FAKE BUT FREE AND WORTH EVERY CENT

Robert Lipovský, Daniel Novomeský, Juraj Malcho
ESET, Slovakia

Email {lipovsky, novomesky, malcho}@eset.sk

ABSTRACT

In 'Is there a lawyer in the lab?' [1], Juraj Malcho discussed the thin boundary between legitimate and malicious applications, and presented the difficulties AV companies have encountered dealing with greyware or potentially unwanted applications (PUAs). The severity (and sensitivity) of the situation has been borne out by numerous legal cases.

Two years later, the state of affairs is an even greater pain in the butt. The swindlers have noticeably improved their scam plots and social engineering, and the challenge for the anti-malware industry is as great as ever. And the technical aspects of the adware or other potentially unwanted applications are not what we have in mind. We're talking about the effort that the authors invest into trying to convince people that their software is legitimate. They're trying to persuade not only the potential victim – which is basically what every trojan does – but also those of us who are responsible for malware detection! In effect, deciding whether or not to detect a PUA is often peculiarly difficult for malware researchers.

In this paper we discuss a range of issues from various blatant online scams to applications which are much less useful than they may seem at first glance. The common factor here is selling a pig in a poke to the everyday, trusting computer user. The shift from rogue security software towards various PC tuning applications is just one example of an obvious trend.

Indeed, the surface characteristics of such software differentiate it from typical trojans and other malware. But aren't the goals of the perpetrators in both cases, fundamentally, the same? And what is the role of an AV solution today? Just preventing PCs from being infected by viruses, worms and trojans? Don't we also have a responsibility to keep the Internet clean and free of junk? This is about boxing the ears of those software vendors who only care about raking in the profits, and offer no value in return.

INTRODUCTION

Adware and potentially unwanted applications (PUA) have irritated computer users for quite a few years now. During this time, the authors of such dubious software have improved their strategies a great deal. The tactics they utilize fool computer users and at the same time often suffice to keep anti-virus 'off their back'. Adware, for example, is no longer as conspicuous as it used to be, and advertisements are often slipped into less common places (such as installers) rather than using blatant pop-ups. Rogue anti-viruses are still omnipresent, but their authors have also put a lot of effort into avoiding detection. Unlike regular trojans, which attempt to defeat anti-virus engines technologically, greyware relies mostly on good marketing (and often lawyers).

SELLING A PIG IN A POKE… FOR FREE

The current hot topic is registry cleaners. When analysing the fundamentals of this type of software, the evolutionary differences from rogue AVs become apparent. The business model of these two greyware categories is very similar. Both of them can be considered scareware – they warn the victim that his/her computer is in a bad condition (suffering 'infections' and 'malware' in the case of rogue AVs, 'problems' and 'errors' with registry cleaners) and then try to get the user to pay for the solution. There are, however, several differences that make dealing with registry cleaners more problematic.

This 'ambitious' greyware no longer relies on apparently malicious trojan-downloaders for spreading. The affiliate distribution model is still used, but to a much lesser extent. Instead, registry cleaners usually handle distribution on their own and act as even more wanna-be-legitimate software than rogue AVs. Let's take a closer look at the methods these guys use.

Technique 1 – 'free'

Marketing is the key to a greyware vendor's success, and 'free' is his buzzword of choice. The victim is lured into installing a free application but eventually is asked for his credit card information. One claims 'it charges nothing to allow you to enjoy the no error system…' But contrary to what is advertised, the tool frightens the user into paying for this 'free' functionality. Another example of a typical registry cleaner characteristic is pretending to fix 'problems' found on your computer. Scareware tactics are used to 'show' many make-believe errors on the victim's computer and, obviously, only the 'scan' was free: the user has to pay to get the 'problems' fixed. As shown in Figure 1, the GUI of this application offers 'Buy Now' as the only option.

