PandaLabs Bulletins:

Profitability of rogue antimalware

wwwpandasecurity.com/homeusers/security_info | www.pandalabs.com

Index

Index....2
1.- Introduction....3
2.- Key Features....3
3.- Common infection vectors....5
4.- Figures....7
5.- In-depth analysis: MalwareProtector2008....9
6.- Consejos....13

1.- Introduction

The last few months have witnessed the appearance of many false anti-malware programs, also known as rogue anti-malware. Even though these types of programs are not at all new, they have proliferated lately due to the significant economic return they bring to cyber-crooks.

Also, numerous spam messages have been found lately carrying these annoying programs. These messages use social engineering techniques to trick users by exploiting the latest news, controversial issues or celebrity videos.

Rogue anti-malware continuously displays alarming messages to exhaust the victim's patience and get them to register the product after paying the corresponding fee.

Cyber-crooks take advantage of users' main concern about the Internet: theft of passwords, banking data or personal information. Therefore, there is no better way for criminals to achieve their objectives than to display messages that indicate the user's data is at risk as their computer has been infected by a password-stealing Trojan.

It is quite simple for cyber-crooks to design these programs, as they are similar to one another and it is sufficient to make a small change to their configuration to produce a new program from which they can continue to profit.

Therefore it is very important for users to learn to recognize these phony programs and avoid falling into the trap. Although many of these programs show interfaces and features very similar to those of real antiviruses, they are actually fake.

This article describes these programs, the usual infection vectors and how to respond to this threat. You can also see a series of graphs that show the significant growth of this type of malware that directly targets users' money.

2.- Key Features

Generally speaking, rogue anti-malware applications report a false infection on the computer and offer a solution to remove it. To do this, the user must register and pay a certain amount of money.

Although these tools are initially offered for 'free', users must pay to register. They offer free antivirus scans which are actually a fraud as they warn of non-existent threats or because those threats are actually installed by the tools themselves. They also display continuous, annoying messages claiming that the computer is infected.

After analyzing several examples of this type of malware, we can conclude they all behave in a similar way, not only with regard to the messages displayed but also to the changes they make to the system.

These are these programs' common traits:

- They display fake warning pop-ups, messages on the taskbar and change the screensaver.
- They look and pretend to work like a real antivirus.
- They complete scanning of the entire system very quickly.
- The infections they report refer to non-inexistent files on the affected system or files downloaded by the applications themselves.
- All of them ask users to pay a certain fee to register the product and disinfect the system.

As for the effects they have on computers, they make changes to the Windows Registry to trick the user into believing they are truly infected.

These changes have the following consequences:

- Modify the desktop theme.
- Establish a screensaver designed by the adware.
- Hide the Desktop and the Screen Saver tabs on the Display Properties screen. This way, users cannot modify the desktop theme or the screensaver.

Usually, the desktop theme and the screensaver established by the adware contain messages that warn the user that the computer is infected.

The purpose of these techniques is to exhaust the user's patience so that they finally register the product and pay the corresponding fee.

In the end, what seemed free is actually rather costly.

Many of these programs advertise themselves by claiming to detect more than other programs. The question is not that they detect more than the others, but that they detect non-inexistent threats or even threats the tools themselves have introduced on the computer.

They exploit the myth that a security program that detects something others can't is a better product. That is, the more a security solution detects, the better. However, this couldn't be further from the truth; in this particular case, these solutions detect more simply because they detect false threats.

The purpose of these programs is purely economic: to get as many users as possible to buy the corresponding license.

3.- Common infection vectors

One of the possible infection vectors is visits to web pages of dubious content, such as web pages with adult content. To do this, they use a technique known as Drive by download to download files. Through this technique, files can be automatically downloaded to computers without users' knowing by exploiting system flaws. They also use advertising banners that offer free downloads.

Another means of distribution is web pages offering pirate software. They use social engineering techniques to trick users as they rename files with attractive names to make users believe they are downloading cracks, serial numbers, etc.

However, cyber–crooks are aware of the profitability of this business and do everything they can to distribute these programs. Thus, not only can these programs be downloaded from pages of dubious reputation, but also from legitimate web pages. We published an article dealing with infections from legitimate pages back in July (Social Networks in the Spotlight).

