Playing Dirty

Cristian Borghello, CISSP
Technical & Educational Manager for ESET in Latin America

This paper is a translation of the author's paper titled "Jugando sucio";
see http://www.eset-la.com/press/informe/jugando_sucio.pdf.

Table of Contents

Introduction

"Fantasy has no limits..."

The Neverending Story, Michael Ende, 1979

...nor does the number of current examples of malware.

"The Neverending Story" seems to be a precise mirror image of what happens today: Good and Evil, represented by anti-malware companies and malware authors, locked into an "eternal" battle.

This combat is now moving onto another battlefield, into areas unknown and unexplored until recently, and affecting online game players (or gamers) who dwell in a virtual world where everything is fantasy... but also reality.

Since we were children, we have always been motivated to play games because they stimulate new abilities in human beings. Nonetheless, the new online game generation of the 21st century seems to challenge that essentially positive rule, establishing new perils of which just one will be mentioned in this paper: the way in which malware authors can take advantage of gamers.

It seems unacceptable that harmless game play can become a threat, but unfortunately malware creators have found a new way of making money in the gaming arena, ensuring that they will continue to exploit this attack vector.

Fantasy, MMORPG and Theft

Fantasy stories, literature and games have always represented one of the most entertaining ways of appealing to the human intellect, even more so when the game allows flexible and creative strategies rather than conformance to strict rules. This appeal fueled the popularity of the role-playing games[1] that appeared in the 1970s in the U.S., when the development of Dungeons & Dragons[2] launched the era of the role-playing game.

These games also have an online equivalent, based on the connection between a client (gamer) and a server (where the game platform is executed and administered). At the very beginning, these types of games had at most a basic interface, evolving into the MUD[3] (Multi-User Dungeon). This was generally text-driven and did not require additional tools or software apart from a terminal network connection (usually telnet or similar).

In time, these evolved naturally into an exceptionally sophisticated interface, enabling greater player interaction, and leading to the advent of the contemporary MMORPG (Massive Multiplayer Online Role-Playing Game).[4] Such games allow thousands of gamers to interact simultaneously in a virtual world distributed throughout the Internet; as a result, a great deal of time is invested in playing. According to one research paper,[5] 70 percent of game players spend more than 10 hours at a time in a single session in an MMORPG game.

The MMOG (Massively Multiplayer Online Game)[6] has recently appeared, inheriting some of the original MMORPG components, but available for any kind of computing platform that can access the Internet, including PlayStation, Xbox, Wii and other game consoles.

This sort of game is based on a virtual character (avatar), whose life develops within an environment pertaining to the game. Each avatar is capable of interacting with its peers in different adventures, and gains rewards of social, political and economic experience, as well as treasure, weapons, garments and evolutionary attributes, according to the aspects and features of each particular game.

In short, each avatar (virtual representation of the "real" person) takes part in a fantasy story, in a fantasy world that enables it to evolve, but the action takes place in the virtual company of real players (physical persons), in real time, with real information and real losses (of time, money, the avatar, etc.).

Cybercriminals are particularly interested in getting hold of this information, since it represents a viable source of income from stealing real money in spheres where fantasy gives scope to real-world fraud and theft.

Reality and Million-Dollar Transactions

Games on virtual platforms became popular in the mid-1990s in Asia (mainly China and Korea) with games such as The Golden Age, EverQuest and Lineage. However, the greatest boom took place at the beginning of the 21st century with the release of games like World of Warcraft (WoW), Dark Age of Camelot, Legend of Mir (LoM), Second Life (based on the science-fiction book Snow Crash), Tibia, RuneScape, Habbo and the Lineage sequel.[7]

Nowadays, the MMORPG market represents a multimillion-dollar business[8] where hundreds of games struggle to outmatch their most famous and popular predecessors and competitors, such as WoW, which already has more than 10 million subscribers and owns 62 percent of the market, and Lineage, which had already exceeded 3 million subscriptions by May, 2007.[9]

To better understand what happens in these games, the following should be taken into account:

1. Some of these games require a paid registration or subscription (often called VIP) to access the server. In many games, people can play for free, and, in others, the gamer is offered a dual-mode subscription (combining paid-for and free access), allowing regular but restricted access and game play.