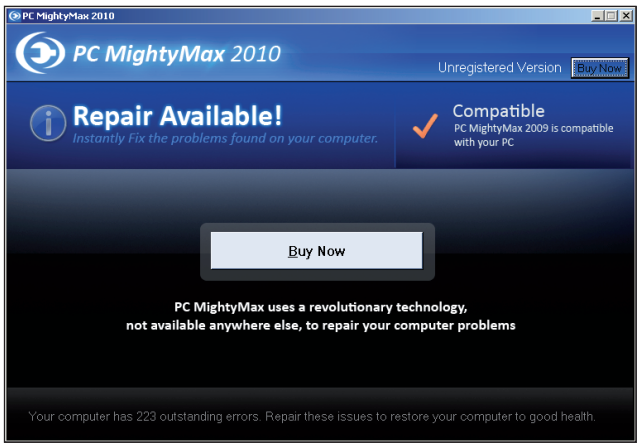

Figure 1: Window displayed by a 'free' application.

Technique 2 – nuisance

The application in our example is also one of the most importunate and annoying cases of scareware and the tactics it uses bear a great resemblance to typical rogue AVs. Closing the window (Figure 1) doesn't help and a pop-up is displayed that reminds you of the unhealthy state of your computer, and again the only button available is the option of buying the software. If you somehow manage to close the pop-up, the application continues to run in the system tray (Figure 2) and there isn't a regular option to shut it down.

Figure 2: Registry cleaner in system tray icon.

This software is pure nuisance and it's pretty straightforward for the AV vendor to decide that it is indeed malicious, and should therefore be detected. Thus, it came as quite a surprise when we checked this application against *VirusTotal*, to find that *ESET* was the only company to detect it.

Technique 3 – rebranding

Another technique that the authors of registry cleaners have borrowed from rogue AVs is rebranding. We come across a great number of applications which have a slightly (sometimes more, sometimes less) modified graphical user interface and a different name, but which are essentially the same thing, with the same code underneath the GUI. An example, where the authors put a moderate amount of effort into changing the appearance of two PC 'tuning' products, is shown in Figure 3. Obviously, these two applications come from a single company.

The reason that rebranding is such a heavily used technique is analogous to the reasoning behind the mass generation of different variants of trojans. The difference, however, is that this technique aims to fool the unsuspecting ordinary computer user, rather than to conceal itself from security software. When this kind of rogue application is publicized and users are warned to stay away from it, the perpetrators react by simply changing the appearance of the software, giving it a different name and starting off again with a clean slate.

Figure 3: GUI rebranding.

Technique 4 – false testimonials

One way of finding out whether a questionable application is legitimate or not is by 'Googling' it. Anti-virus companies often write about rogue applications in their blogs, discussion forums and threat encyclopedias, and even the occasional warning about some registry cleaner shows up. The greyware authors are very well aware that reputation is the key component in the success of their creations. With this in mind, they often include false user testimonials on their websites that make claims for how amazing their software is. What's really interesting, though, is that exactly the same wording can be found in customer reviews for different software. Just look at the testimonials by a certain 'Diane Parker' for two supposedly different products in Figures 4 and 5. The registry cleaner's authors also attempt to add credibility to the reference by making a cursory but positive reference to legitimate security programs.

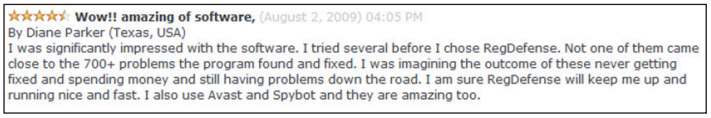

Figure 4: 'Customer' review of a registry cleaner.

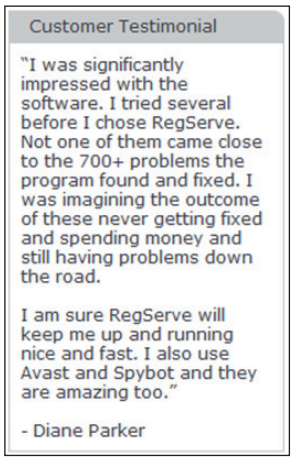

Figure 5: Same 'customer' review for a different product.