Now, all is left to do is get users to visit these web pages; but, how? Through spam.

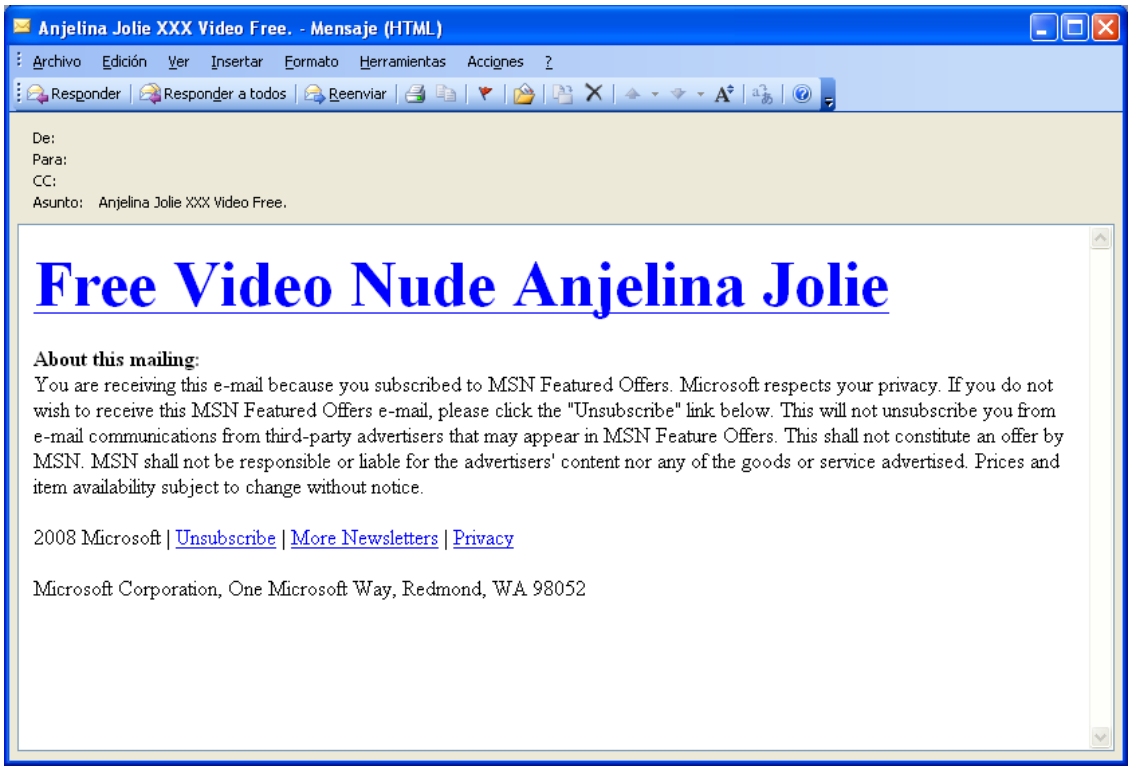
Some Trojan families like *Exchanger* and *Spammer* have been designed to send out spam messages massively.

This type of message includes the adware or contains a link to a web page where users inadvertently download the malicious file through the drive by download method above.