2. Each avatar acquires virtual commodities as he or she evolves, giving him or her increased value.
3. Each gamer invests a great amount of time into developing his alter ego, which can then be resold to other gamers wishing to experience or to play with a more developed or evolved avatar.
4. Interaction among gamers tends to require the acquisition of money (or other commodities) in order to perform exchanges, trades or commercial agreements, or simply to sell or purchase other objects and skills pertaining to the game.
5. The virtual money traded in many games corresponds to real money in the physical world. For example, in Second Life, one dollar fluctuates between 250 and 275 Lindens (L$).[10]
6. If an avatar reaches a high enough level of evolution, it may be able to gain access to large amounts of money and resources.

In other words, millions of users have found a way to become virtual and actual "millionaires," which is highly relevant to the interest that malware authors have shown in gaming.

Malware creators have overlooked the profit potential of gaming in the past, but the high profit potential of these gaming platforms has now attracted their attention, since by controlling the gamers' virtual resources it is possible to control the access to the real money invested in the virtual world.

The use of malware to take advantage of game players and gaming software reflects the pattern seen in the original gaming boom. Exploitation of gaming by malware started in Asia in 2006 (at the same time that Second Life started to excite the attention of the media), and most attacks are based on the same principle: the use of social engineering[11] to trick gamers into revealing their credentials (username, password and any other kind of exploitable information).

The graph below (Figure 1) shows malware growth in relation to the MMOG:

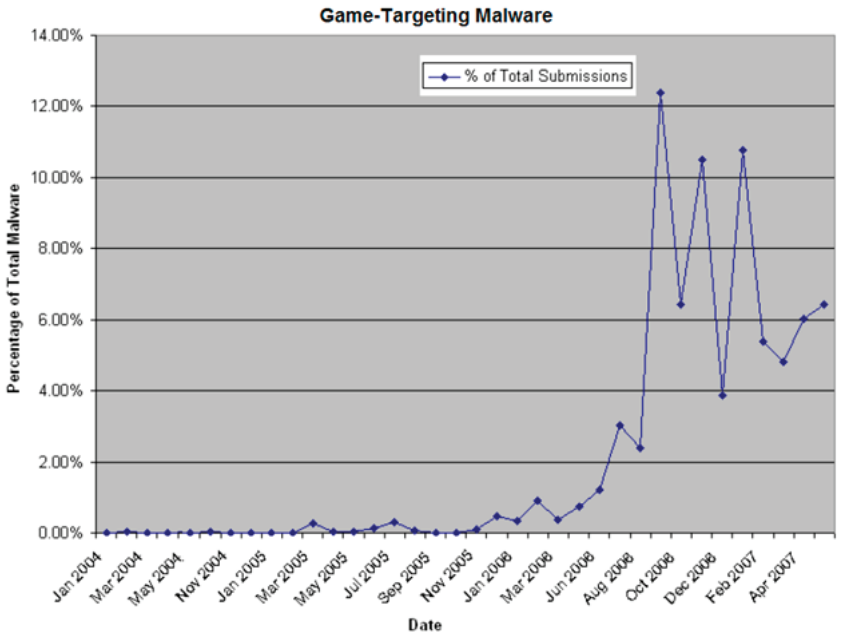

Figure 1: Malware growth in the last three years
Source: Virus Bulletin Conference, 2007

By the end of 2006 and into 2007, ESET Latinoamérica had become aware of the considerable importance of preventing this type of attack[12] because critical mass had been achieved in attacks on gamers in the U.S. This trend was highlighted in ESET's June 2008 ThreatSense report, where it is evident (see Figure 2) that the Trojan family detected by ESET as Win32/PSW.OnLineGames reached the first place in the "Top 10" with an impressive lead.[13] This class of threat has continued to be highly ranked, according to ThreatSense.Net® throughout 2009. Indeed, it persists in the top two to three, generally alternating with Autorun exploiting malware and (more recently) Conficker in the top spot.