These texts are obviously generated using a template, where only the name of the software is changed. Essentially, this is just another case of rebranding, whether it concerns the GUI, false customer reviews or websites, as illustrated by the example in Figure 6.

Customer testimonials are, indeed, one of the tricks that can fool victims into installing this junk on their computers. After all, who could refuse an application such as the following?

> '*It is no exaggeration to say that my computer and Internet surfing now run about 10 times faster since I used your software. I can't thank you enough for your great program!*'

But more on the topic of the 'usefulness' of registry optimizers later…

Figure 6: Website rebranding.

Technique 5 – false certificates

If testimonials from satisfied customers isn't enough to convince you to install these registry optimizers, the perpetrators go even further by faking approvals and even recommendations by trustworthy sources. The website of WorkStation Optimizer, for example, displays a number of certificates and even mentions that the software has 'passed deep testing' by three anti-viruses: *ESET NOD32*, *Kaspersky Antivirus* and *Dr.Web Antivirus*. This statement is obviously a blatant lie in the eyes of a malware researcher, however an everyday, unsuspecting user has no way of knowing this and may end up installing the rogue application.

Many of these scareware tools present themselves as 'award-winning' and show off their 'success' by posting an abundance of different logos on their websites. Sometimes the logos from various download servers are valid, because, in reality, they are not related to the quality of the software. They simply indicate that it was not detected during an anti-virus scan when it was added to the particular download server. And as with other malware that guarantees that it is not detected at the time of release, it isn't too difficult for the authors of the greyware to obtain such awards. Obviously, when the truth about the software comes to light, the download servers (usually) revoke the certification and remove the application from their site. Of course, the authors of the software are able and more than happy to keep on using the 'awards'. One of the most commonly abused awards is the '100% Clean, No Spyware, No Adware, No Viruses' logo by *Softpedia*. The website of the following registry cleaner shows the *Softpedia* logo and a number of others (Figure 7).

Figure 7: An 'award-winning' registry cleaner.

Other certificates, which often appear on the websites of registry optimizers, are the *Microsoft Gold Certified Partner* and *McAfee Secure* logos. The effect of apparent trustworthiness is the same as with the other logos, but what's interesting about these (and what makes the decision whether to detect the software or not even more difficult) is that they might have been acquired in a legitimate manner. But even if

Figure 8: Website of Windows PC Doc featuring the McAfee Secure logo.

the website and its contents aren't considered to be outright malicious, the certificate in itself guarantees neither fair practices on the part of the vendor, nor the quality of the software. The *McAfee Secure* logo can be seen on the website of Windows PC Doc (Figure 8) and the websites in Figure 6.

Technique 6 – communication with us

Windows PC Doc brings us to the huge number of emails exchanged between the greyware vendors and *ESET*'s Malware Research Lab. The fact is that these people take their business very seriously and the number of registry cleaners that we have detected without receiving any complaints from the greyware vendor as a result is very low. The contents of the emails we receive from these companies are all the same. They write to inform us that we have a false positive in detecting their application and that this hurts their reputation, and they demand that we remove the detection.

Both of the examples mentioned above (Windows PC Doc and Workstation Optimizer) are rebranded clones of software called RegGenie. *ESET* detects these applications as Win32/Adware.RegGenie. Below is an extract from a complaint email from them:

> Dear Sir/ Madam
>
> I have written to your samples team but have yet to hear back from them about a false positive. May I ask how long it takes to hear back as this is a serious issue and been over a week since we may the submission about our product
>
> … when ran the executable files that is installed in program files after running the installer, its flagged as Win32/Adware.RegGenie
>
> **Please can let us know what this is as we have nothing to do with RegGenie**
>
> We also participate in white listing partnership programs with McAfee and more recently became a Kaspersky Lab white list partner. We do continue to work with any vendor and genuinely interested in addressing any concerns. More recently we addressed concerns of Malware Bytes Corporation after clarifying the issue with them. We have applied for whitelisting with AVG and Norton/

Figure 9: Extract from an email from Windows PC Doc.