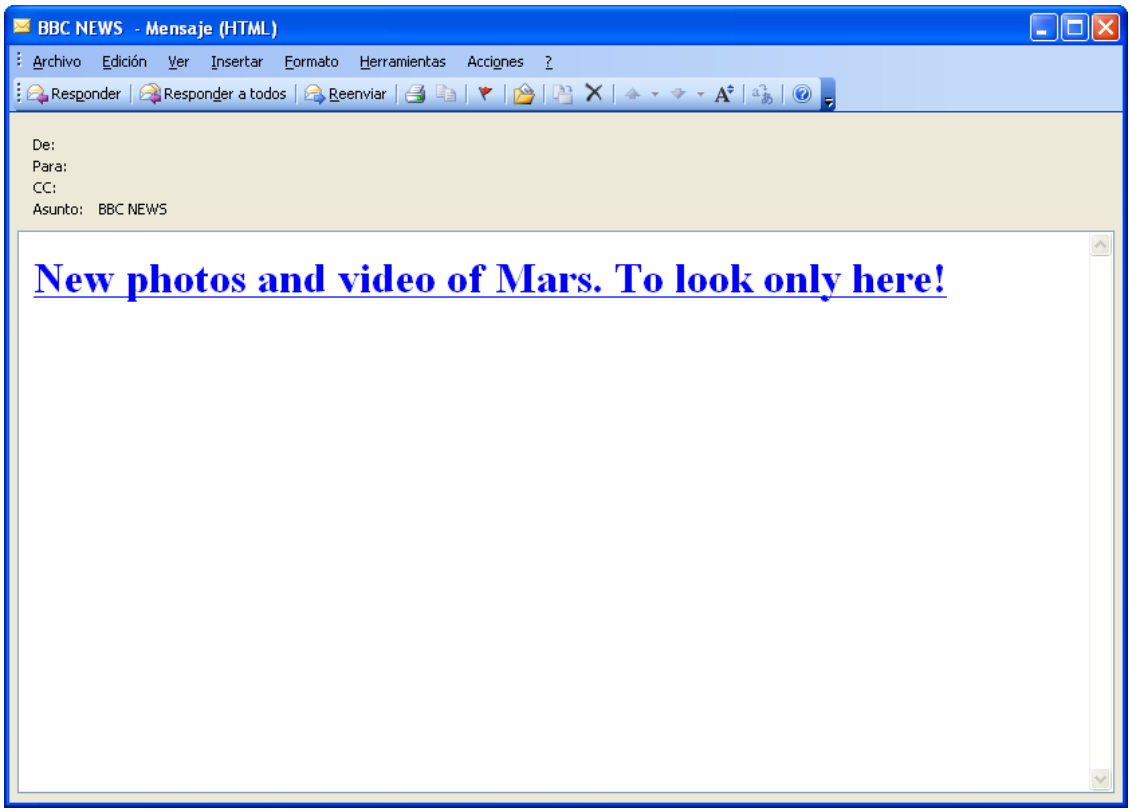
Spam messages are used to distribute all types of malware. However, in most cases they were used to spread Trojans, password-stealer Trojans more specifically. However, over the last few months we have detected a change in the type of malware distributed through spam. Now, it is these false anti-malware programs that are top of the list.

The main topics used to trick users continue to be the same: latest news and celebrity videos.

The following images show email messages used to distribute these programs:



Email referring to a celebrity video



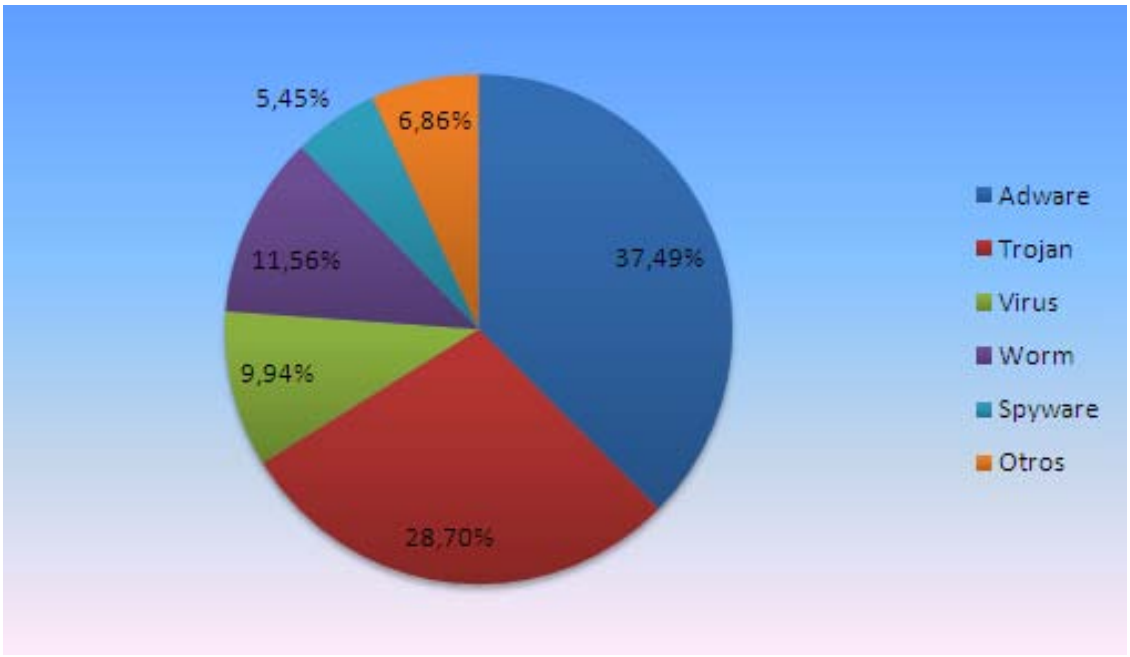
Email referring to a fake BBC news story

