



:: Free but Fake: Rogue Anti-malware

Cristian Borghello, CISSP



Table of Contents

Introduction	2
Analysis of a Well-known Case	3
Conclusion	7
Further Information	8



Introduction

Most antivirus products are commercial and typically offer, as is the case with ESET® solutions, free trial versions for a 30-day period. This limitation is the perfect excuse for criminals to recommend their “free and magical” antivirus software which guarantees to solve problems that the user does not really have.

These kinds of programs are called “Rogue Anti-Malware” or “Purportedly Protective Programs” and their creators want users to download them in order to infect their systems, while believing that they are protecting themselves. In many cases, a Social Engineering technique is used to trick the user into downloading a malware application in the belief that they will receive a product which is both desirable and free..

Nowadays, there are several scenarios in which these programs may be introduced:

1. A free solution for a specific malicious program is offered on a website. Once the user downloads and installs the product, the user's system is (or appears to be) disinfected but other types of malicious software are installed, such as spyware and adware.
2. The user meets with the same scenario, but in this case is notified of an infection that (may or may not be real) and if the user decides to clean the system, the program demands the registration of the software and the payment of a set fee.
3. One of the previous scenarios is met with but, at the time the product is to be downloaded, the user is required to give his credit card data.
4. Any of the previous scenarios occurs but in addition, the program keeps notifying the user that his computer is infected. The warning is insistent and may be repeated in different ways. Its main goal is to “exhaust” the user and make him believe that a real malware attack is taking place, so that finally he enters his personal data or makes a payment to activate the security solution that will “disinfect” the system.

Unfortunately, people are frequently seduced by the word “free” and overestimate the supposed benefits such products offer: it doesn't occur to them that all security products must undergo strict controls and quality assurance which ultimately guarantee the product's reliability, but which also generate cost overhead that has to be paid by someone, somehow.



For example, it is quite usual for people who browse the Internet regularly, looking for free tools to eliminate the Internet threats they rightly fear, to happen upon fake antivirus or antispyware applications. This search model is specifically targeted by criminals using well-known techniques to subvert Google's search algorithms with the intention of pushing their malware to the top of the search list.

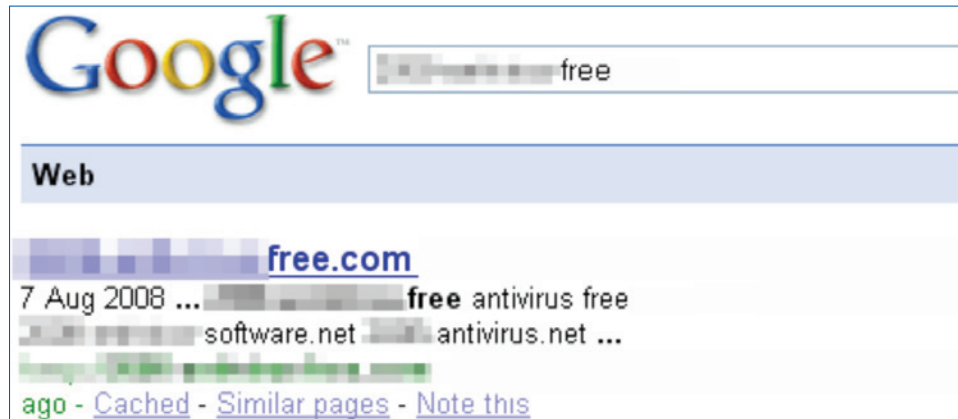


Figure 1 – Results of a Search for Free Tools

When this kind of search is carried out, it is of utmost importance to make sure that these security tools are supported by well-known product tests and certifications, and that they also have a respectable track record. It is one thing to download a product with years of research and development behind it. It's not at all the same thing to download a "free" tool like the one shown in the image above, however miraculous the results it promises. Furthermore, it's common for a fake anti-virus or anti-spyware product to claim the same certifications and endorsements that a good, genuine commercial product is likely to have. It's therefore important to verify such claims independently.

Analysis of a well-known case

In order to illustrate this type of malicious methodology, the case of a rogue product that has proliferated throughout Latin America is analyzed here: that is, Antivirus XP 2008 (also known as Antivirus XP 2009 or MalwareProtector 2008), which offers a fake antivirus solution and, by using the techniques previously described, tries to lure the user into purchasing the registered version of the product.



Although there are several ways in which the user can be enticed onto the website where the program is downloaded, nowadays spamming is most frequently used: when the user clicks on the link embedded into the spam message, the fake antivirus will be downloaded.

