer forms of botnet administration. According to reports on the ESET Latin American Lab's Blog throughout the year, there is a persistent decline in botnets that use channels that were formerly more popular, such as P2P.

Microsoft statistics [5] tally with the behavior that has been observed and reported by ESET Latin America's Lab during 2010: the protocols that are most frequently used for the administration of these networks are IRC and HTTP, as shown in the following chart:



Nevertheless, apart from the decrease in botnet networks through peer-to-peer, there is also a high percentage (30%) of unconventional administration methods, a figure that will probably rise during next year, especially with administration methods through social networks.

During 2010, ESET Latin America's Lab has noted the particular use of two different tools used for the creation of bot malware, which allowed the **control of zombie computers through Twitter** [6]. The malicious codes, detected by ESET as *MSIL/Agent.NBW* and *MSIL/TwiBot.A* respectively, allow the infected system (zombie computer) to wait for instructions by reading the Twitter contents published by a particular user, indicated at the time of the malware's creation with these tools:



Consequently, by publishing entries in his Twitter account, the hacker can make all the zombie computers follow his instructions, such as sending spam, executing files or performing denial of service attacks, among others [7]. Even in this manner, the possibility for a botnet administrator to send instructions to

zombies directly from a mobile device is made easier: he is able to launch attacks, massive spam email campaigns or other crimes straight from the palm of one hand.

It can be expected that next year this kind of botnet will be more frequently seen and will be controlled by unconventional methods, in particular through social networks, since it these are not usually blocked by the victim's Internet provider.

Botnet Dismantling

The botnet growth rate gives rise to another problem: how can we bring this threat to an end? Taking into account the number of existing networks (as indicated in previous sections), it is practically impossible to terminate all of them, which is why it is important that the user maintains protection against the infection of his system. However, in relation to those botnets with a large number of users, or with an important impact on the criminal scene, it is possible to take different actions to dismantle the botnet network, a process known as *takedown*.

During 2010, three important networks of zombie computers were dismantled:

- **Waledac** [8], a botnet network that sent out pharmaceutical spam – which had a life of almost two years – was dismantled in February 2010, after the shutdown of 277 domains it was using. The order was given and imposed by the federal court of Virginia, in the United States [9], and **ESET participated in the process by offering information through its professionals and researchers** to the local security forces.
- In the same month, the Spanish Civil Guard dismantled a network of zombie computers known as **Mariposa** (*Butterfly* in Spanish), which was administered by three Spanish citizens [9].
- On October 25th, 2010, the Dutch government shut down the botnet known as **Bredolab**, which was well known for its theft of banking account credentials. Over the years, it affected more than 30 million users [10]. Anyway, it is estimated that by using new variants, their creators managed to keep part of the network structure active [11].

Moreover, there have also been "partial" successes against the servers of other important botnets, such as Koobface in November of 2010[12].

In the future, collaboration between security companies, independent researchers or organizations and the security forces of the countries will be more frequent, and together they will try to carry out such campaigns in their efforts to dismantle the most important botnet networks. Up to date, ESET and the

industry are already collaborating with some security forces, providing information related to active botnets.

Multiplatform malware

Throughout 2010 various platforms have been affected by malware variants. While Windows continues to be the platform most widely exploited by malicious code (**84.3% of users who responded to our survey became infected with malware** during the year [13]), other platforms have also been affected:

- The most popular open-source operating system, **Linux**, suffered from some malware attacks such as a Trojan pretending to be a screensaver and found in legitimate software repositories [14], or a backdoor Trojan that remained active for more than 6 months in the official repository of Unreal IRC software [15], among others.
- Mobile devices have not escaped this trend, and the number of operating systems affected by first versions of native malware has increased. For example, consider the case of the first Android SMS Trojan [16], which was reported in August of the current year. According to ESET's investigations, **malware for mobile devices has increased 95% between 2009 and 2010.**

A more profitable alternative for malware developers is the creation of **multiplatform malicious code**: in other words, files that can affect different platforms with one purpose in common, or using a common infection model. An example of this trend was observed at the beginning of the year: namely, an experiment designed to create botnets on iPhone and Android mobile platforms, compromising more than 8 thousand devices [17].