Finally, another common infection vector for these programs is malware. Some malware familes download this type of program. This is the case with *Nuwar*, or even some adware families that also download other adware strains, such as *Adware/Bravesentry*.

4.- Figures

The third quarterly report already mentioned the significant increase in adware distribution, mainly due to these rogue anti-malware programs.

The graph below illustrates how the adware category has risen to 37.49% this quarter (July –September), whereas last quarter, the percentage was 22.03%.

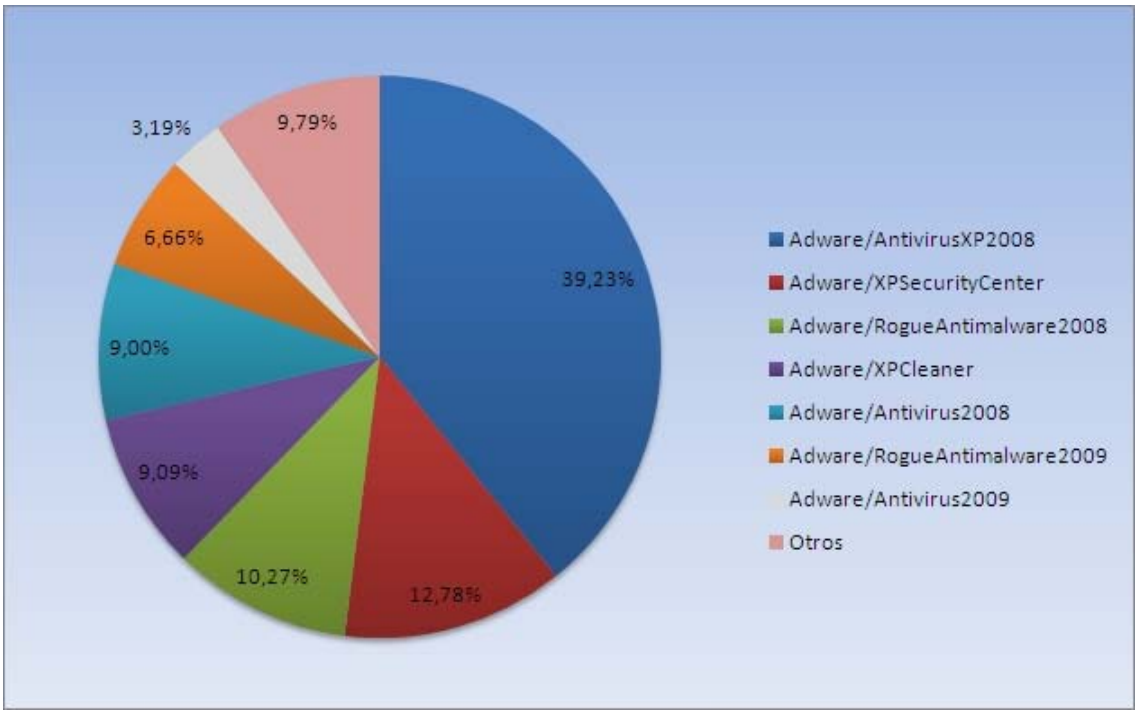


Malware distribution by category

According to data gathered from May to August, rogue anti-spyware started growing exponentially in May and reached its peak in July. From that month, the numbers of anti-spyware started to decline, even though the current levels are still higher than in May.