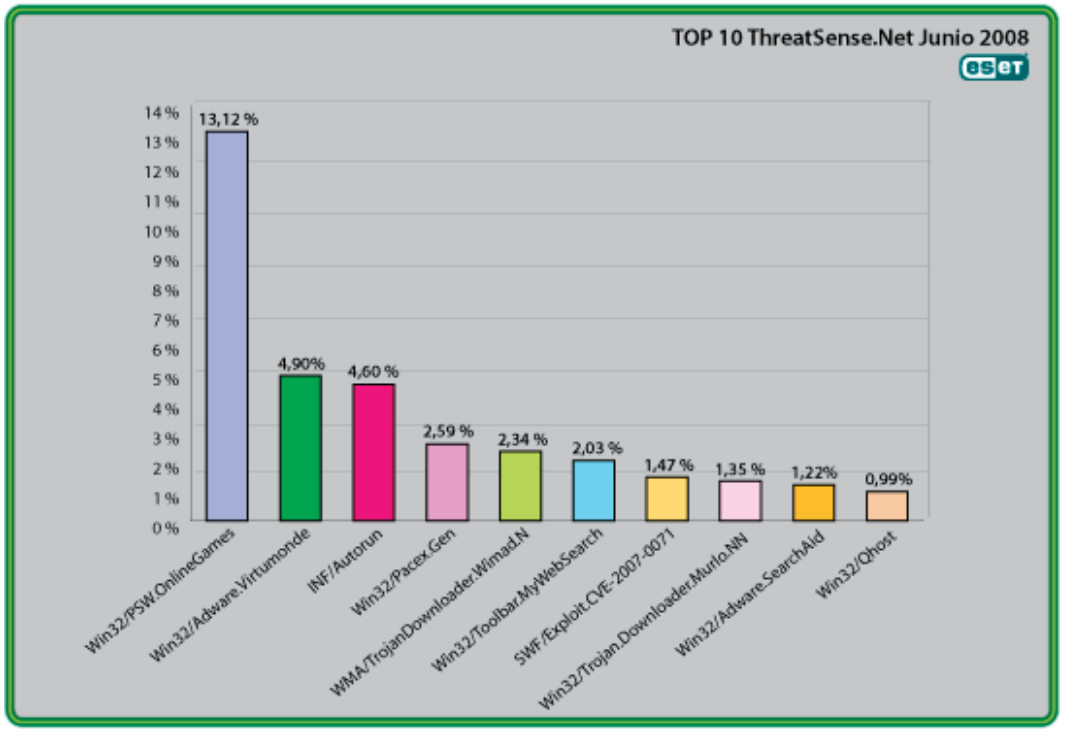

Figure 2: ESET detection ranking in June 2008

Information-Stealing Methods

The methods used by malware to take advantage of MMOGs, and as a direct consequence, of their users, have evolved from rudimentary techniques in the beginning to the much more sophisticated techniques used currently, taking advantage of a wide range of vectors such as :

- Drive-by downloads
- Banner ads
- Malicious URLs posted in chat rooms, web forums, Instant Messaging and so on
- Third-party add-on applications

Nevertheless, they all have the same primary purpose.

That is, the theft of sensitive data from the user so as to gain control of the avatar and its attributes.

The main methods used to obtain user information are as follows:

- Installation of Trojans onto the gamer's system, such as password stealers and keyloggers
- Monitoring of system activities, waiting for an event to take place (for instance, the start of the game)
- Gaining control of the log system and game files in order to gain information
- Searching for registry keys and files that may be open to compromise
- Interception of the calls the game makes to the operating system
- Use of hooking techniques to intercept game calls
- Monitoring of web traffic to capture the information transferred between the game server and the client
- Injection of code into different system processes

Once the malware determines that a game is installed in the system, or that the game is now running, it starts to perform some of these activities in order to collect the information it is programmed to gather:

- Username
- Passwords
- Data concerning the server used
- In the case of paid service subscriptions, financial information such as credit card numbers, expiration dates, PIN (Personal Identification Number), and so on.
- Gaming information such as sums of money transacted; evolution, equipment, defense, intellect, speed, number and types of objects; role, occupation, game level, maps, genre, and so on.

The stolen information is then transferred to the cybercriminal by different methods such as the use of a website controlled by the attacker (by HTTP Post), an FTP server, via email (by means of the criminal's own SMTP server), or other open or encrypted communication channels, depending on the type of malware used.

The main target platforms for stealing such information are the most popular and widespread games such as WoW, Lineage I and II, LoM and Second Life, but the similarities among the games, in terms of the registration methods and the data required to play, make it possible for current malware to be easily modified and adapted to other games if necessary, bringing into potential existence thousands of different variants.

Analysis of a Particular Case

Next, we will analyze a sample of the malware family detected by ESET as Win32/PSW.Lineage, specifically developed for the game Lineage II, Chronicle 4.

This malicious program is a Trojan with keylogger and rootkit functionality[14] that uses websites, P2P (peer-to-peer) networks, emails or removable devices such as USB drives and flash media in order to proliferate.