This trend was confirmed by the end of the year, after the appearance of a new Trojan closely resembling Koobface, known as Boonana and identified by ESET with the *Java/Boonana.A* signature [18]. This variant involved the first multiplatform version of a Trojan that has been active since 2008 and, two years after its initial creation, has begun its propagation beyond the Windows systems, infecting Linux and Mac OS as well.

In this context, botnet networks are one of the best alternatives for multiplatform malware. Is it at all relevant for the attacker whether the spam is sent from a system running Windows or Linux? Does it make any difference to the botnet administrator if banking credentials are stolen from a Mac OS user via his laptop from a Symbian user accessing a home banking service through his mobile device?

The following image shows how a botnet network has infected computers from different platforms, in differing proportions that confirm our explanations above.



Operation Systems:	Totals:
Windows XP	23529
Windows 7	4060
Windows Vista	1585
Linux	168
Mac OS	162
Windows 2000	115
Windows 2003	111
Mobile phone	76
Unknown OS :(25
Power PC	25
Windows 98	22
Symbian OS	15
iPhone OS	11
Windows ME	5
Windows 95	3
Bots	2
Windows NT 4	1
PlayStation	1
Nintendo Wii	1

It will also be noticed that this particular botnet has affected a PlayStation and a Nintendo Wii system. Although they have not been seen propagating through the network, the image demonstrates that the hackers are already working on extending the range of platforms that may be turned into zombies.

With multiplatform malware, the malicious code used by hackers infects successfully, regardless of the platform the victim uses, and it is to be expected that the trend will keep on rising throughout next year.

BlackHat SEO attacks and social networks

Nowadays, practically no Internet user goes a whole day without making web searches or using some social network. Hackers do not ignore this fact and will not next year; they will incorporate new trends based on attacks that already exist for the following two services:

- **Social Networks:** the growing volume of users has been reflected in the growth of threats propagating through these networks. In 2010, Facebook has exceeded 500 million users, and other networks like Twitter or MySpace have also reached over 100 million users – all of them are expected to keep on growing. Different threats propagate through social networks [19], such as malware, phishing, spam or scam, and will continue doing so, making use of all the popular social networks, or any networks whose users are willing to follow their contents and links.
- **Browsers:** the BlackHat SEO (Search Engine Optimization) attacks [20] fundamentally consist of the prominent appearance in browser search engine results of links to sites that contain malware (or other malicious content). They are characteristically associated with topics of general interest or current events and leading news, both globally or regionally. For example, in 2010 the World Cup was one of the events most exploited by BlackHat SEO attacks [21]. Malware is closely linked to this threat, especially rogue AV and other security utilities. According to Google, fake software represents 60% of the malware associated with keyword searches [22].

What is to be expected in this respect for 2011? First of all, hackers will continue to refine and optimize BlackHat SEO techniques. Firstly, optimizations will concern what is called positioning time: the delay between the occurrence of an event and the location of poisoned results in browsers by BlackHat SEO. According to various investigations, hackers can locate their first poisoned links in browsers in less than 24 hours after the occurrence of an extraordinary event; and in respect of planned events such as public holidays they can manage to place results of this kind at the top of search lists even before searches on those terms start to increase, according to Google Trends, a service that measures search trends.

Secondly, the combination of BlackHat SEO with social networks will cause the poisoning of the results of these networks in order to steer users towards malware or other attacks. The social web has been lately characterized by the optimization of its searches, particularly those performed in real time. On the other side, browsers are starting to show not only websites but also results from social networks (a page from Facebook, a tweet from Twitter, and so on.) Therefore, a new form of BlackHat SEO is appearing based on social networks, where it is no longer necessary for hackers to create poisoned websites. They can achieve the same ends directly do it by means of false profiles in social networks (or from the profiles of infected users) generating content which links to malware.

A clear example of this approach is the use of hashtags in Twitter for the follow-up of real-time events. A hacker could create hundreds of false profiles in Twitter and generate content with that particular hashtag every 10 seconds, therefore appearing in all the real time searches made worldwide, and even probably achieving a good positioning in the results shown by browsers. This type of attack will be more frequent in 2011, provided that browsers and social networks keep on optimizing their relations at the search level.