Evolution of anti-spyware detection (May - August)

As for the most active adware, the graph below shows that the most active specimen over the last few months was AntivirusXP2008 (39.23%).

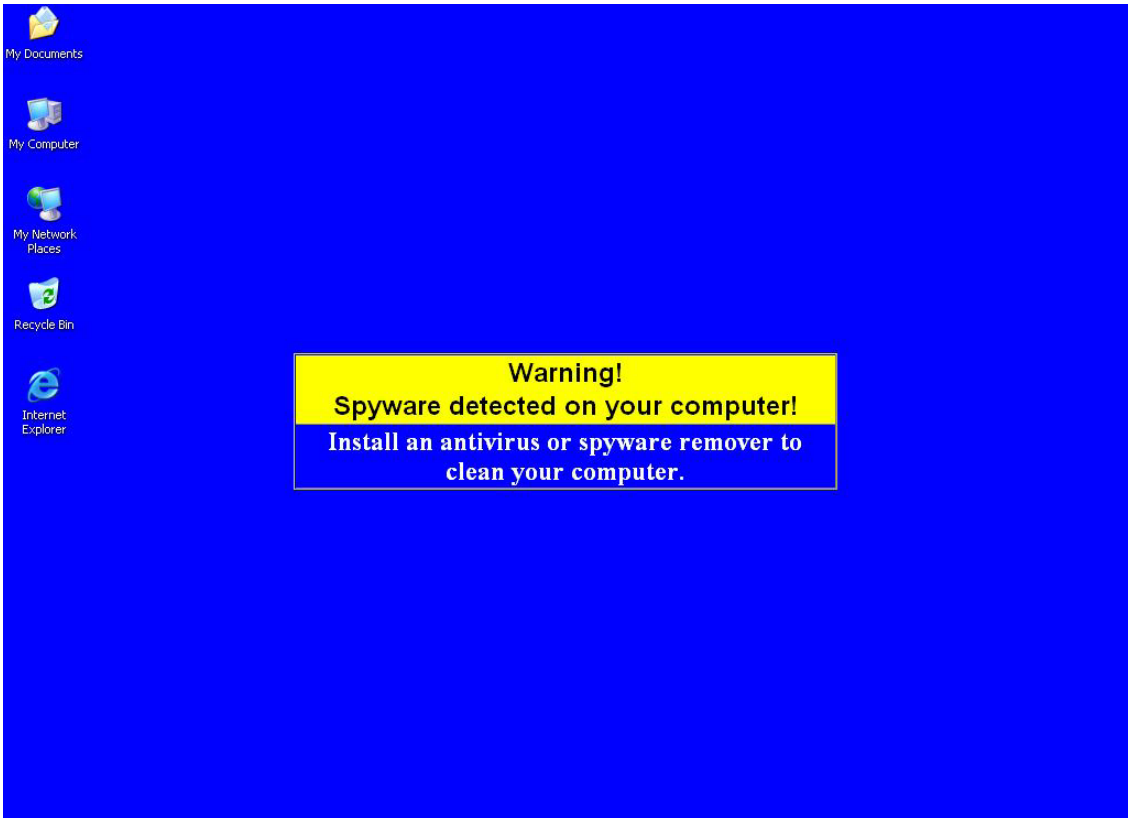


Distribution of most active adware

As for the malware strains we have analyzed over these months, one really caught our attention due to the 'scary' screen saver it uses: a group of cockroaches eating up the desktop.