There are two very interesting points in this email. Firstly, they stress that they have 'nothing to do with RegGenie'. Figure 10 shows part of the disassembly of Windows PC Doc, containing the 'RegGenie2008' registry key. Do these people not know what they have in their code? Or do they think we are naïve enough to believe their claims?

The other fascinating approach found in this email, as well as in many others, is the persuasion factor. All the previously mentioned techniques (rebranding, testimonials, etc.) are aimed at the user – the potential victim of their scams. This time, they are trying to convince us, malware researchers, that their software is legitimate by saying that the application is whitelisted by other anti-virus companies.

Let's meet Angela now… Another detection that we've added was Win32/Adware.RealRegistryCleaner. Shortly after, we received the following email:

> Hello,
>
> My name is Angela from Advanced Registry Clear.
>
> Our product Advanced Registry Clear is a popular software which helps users fix registry errors.
>
> Here is our product website: http://www.advancedregistryclear.com/
>
> ESET NOD32 Antivirus has detected Threat: a variant of Win32/Adware.RealRegistryCleaner application in it.
>
> Please see the attached pictures.
>
> The version of ESET NOD32 Antivirus is 4.2.58.3 and Virus definition version: 5802 (20110120).
>
> There must be some mistakes. Our product is clean.
>
> Please check it ASAP! Many thanks!
>
> Angela

Figure 11: Email from 'Angela'.

Due to a generic signature, we were able to detect all the clones of this rogue software and were rewarded by emails with the same text in each case, with only the application name and website changed:

> My name is Angela from Genuine Registry Doctor.
>
> My name is Angela from Instant Registry Cleaner.
>
> My name is Angela from Registry Cleaner Free.
>
> My name is Angela from Registry Cleaner Flash.
>
> My name is Angela from Registry Optimizer Free.
>
> My name is Angela from System Boost Elite.
>
> My name is Angela from System Speed Booster.
>
> My name is Angela from System Optimize Expert.
>
> My name is Angela from Registry Clean Easy.

Obviously, Angela must be some kind of superwoman, since she's able to work for 10 companies at the same time, right? ;-)

```
CODE:006D668B    mov     eax, [ebx+54h]
CODE:006D668E    mov     ecx, [eax]
CODE:006D6690    call    dword ptr [ecx+38h]
CODE:006D6693    mov     edx, offset aHkey_current_7 ; "HKEY_CURRENT_USER\\Software\\Microsoft"
CODE:006D6698    mov     eax, [ebx+54h]
CODE:006D669B    mov     ecx, [eax]
CODE:006D669D    call    dword ptr [ecx+38h]
CODE:006D66A0    mov     edx, offset aHkey_current_8 ; "HKEY_CURRENT_USER\\Software\\Policies"
CODE:006D66A5    mov     eax, [ebx+54h]
CODE:006D66A8    mov     ecx, [eax]
CODE:006D66AA    call    dword ptr [ecx+38h]
CODE:006D66AD    mov     edx, offset aHkey_current_9 ; "HKEY_CURRENT_USER\\Software\\RegGenie2008"...
CODE:006D66B2    mov     eax, [ebx+54h]
CODE:006D66B5    mov     ecx, [eax]
CODE:006D66B7    call    dword ptr [ecx+38h]
CODE:006D66BA    mov     eax, [ebx+50h]
CODE:006D66BD    mov     dl, byte_6D6864
```

Figure 10: RegGenie2008 string in Windows PC Doc code.

But malware researchers aren't the only people approached with complaints from the greyware authors. The registry cleaner vendors are relentless and go through every possible channel to achieve their goal. Sometimes the conflict is escalated to our legal department, sometimes their representatives even approach our people personally!

Technique 7 – parasitizing legitimate brands

The names that the developers of rogue anti-viruses and registry cleaners give their creations (especially absurd ones along the lines of 'Super XP Police Antivirus 2010') are often a source of amusement. Sometimes it is hard to believe that users actually install this junk and are not put off from the start by the very name.