Once the malware has been downloaded to the system and executed, it hides its activities from the system and intercepts the initiation of game play, where the user is prompted to enter his credentials (see Figure 3).

Rootkit functionality hides the malicious software processes from the system and the user. By using ESET's free utility SysInspector[15] however, the executables responsible for the keylogging can be found in the directory X:\windows\system32 (where X:\ stands for the system drive) (see Figure 4).

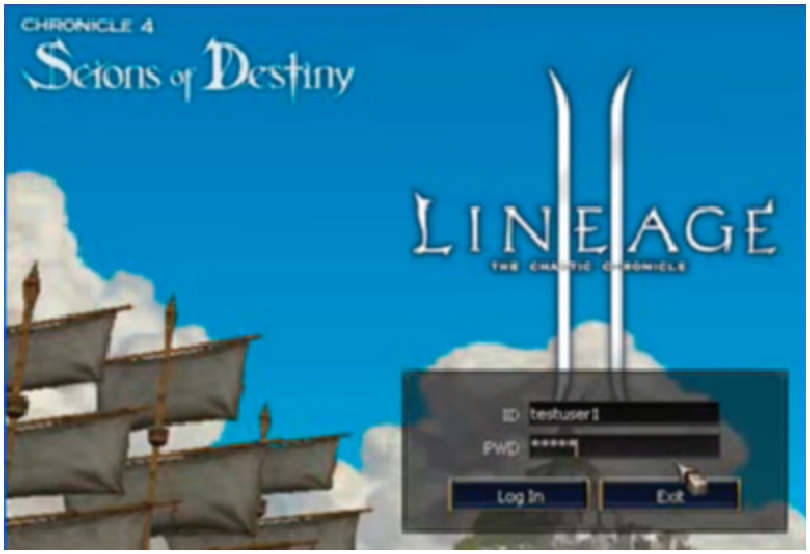

Figure 3: Credential request in Lineage II

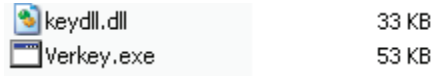

Figure 4: Malware files responsible for keylogging

The keydll.dll and Verkey.exe files are detected in this instance by ESET NOD32 heuristics as probably a variant of Win32/PSW.Lineage. These files are injected into different system processes so as to control the user's actions. ESET SysInspector[15] shows this system snapshot (Figure 5).

From this moment, the keylogger records the keys pressed by the user and stores them in a file within the operating system root directory (Figure 6).

In this instance, the stored information corresponds to the username and password (in hexadecimal encoded format).

Note: To learn about the performance of this malware in detail, it is recommended that you watch the educational video prepared by ESET Latinoamérica on this particular case study[16] (in Spanish).