User awareness will have a critical impact in this situation. Various surveys conducted by ESET Latin America indicate that half the user population considers that there is no risk from malicious code when accessing social networks [23]. Social networks are becoming the Internet axis and hackers are not oblivious to this fact: consequently, they are focusing the design of their attacks so that they are effective among users of these networks.

The "Usual" Trends

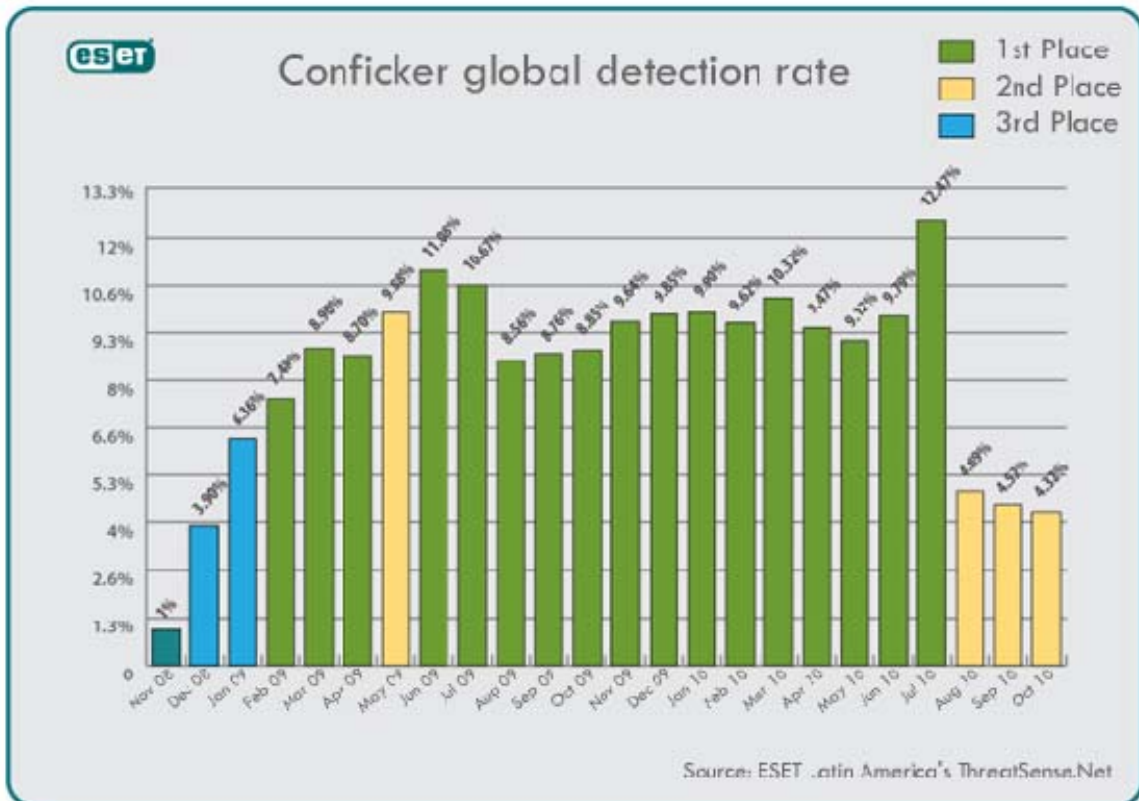
While some upcoming trends are based on new attacks or emerging technologies, others are simply the continuation of malware types or attack vectors that were already known in previous years, but that remain relevant nonetheless due to their continuing effectiveness against users.

Vulnerability Exploits

Software vulnerabilities will remain one of the most important infection vectors for malware creators, since they allow the execution of code without user intervention, and therefore the victim may not notice the infection until anomalies appear on his system.