But sometimes we observe much cleverer names. There are rogue AV applications that parasitize the reputation and brand of legitimate anti-virus products, even our own. We are certainly not aware that we've released a registry cleaner! An example of this kind of parasite is E-Set Antivirus (Figure 12). What's interesting about this one is that they use a modification of our name, but steal 'their' logo from *AVG Technologies*.

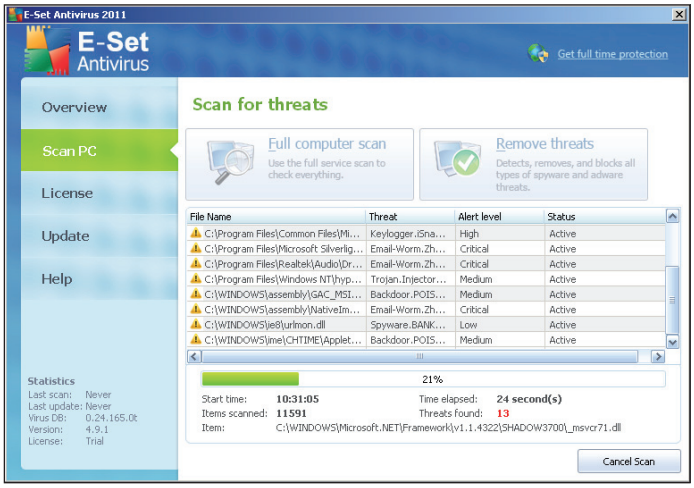

Figure 12: Rogue E-Set Antivirus.

More about these and other cases has been written on *ESET*'s *ThreatBlog* [2, 3] and support pages [4].

10X FASTER!

With the abovementioned techniques we have outlined the unfair business practices of the registry cleaner vendors. But what about the functionality of the software itself? The fact is that with registry cleaners, it is much more difficult to explain that they're bogus than it is with rogue AV.

The main idea behind them (if we ignore all the marketing and the scareware tactics that they use) is that the decrease of performance over time of some *Microsoft Windows* installations is caused by so-called registry junk and redundant files on the hard drive. It is indeed true that many uninstallers don't remove all traces of the uninstalled application and often leave some registry keys and files behind. There are a number of reasons for this, ranging from simple poor quality of the uninstaller, to valid reasons such as shared DLLs. But what is important is that this 'junk' does not influence the performance of the system and its removal certainly has no positive effect. But don't take our word for it. *Microsoft Windows* expert Mark Russinovich states that 'even if the registry was massively bloated there would be little impact on the performance of anything other than exhaustive searches' [5]. He also addresses the issue of registry cleaners and adds that he hasn't and 'never will implement a registry cleaner since it's of little practical use … and developing one that's both safe and effective requires a huge amount of application-specific knowledge'.

And that brings us to the fact that registry cleaners not only fail to deliver the amazing performance boost of the system (contrary to the claims of the vendors), but they may have the opposite effect and make the system less stable when they remove something that they shouldn't have. Cleaning the registry should not be a regular maintenance chore and if done, should definitely not be automated, for reasons summarized by Bill Castner and others in a thread at [6].

For another case in point, let's go back to the registry cleaners that we've analysed. Many of them promise to fix the computer and return it to a state just like a new *Windows* installation. What's interesting, though, is that when these tools are run on a fresh installation of *Windows*, some of them find hundreds, some even thousands of errors on the computer. As shown in Figure 13, the majority of so-called 'errors' are just empty registry keys. Reporting them as errors with 'High Damage level' is a misleading exaggeration, to say the least. They are only used to increase the error count and their removal is not able to provide the promised performance boost. After all – with so many problems on fresh *Windows* installations, are the people at *Microsoft* doing something wrong?

Figure 13: 'High damage level' due to empty registry keys.

A PARASITE OR ADDED VALUE?