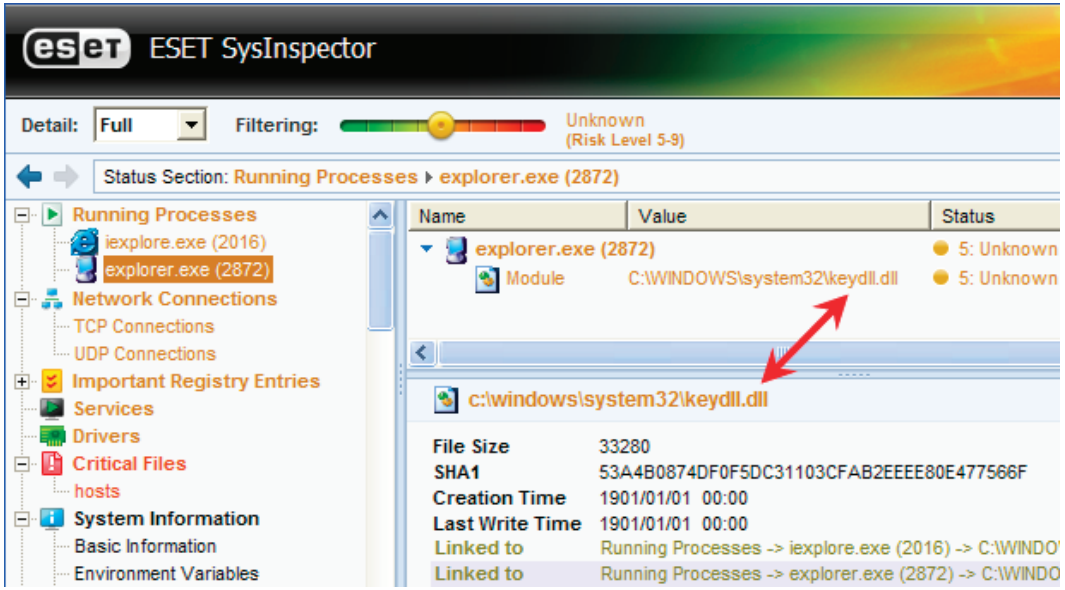

Figure 5: Detection of injected processes by ESET SysInspector

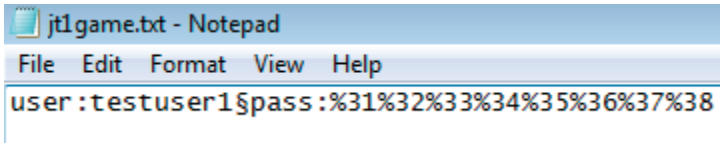

Figure 6: Data recorded by the Trojan

Detection and Protection

The number of current variants of this malware has reached many thousands, and new versions appear every minute, making any attempt to analyze and describe each distinct variation using signatures entirely useless and leaving only two detection options: generic detection and the use of heuristics in order to identify new variants and sub-variants (Figure 7).

Prevention of this kind of malware is similar to that of any other threat since, as discussed, almost any propagation methods can be used.

- Use an antivirus with proactive detection capabilities (generic and heuristic detection).
- Do not simply disable antivirus software when playing games that have a significant impact on system performance. It is far safer to look for a solution that uses few enough resources to enable the user to play this kind of game without having to turn the anti-malware protection off.
- Do not download files from suspicious or untrustworthy sources.
- Use the antivirus to scan any downloaded file before executing it.
- Scan all removable media such as USB drives.
- Verify emails you receive to check they are really from the person who appears to have sent them.

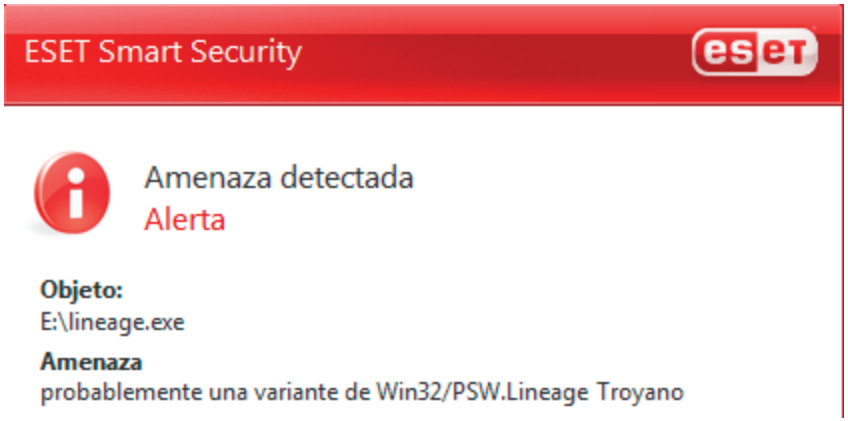

Figure 7: Heuristic detection of the Win32/PSW.Lineage malware

Considering the characteristics of this type of malware and its ability to target online games, apart from the tips mentioned above, gamers should also keep in mind the following recommendations:

- Use reliable game servers.
- Before downloading updates, mods, hacks, cheats and other tools from third parties, verify that they come from an official or reliable server.
- Use strong passwords to avoid their being cracked by brute force attacks, and use two-factor authentication, as offered for WoW among others, where possible. A notable trend is the use of cell phones or cheap authentication token devices for this purpose.
- Do not reveal or discuss confidential data relating to the player or his avatar in chat forums, email lists, etc.
- Visit the official websites for each game to learn about the specific recommendations made there. Read the EULA (End User License Agreement) of each game to be acquainted with the permitted and the illegitimate practices pertaining to each particular game.
- Some games include applications that detect harmful programs specifically developed for those games (Anti-Cheat, GameGuard, PunkBuster, Blizzard Launcher, among others), and it's worth making use of them.
- Take precautions against the massive quantities of emails received (spam) which may generate phishing attacks, or which appear to grant "special privileges" to gamers. These types of email tend to deceive the user with the intention of stealing information or installing harmful programs onto his or her system.

Conclusion

Nowadays, malware creators are people with excellent knowledge of the gaming market, and they target those areas where they know their earnings will be maximized when they distribute their creations.