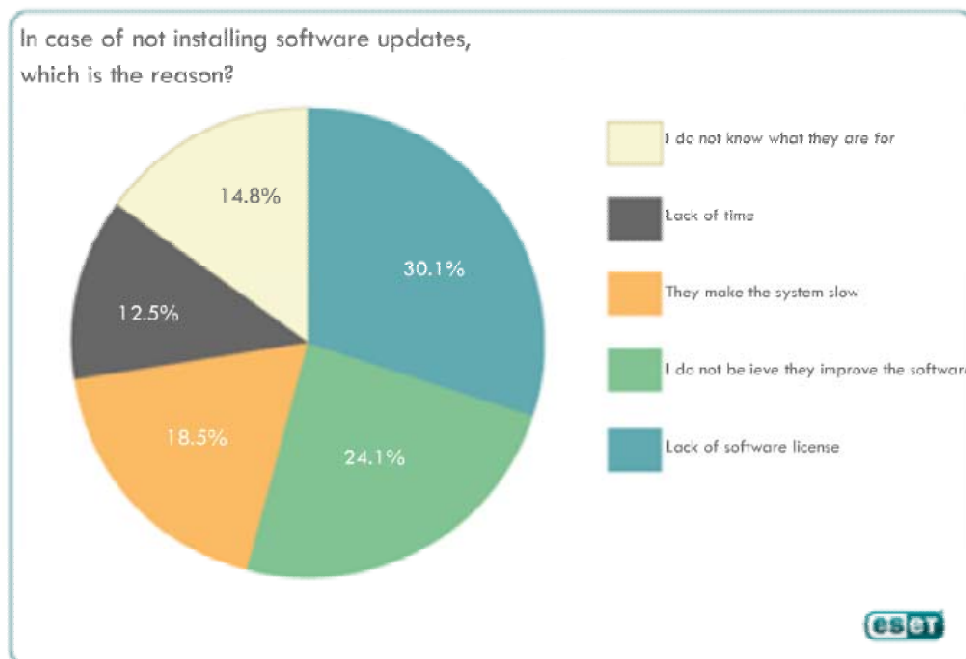
In this context, zero-day vulnerabilities (those for which a security patch is not yet available) represent an opportunity for hackers, and they will continue to seize such opportunities as they arise. In cases that occurred during 2010, such as the Stuxnet worm, ESET Latin America detailed the attack chronology, and its analysts indicated that it took "**16 days since the vulnerability was published until a conclusive patch was created** by the developer, a time window during which several malicious programs took advantage of the situation, generating large volumes of problems in the computer environment by breaching information security" [24]. Only those users that had antivirus software with proactive detection capabilities, such as ESET NOD32 and ESET Smart Security, remained protected during that "time window" in which the vulnerability remained at the hackers' disposal to use to propagate their threats.

Nevertheless, it is not only zero-day vulnerabilities are exploited by hackers: any type of vulnerability represents an opportunity for malware developers. For example, the Conficker worm has been active since October 2008, and more than two years later it is still active and frequently tops the rankings determined by ESET Latin America of the most frequently detected malicious programs for each month.



In other words, regardless the existence of a patch, vulnerabilities will continue to be exploited by malware. Worms of this kind will probably be the threats that stand out next year due to their high infection rates.

In this regard, the role of the user and the use of non-licensed software stand out as fundamental factors in this continuing scenario. According to the 2010 statistics, **29.5% of surveyed users** pointed out they **are not used to installing security updates**. When asked why they do not install the patches, these were the reasons [25]:



That is to say that the main reason why application security updates are not installed is the **lack of software license**. This fact is particularly pertinent: **three out of ten users do not keep their systems safe because they have non-licensed versions of the software**. In regions like Latin America, where the piracy rates are especially high, this represents an extremely important risk for computer users. Countries like Venezuela occupy the first place among countries using applications without licensing them, with a rate of 89.7%, followed by others such as Paraguay (82%), Guatemala, Bolivia and El Salvador (all of them with 80%). Even countries like Uruguay (68%) or Peru (70%), that hold the lowest rates, also represent high proportions that exceed half of their users.

Social Engineering

In accordance with what was presented in previous sections, regardless of the platform that is being used, beyond the screen there is always a user. We do not underestimate the impact of malware that exploits application and platform vulnerabilities, but exploiting the user is another way of propagating threats, and Social Engineering is the most effective way of doing this, and such techniques will still be used by hackers in 2011.

For next year it is clear that some known facts will most probably be exploited by malware creators, such as the “Copa América” football competition, the Rugby World Cup (sport events seem to be particularly effective social engineering “hooks”) or political events, such as the Argentine and Peruvian elections that will take place next year.

Privacy and Social Networks

Another core issue of concern among users next year is the privacy exposed in social networks. The applications and patterns of usage that are prone to expose the users' personal information (albeit with their consent) to risk will keep on rising, and alerting users to the need to take care of their data will be essential mitigating those risks.