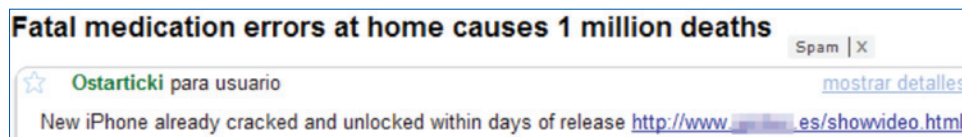


Figure 2 – Spam promoting a website that links to a Rogue Security Program

In some cases, the website downloads and installs the program automatically using the Drive-by-Download technique, so that no action on the part of the victim is required.

Once the product has been downloaded, it installs itself into a directory named using a series of random letters and numbers. The purpose of this random naming is to confuse the user and to hinder the search in case he attempts to remove the fake security solution:

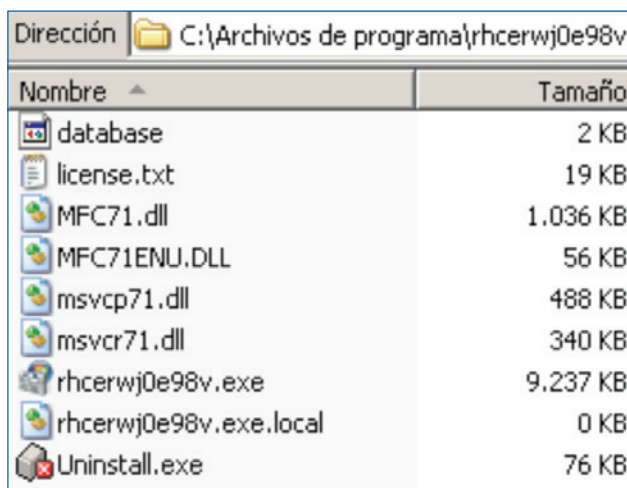


Figure 3 – Product Installation

Each installation will generate a different directory so that the suspicious user will not be able to find the malicious files using a simple string search.

Once running, the program will proceed to perform a fake scan, pretending to search for malware in the user's system, and will always display a notification that the system is infected. The methods used for user notification tend to be invasive and have a disruptive impact on the system performance.

As illustrated in Figure 4, the software notifies the user by changing his desktop wallpaper, making it impossible for the user to change it himself. In addition, a notification continually pops up in the taskbar (approximately once every minute) regarding a supposed system infection, which can be inconvenient and alarming for the user.

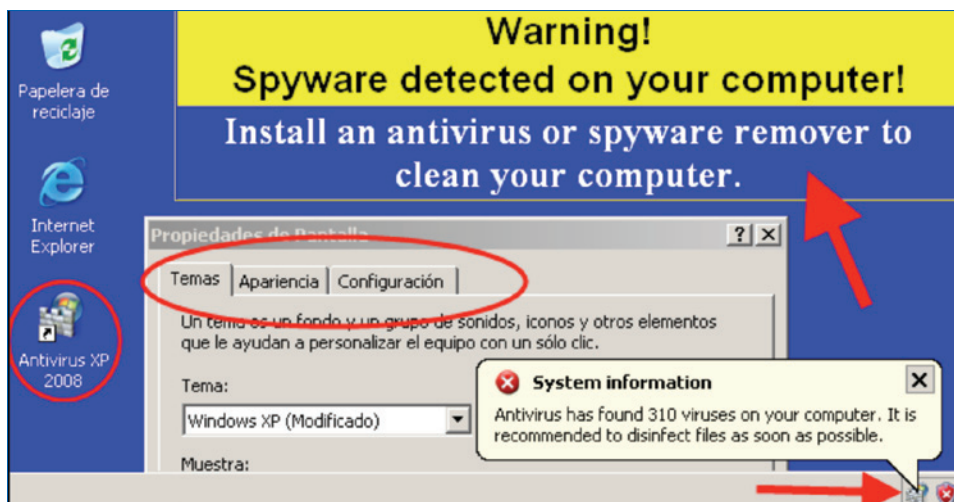


Figure 4 – Program Notification of a Fake Infection

If the user falls for the deception and finally decides to update the program, or tries to disinfect his system, he will need to register the product, which requires him to give his personal and credit card data.