It is now possible to perform almost any kind of activity (work or leisure) over the Internet. If the system in use is not responsibly used and controlled, implementing the proper security measures, these activities can be severely disrupted.

The high numbers of online gamers and the ability to trade objects between the virtual and the real worlds confer upon these objects a value that is high enough to be highly desirable to cybercriminals. Moreover, the trafficking of sensitive information itself holds significant monetary value in the markets where these characters are traded.

As game platforms are so varied, we can expect that these threats will be developed so that there are versions that can attack any operating system and platform.

In this journey through online games and their threats, it has become clear that these role-playing games represent a million-dollar business, which is why online gamers have so much to lose. As always, it is the responsibility of each user to take the proper security measures.

Postscript

This document highlights the importance of protecting the gamer. However, when malware targeting online games is copied to the system, it does not and cannot check whether the owner of the system is a gamer or not, so it will infect the system notwithstanding.

That is to say, the user's system is likely to be infected irrespective of whether he has ever played, and his system will be used as a channel to infect other users using the aforementioned techniques. This is the reason why the propagation rate shown in Figure 2 is exceptionally high, even though many might think that the number of gamers in Latin America is not the same as in Asia.

Finally, it is important to mention that this type of malware is no fantasy and does not confine itself to gamers. On the contrary, the problem embraces all Internet users, making it crucial to take the necessary precautions.

References

1. Role Games http://en.wikipedia.org/wiki/Role-playing_game
2. Dungeons & Dragons Game http://en.wikipedia.org/wiki/Dungeons_&_Dragons
3. MUD http://en.wikipedia.org/wiki/MUD
4. MMORPGs http://en.wikipedia.org/wiki/MMORPG; http://iml.jou.ufl.edu/projects/Spring05/Hill/mmorpg.html
5. Nicholas Yee. "The Psychology of Massively Multi-User Online Role-Playing Games: Motivations, Emotional Investment, Relationships and Problematic Usage" in Avatars at Work and Play: Collaboration and Interaction in Shared Virtual Environments, ed. R. Schroeder, A-S Axelsson (New York: Springer, 2006) Also online at http://www.nickyee.com/pubs/Yee%20-%20MMORPG%20Psychology%20(2006).pdf
6. MMOG http://en.wikipedia.org/wiki/Massively_multiplayer_online_game); http://archive.gamespy.com/amdmmog/week1/
7. An Analysis of MMOG Subscription Growth http://www.mmogchart.com/analysis-and-conclusions/ http://iml.jou.ufl.edu/projects/Spring05/Hill/mmorpg.html
8. Virtual Web Games Move $900 Million a Year http://www.laflecha.net/canales/videojuegos/los-juegos-virtuales-en-la-red-mueven-900-millones-de-dolares-al-a__o/ (in Spanish)
9. MMOG Active Subscriptions http://www.mmogchart.com/charts/
10. Price of Lindens L$ http://blog.secondlife.com/?s=exchange http://blog.secondlife.com/2007/01/04/l-exchange-data-update/ http://www.rankia.com/blog/familyoffice/2007/06/second-life-inversin-para-real-life.html (in Spanish)
11. Social Engineering http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social (in Spanish)
12. Malware Trends in 2007 and 2008 http://www.eset-la.com/threat-center/1538--tendencias-del-malware-para-2007 (in Spanish) http://www.eset-la.com/threat-center/1709-tendencias-2008 (in Spanish)
13. Propagation Ranking in June http://www.eset-la.com/company/1776-ranking-virus-eset-junio-2008 (in Spanish)
14. Rootkits, Playing Hide and Seek http://www.eset-la.com/threat-center/1755-080429-analisis-tecnico-eset-rootkits (in Spanish); http://www.eset.com/download/whitepapers/Root_of_Evil.pdf

15. ESET SysInspector
    http://www.eset.com/download/sysinspector.php
16. ESET Latinoamérica Educational Videos
    http://www.eset-la.com/threat-center/videos/ (in Spanish)

Further Resources

- ESET Latinoamérica Educational Platform: http://edu.eset-la.com (in Spanish)
- ESET Latinoamérica Lab Blog: http://blogs.eset-la.com/laboratorio (in Spanish)
- ESET Threatblog (TinyURL with preview enabled): http://preview.tinyurl.com/esetblog
- ESET Threatblog notifications on Twitter: http://twitter.com/esetresearch
- ESET White Papers Page: http://www.eset.com/download/whitepapers.php