Likewise, incidents associated with social networks and information leaks [26] will be both frequent and widespread, and those resulting in information exposure will have to be addressed by users in order to protect their published information, modifying credentials whenever necessary.

Latin American Attacks

As was announced by the ESET Latin America's team in 2010, the Latin American region is not merely a malware and attack recipient anymore: malicious codes and other threats are being actively developed in the region, a trend that keeps growing and will continue to evolve in future years.

In 2010 all kinds of attacks were generated in the region, many based on Social Engineering, as happened recently with the Chilean miners (or at the beginning of the year with the earthquake in the same country), or the political situation in Ecuador and Venezuela, all of them exploited for malware propagation [27]; the continuity in the creation of bank Trojans in Brazil [28]; and also several countries in the region (like Argentina and Brazil) standing out globally due to the amount of spam sent [29] and even the creation of botnets in countries such as Mexico or Argentina [30].

Phishing is another threat whose growth is particularly noticeable in Latin America and that is developed exclusively by local or regional attackers, especially when they try to obtain bank credentials belonging to Latin American institutions. In countries like Brazil, the amount of phishing observed in the third quarter of 2010 represented a **rise of 150%** on a year-over-year basis [31].

Attackers in the region are growing in number as a consequence of technological advances, ever-increasing access to the Internet and to information, and the growth of the cyber-criminal community, which is not going to go away.

Conclusion

As observed throughout this report, all the trends considered here are interrelated in one way or another: the number of botnets will increase, as will as multiplatform malware; and precisely it's exactly efficacy of the botnet attack that will offer that access across different operating systems. At the same time, there is still a trend towards the creation of spam-generating botnets in Latin America, and countries in the region are among the most problematical in the worldwide distribution of bot malware. On the other hand, there are also zombie computers that are created in the region, usage of localized Social Engineering techniques, which are also related to new trends such as the use of BlackHat SEO techniques in social networks.

These associations sum up what happens with malware nowadays: their close relationship to the business of organized cybercrime and its professionalization across the globe.

Some of these statements, which just a few years ago would have seemed indefensible, **will be confirmed during 2011:**

1. The malware development industry is largely made up of professionals who create their malicious codes for financial gain, and who are associated with career criminals.
2. Malware does not only affect Windows systems, but also impacts on other operating systems and even on different platforms such as mobile devices.
3. Once malware infects a computer, it can perform several criminal tasks: the harm done by modern malware is dynamic and unpredictable.

The most important fact, as has been highlighted throughout the whole of this report, is that this final point becomes truer by the day: **an infected computer is a zombie computer**. This initial fact is the one that drives the other trends presented in this report: dynamic malware offers attackers new alternatives, greater financial benefits and a special connection with IT-related criminality executed from infected computers.

References

- [1] <http://www.eset-la.com/centro-amenazas/amenazas/2136-Troyanos>
- [2] <http://www.eset-la.com/centro-amenazas/1573-botnet-redes-organizadas-crimen>
- [3] <http://www.shadowserver.org>
- [4] <http://www.eset-la.com/centro-amenazas/2313-costos-negocio-delictivo-crimeware>
- [5] http://www.microsoft.com/security/sir/story/default.aspx#section_2_2_1
- [6] <http://blogs.eset-la.com/laboratorio/2010/05/14/botnet-a-traves-twitter/>
<http://blogs.eset-la.com/laboratorio/2010/08/27/twitter-mira-botmasters/>
- [7] <http://www.youtube.com/watch?v=EoATrwF4DdM>
- [8] <http://www.eset-la.com/centro-amenazas/2042-waledac-troyano-enamorado;>
<http://blog.eset.com/?s=waledac>
- [9] <http://blogs.eset-la.com/laboratorio/2010/03/03/redes-botnet-desaparecen-adios-waledac-mariposa/>
- [10] <http://blogs.eset-la.com/laboratorio/2010/10/29/gobierno-holandes-cierra-botnet-de-30-millones-de-victimas/>
- [11] <http://blogs.eset-la.com/laboratorio/2010/11/03/bredolab-no-se-rinde-y-sigue-dando-pelea/>
- [12] [http://blogs.eset-la.com/laboratorio/2010/11/15/piedra-libre-a-koobface/;](http://blogs.eset-la.com/laboratorio/2010/11/15/piedra-libre-a-koobface/)
<http://blog.eset.com/2010/10/31/boonana-threat-analysis>
- [13] <http://blogs.eset-la.com/laboratorio/2010/10/13/%C2%BFquien-se-salvo-del-malware-en-el-2010/>
- [14] <http://blogs.eset-la.com/laboratorio/2009/12/10/troyano-para-linux/>
- [15] <http://blogs.eset-la.com/laboratorio/2010/06/15/troyano-para-linux-activo-por-mas-de-6-meses/>
- [16] [http://blogs.eset-la.com/laboratorio/2010/08/10/primer-troyano-sms-para-android/;](http://blogs.eset-la.com/laboratorio/2010/08/10/primer-troyano-sms-para-android/)
<http://blog.eset.com/?s=android+%2B+trojan>