5.- In-depth analysis: MalwareProtector2008

Once run, the adware replaces the desktop theme with the following:



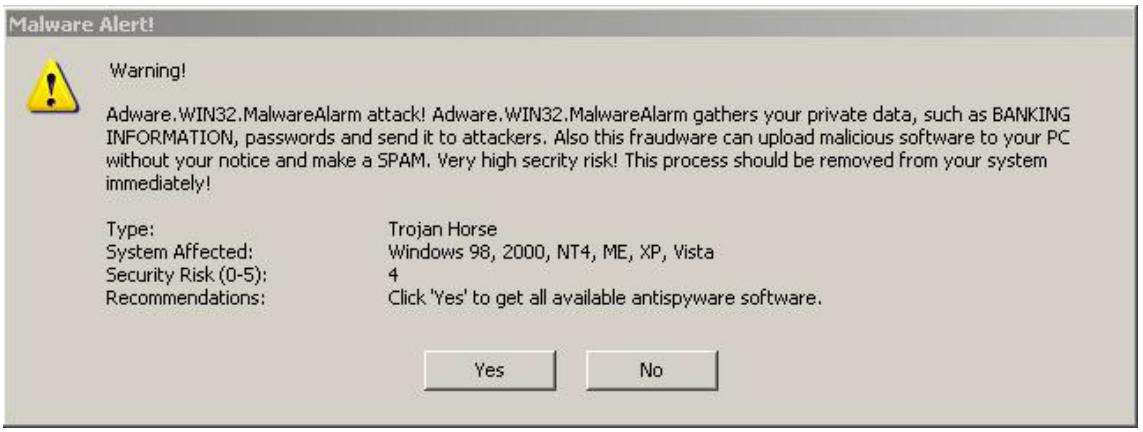
Desktop theme established by MalwareProtector2008

The message reads as follows:

Warning! Spyware detected on your computer! Install an antivirus or spyware remover to clean your computer.

This way, it tricks the user into believing their computer is infected.

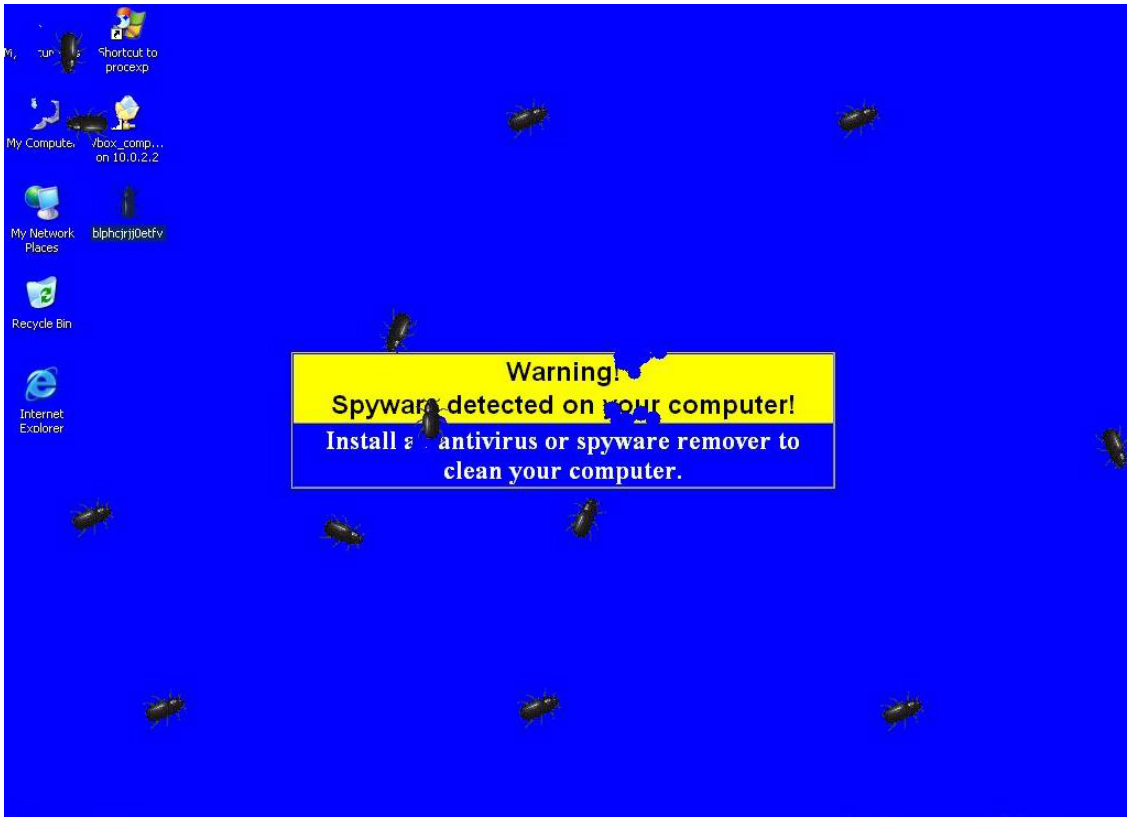
Then, it shows a message warning users that their computer contains adware designed to steal passwords or banking data.