Registry cleaners and rogue AVs are certainly not the only kinds of greyware that we have to deal with and there is other dubious software out there, even more problematic. One such category is that of downloader parasites found on various download servers. These applications are part of shady advertising campaigns to promote disreputable software. The downloaders often parasitize a popular application that is distributed freely. Win32/Multibar can be found on a Russian server that offers the download of the free trial version of *ESET NOD32 Antivirus*. But instead of simply downloading our anti-virus, an intermediary – the downloader – shows up. Its purpose is to distribute a third-party toolbar.

More examples of similar parasites appear when a user seeks to install the free *VLC Media Player*. The freeze.com download server features a potentially unwanted application. These smart operators have even managed to procure a *TRUSTe* certificate to increase their credibility. If you attempt to download *VLC* from the website vlc7.com, you will be presented with adware (Figure 14). This particular example changes the browser's search settings and asks for personal information.

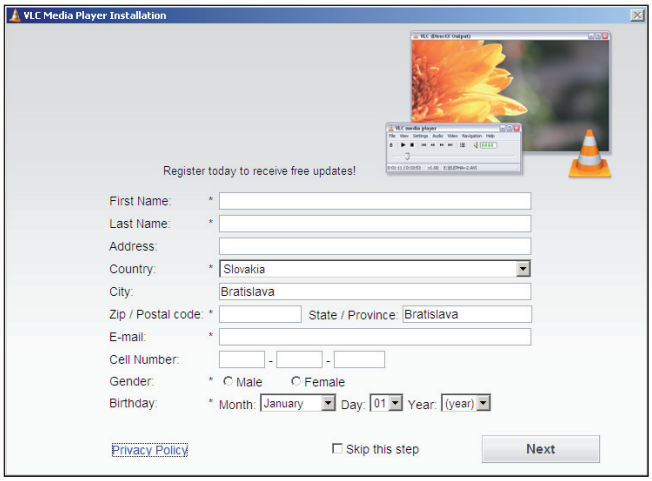

Figure 14: Greyware installation of VLC Media Player.

It is hard to think of a valid reason why users shouldn't download freeware applications from their official websites. Although this category of malware is not the typical trojan, in our opinion, it is nevertheless far from legitimate software.

60 EURO WEBSITES

A totally different type of scam is what we call '60 euro websites'. A current example preys on Slovak Internet users. The perpetrators behind it, a company called Online Investments Group Ltd., have taken advantage of the popularity of the 2011 World Ice Hockey Championships that took place in Bratislava and Košice. They have created a website that offers information about the World Cup (Figure 15). The only catch is that they offer 'premium content' at a steep price. The registration charge at the website sampionat.sk (with many other aliases) is €49.95 for 12 months' access. The website also tries to lure users to register by offering a contest to win a 3D television, laptop and other prizes.

The techniques used in this fraud very much resemble those used in other types of fraud, such as rogue AVs. The mention of the 50 euro fee is hidden in a long terms of service contract, written in tiny letters, that almost no one reads. The scammers make use of black hat search engine optimization and their malicious websites sometimes even achieved first place in web searches relating to the World Cup. In order to look more convincing (and safe), the website displays the official World Cup mascot and a banner claiming that it was tested by *ESET* security software. The owners of the respective logos (including our company) have each filed criminal complaints.

What makes this case even more serious is that the perpetrators send demands for payment to victims and threaten them with distress warrants and other legal

Figure 15: Ice Hockey World Championship online fraud.

repercussions if they don't pay the fees. The warnings are sent to non-paying registered users, but also to users that have never registered, where the criminals somehow managed to get hold of their contact information anyway. The contract and the following legal threats are not in accordance with the law, but they fulfil their purpose in frightening the user and extorting money from him.