- [17] <http://blogs.eset-la.com/laboratorio/2010/03/10/un-experimento-crea-botnet-en-dispositivos-moviles/>
- [18] <http://blogs.eset-la.com/laboratorio/2010/10/28/koobface-llega-a-mac-os-y-linux/>;
<http://blog.eset.com/2010/10/31/boonana-threat-analysis>
- [19] http://www.eset-la.com/centro-amenazas/2348-dudas_certezas_redes_sociales_empresa;
<http://blog.eset.com/2010/07/29/incidents-on-facebook> ;
<http://chainmailcheck.wordpress.com/?s=social+network&x=8&y=11>
- [20] <http://www.eset-la.com/centro-amenazas/2333-ataques-black-hat-seo>;
<http://blog.eset.com/?s=BHSEO>
- [21] <http://blogs.eset-la.com/laboratorio/2010/05/28/buscadores-mundial-futbol-malwar/>;
<http://blogs.eset-la.com/laboratorio/2010/05/20/mundial-futbol-2010-te-puede-infectar/>;
<http://blog.eset.com/?s=world+cup+seo>
- [22] <http://blogs.eset-la.com/laboratorio/2010/04/20/60-malware-keywords-rogue/>
- [23] <http://blogs.eset-la.com/laboratorio/2010/06/10/la-mitad-de-los-usuarios-consideran-que-no-hay-malware-en-redes-sociales/>
- [24] <http://blogs.eset-la.com/laboratorio/2010/08/16/cronologia-de-un-ataque-0-day/>
- [25] <http://blogs.eset-la.com/laboratorio/2010/09/24/actualiza-tu-software-licenciado/>
- [26] <http://blogs.eset-la.com/laboratorio/2010/10/22/facebook-android-e-iphone-fugan-datos-de-usuarios/>
- [27] <http://blogs.eset-la.com/laboratorio/2010/10/14/mineros-chilenos-malware-brasil/>
<http://blogs.eset-la.com/laboratorio/2010/07/14/caso-bruno-propagacion-malware/>
<http://blogs.eset-la.com/laboratorio/2010/11/08/politica-en-venezuela-usada-para-propagar-malware/>
<http://blogs.eset-la.com/laboratorio/2010/05/26/falsa-noticia-terremoto-chile-propaga-malware-bancatio/>
<http://blogs.eset-la.com/laboratorio/2010/02/28/terremoto-chile-japon-usado-propaga-malware/>

[28] <http://blogs.eset-la.com/laboratorio/2010/07/31/troyano-bancario-y-brasileno-%C2%BFsuena-conocido/>

<http://blogs.eset-la.com/laboratorio/2009/08/11/codigo-malicioso-made-in-brasil/>

[29] <http://blogs.eset-la.com/laboratorio/2009/08/13/spam-argentina-brasil-top-10/>

<http://blogs.eset-la.com/laboratorio/2010/06/25/crimeware-global/>

[30] <http://blogs.eset-la.com/laboratorio/2010/06/04/mariachi-botnet-latinoamerica-atacada-ciberdelincuentes-mexicanos/>

<http://blogs.eset-la.com/laboratorio/2010/11/15/nueva-botnet-argentina/>

[31] <http://www.nic.br/imprensa/releases/2010/rl-2010-23.pdf>