Warning message displayed by MalwareProtector2008

Also, users are prompted to remove the threat from the system as soon as possible. To do so, they are offered an anti-spyware program to disinfect the computer.

If the user selects 'No' a screensaver runs from time to time showing a group of cockroaches eating up the desktop.

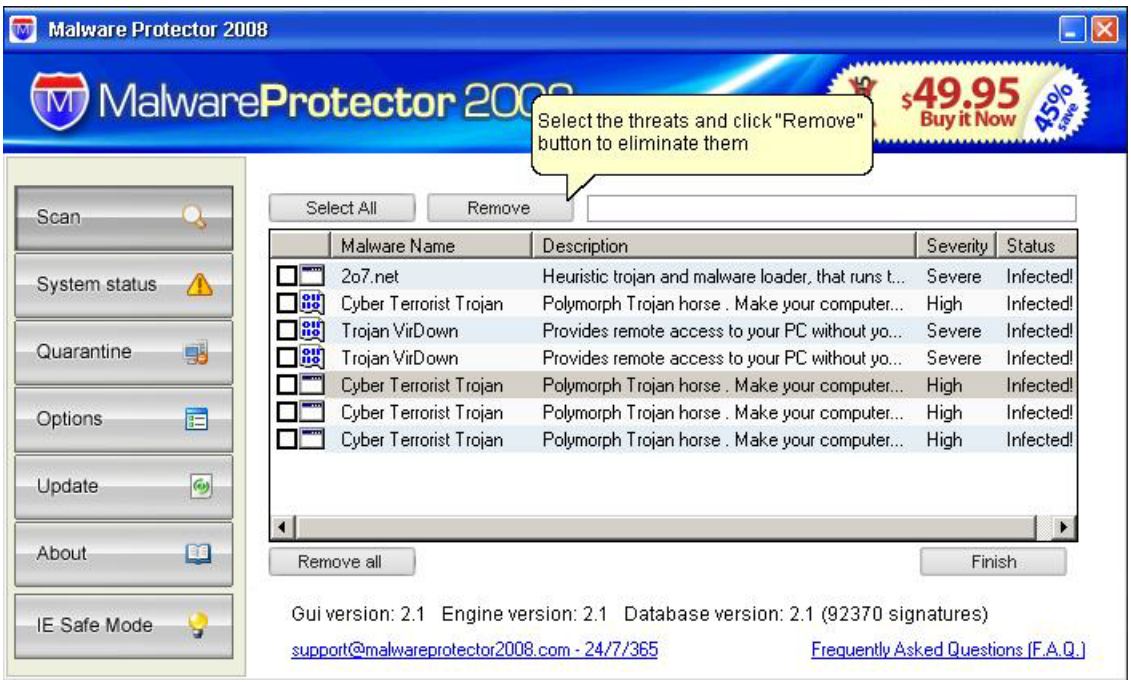


Screen saver displayed by MalwareProtector2008

This is another technique used to get the affected user to accept the message and download a false antivirus program.

If the user accepts the message, the false anti-malware program will start to download. Once downloaded, the program starts scanning the system for possible malware.

However, the scan result is a complete fraud and shows a series of non-existent threats that have supposedly infected the computer.