This fraud, however, is nothing new and this organized crime group is responsible for scamming a large number of victims through different thematic websites, both in Slovakia and in other countries. Other websites that they have used include a portal featuring Slovak poetry, an online gaming site, a download server and so on. The Slovak liaison in the international crime scheme is known as the Adamco 'clan'. The 'boss' of the whole network seems to be a certain Michael Burat of Germany who is in charge of hundreds of similar websites in England, Germany, Slovakia and Italy. This group has extorted money from people using websites focused on last year's FIFA World Cup in South Africa, the Ice Hockey Championship in Slovakia this year, and is most certainly preparing for next year's major sporting events including the 2012 Olympic Games. They will surely succeed in ripping more people off unless someone stops them.

TO DETECT OR NOT TO DETECT?

The topic of potentially unwanted applications is an extremely sensitive one and the decisions that malware researchers have to make about their detection are often problematic.

The registry cleaners and other greyware that we've covered are not typical malware: however they are also, in our opinion, very far removed from legitimate applications. When analysing the 'maliciousness' of this kind of software, a range of different factors have to be considered, including the proposed benefits to the user, the potential threats, as well as the distribution channels.

Google summarizes the latter in its proposed software principles: 'Many internet users find that over time their computers become loaded with unwanted software – be it adware, spyware or just plain junk … Usually there are complex business relationships among the companies participating in a bundle. This can result in well-intentioned companies benefiting from the distribution or revenue

generated by software that does not benefit you. Getting paid to distribute, or paying money to be distributed with undesirable software enables more undesirable software. Responsible software makers and advertisers can work to prevent such distribution by avoiding these types of business relationships, even if they are through intermediaries. We are alarmed by the size of this problem, which we estimate to be causing hundreds of millions of dollars to be changing hands annually. Because of this magnitude and user impact, strong action by the industry is imperative.' [5]

More detailed explanations of what *ESET* considers a Potentially Unwanted Application or Potentially Unsafe Application are given in the white paper 'Problematic, Unloved and Argumentative'. An example definition of a PUA is 'software of dubious quality and reputation, which include programs that make outlandish, unverifiable and unsupportable claims about their efficacy, and/or generate deceptive false positive alarm reports of threats where none exists in order to mislead people into purchasing something they do not really want or need. Sometimes such programs make claims so misleading that they actually border on – or step across the border of – outright fraud' [7].

As we have mentioned, cases where the affected vendor does not complain about the detection of the PUA are very rare. The number of protests has risen in 2010 and the first half of 2011 at such a rate that it has become difficult to keep track. This increase, both in number and in complexity of the cases, has meant that *ESET* has had to dedicate three analysts to specialize only in this type of software. Legal threats are often involved, and therefore the Malware Research Lab receives complaints from two battlefronts – both the affected vendors, and our own frustrated legal department. These are understandably the reasons why the examples mentioned in this paper are, according to *VirusTotal*, detected by very few security companies.

The registry cleaners and other greyware that we have covered are not typical malware: however we feel that an application whose sole purpose is to make profit for its developer and/or distributor and which provides no value to the user, should not be given a 'free pass'. And since AV companies offer not only simple 'anti-virus' products, but also complex 'security suites', they should also protect users from such ambiguous and complex threats.

REFERENCES

[1] Malcho, J. Is there a lawyer in the lab? Proceedings of the 19th Virus Bulletin International Conference, 2009.

[2] Patanwala, T. ESET Threat Blog. Imitation is not always the sincerest form of flattery. 8 October 2010. http://blog.eset.com/2010/10/07/imitation-is-not-always-the-sincerest-form-of-flattery.

[3] Harley, D. ESET Threat Blog. More unflattering imitation. 17 March 2011. http://blog.eset.com/2011/03/17/more-unflattering-imitation.

[4] ESET Knowledgebase. Fake/Rogue E-Set Antivirus 2011 malware. 6 April 2011. http://kb.eset.com/esetkb/index?page=content&id=SOLN2697.

[5] Google. Software principles. 23 June 2006. http://www.google.com/about/corporate/company/software_principles.html.

[6] http://aumha.net/viewtopic.php?t=28099.

[7] Goretsky, A. Problematic, Unloved and Argumentative: What is a Potentially Unwanted Application (PUA)? In press. Will be available at http://www.eset.com/us/documentation/white-papers.