Figure 5 – Payment Request for Product Registration



To make the scam even more complete, the product also notifies the victim about the supposed infection when he attempts to browse the web. In this message, the user is informed he must register the product in order to clean his system:

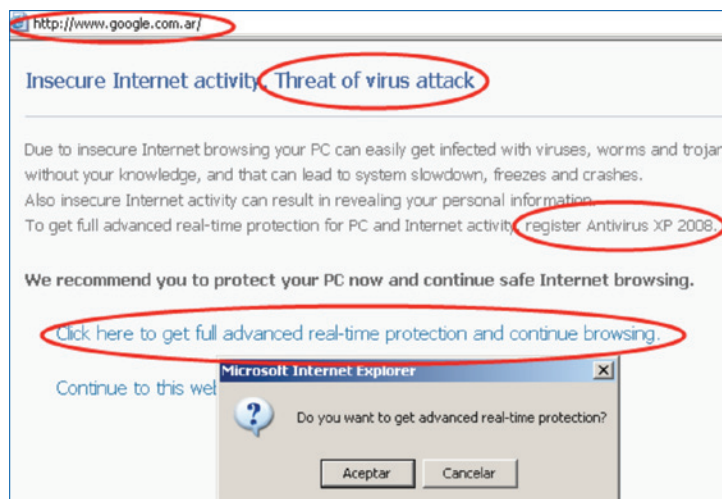


Figure 6 – Webpage Accessed when Trying to Surf the Web

This type of program significantly modifies the system on which it is installed, and its main objective is to persuade the user to register the product by any possible means. In addition, such programs generally install other malware such as adware and spyware in order to control and monitor the user's actions, and to send stolen information to the malware creator or distributor.

If the user tries to uninstall the program will pop up when the system is restarted with yet another notification of a supposed threat and the removal will not take place:

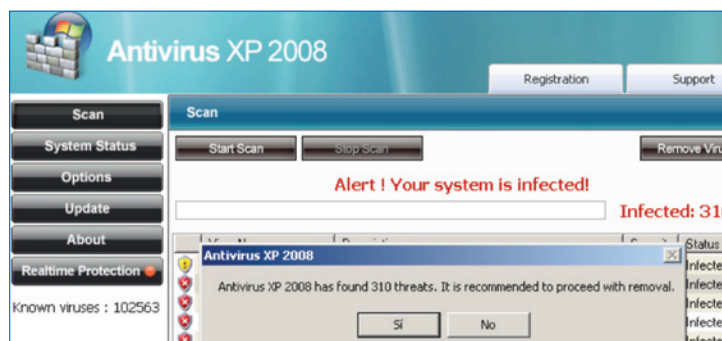


Figure 7 – Fake Detection of Malware



In the case described, ESET NOD32 detects the fake security program as Win32/TrojanDownloader.FakeAlert, and the different websites associated with the program are blocked when the user tries to access them. This last option prevents the user from accessing the website and accidentally installing the harmful program.

Conclusion

Rogue or fake security tools have quickly become a preferred means by which malware creators try to deceive the user, under the pretext of offering a “free product to clean your system,” because many users prefer to try these tools rather than downloading well-known commercial product versions, or even free or online scanners. It is thus of the utmost importance that the user is properly informed and aware. When it comes to choosing an effective security solution, the purchaser must be sure that it provides genuine real-time protection against malware and has proactive abilities enabling the heuristic detection of the fake programs and their variants that we see appearing day after day.

In order to illustrate performance of this rogue program, ESET Latinoamérica developed an educational video which demonstrates its mode of operation, as well as the actions the user should follow to avoid being infected by it.



Further information

Social Engineering. <http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social> (in Spanish)

ESET NOD32 Antivirus Free Trial. <http://www.eset-la.com/download> (in Spanish)

Drive-by-Download. <http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web> (in Spanish)

ESET Latinoamérica Educational Platform. <http://edu.eset-la.com> (in Spanish)

ESET Latinoamérica Lab Blog. <http://blogs.eset-la.com/laboratorio> (in Spanish)



Corporate Headquarters

ESET, spol. s r.o.
Aupark Tower
16th Floor
Einsteinova 24
851 01 Bratislava
Slovak Republic
Tel. +421 (2) 59305311
www.eset.sk

Americas & Global Distribution

ESET, LLC.
610 West Ash Street
Suite 1900
San Diego, CA 92101
U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 876-5845
www.eset.com



© 2009 ESET, LLC. All rights reserved. ESET, the ESET Logo, ESET SMART SECURITY, ESET.COM, ESET.EU, NOD32, VIRUS RADAR, THREATSENSE, THREAT RADAR, and THREATSENSE.NET are trademarks, service marks and/or registered trademarks of ESET, LLC and/or ESET, spol. s r.o. in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.



MAXIMUMPC