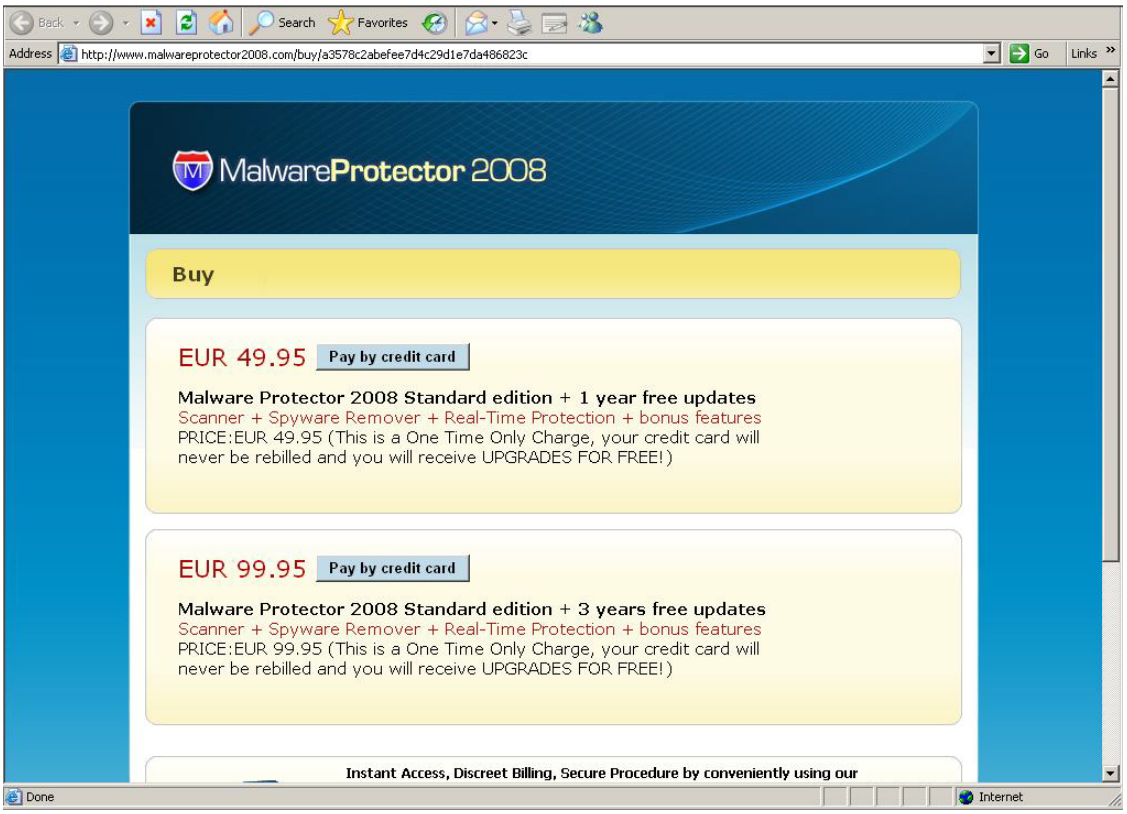


MalwareProtector2008 scan result

If the user selects the option to remove malware, a screen is displayed informing that the computer is infected with adware and spyware. They are also encouraged to register to remove these threats and stay protected:

MalwareProtector2008 interface

To register, the user has to pay the price indicated on the website they are taken to after clicking the button to get the full version.



MalwareProtector2008 web page

However, even though you have registered and paid the corresponding fee, the computer will still be unprotected and vulnerable to all types of threats.

This adware's characteristics are very similar to those of other rogue anti-malware: the messages displayed, the application interface, the way it works... We hope this in-depth analysis will allow users to identify this type of program.

6.- Practical Tips

Spam is the usual means of propagation for this type of program. Be extremely careful with any email message you receive with eye-catching news stories or subjects. These emails typically invite users to click a link to watch a video or images of some false news. Don't click on links included in these messages, as you might be downloading one of these false anti-malware programs into your computer.

Be wary of programs you don't remember installing and which start showing false infection warnings or pop-ups that encourage you to buy some kind of antivirus software. Most probably, one of these malicious programs has installed itself on your computer.

Always keep programs up-to-date. An out-of-date program can be a vulnerable program. Keep all programs up-to-date as many malicious codes exploit vulnerabilities on computers to infect them.

Scan your computer regularly with a reliable antivirus, so that if any of these codes is hiding on the computer, it can be detected and removed.