

Combating Twilight Zone Rogues

Using Legislative Derivatives to Fight Borderline Applications

Pekka Andelin
Malware Analyst, Lavasoft AB

Combating Twilight Zone Rogues

Using Legislative Derivatives to Fight Borderline Applications

Pekka Andelin
Malware Analyst
Lavasoft AB

When judging if an application can be considered a rogue program, malware analysts must look at a number of parameters. This has to be done in order to form a basis to decide if the application should be put into a security software program's detection database. Vendors in the anti-spyware/anti-virus industry, like Lavasoft, formulate their own criteria for what is considered improper practice or threatening to computer system integrity and/or user privacy. The detection criteria, or rule-base, is combined in a "strategic basis of detection criteria" which may bear different names. At Malware Labs at Lavasoft, this is called the Threat Analysis Index (TAI). Some applications are harder to index than others, due to the fact that they walk the line in a twilight zone between proper and improper practices. Taking action in such cases may generate a complaint from the vendor behind the detected application. The complaint may even escalate to a lawsuit where the defendant and the plaintiff have to drive their cases and defend their positions. If and when the matter reaches this point, the strategic basis of detection criteria is tested against the law.

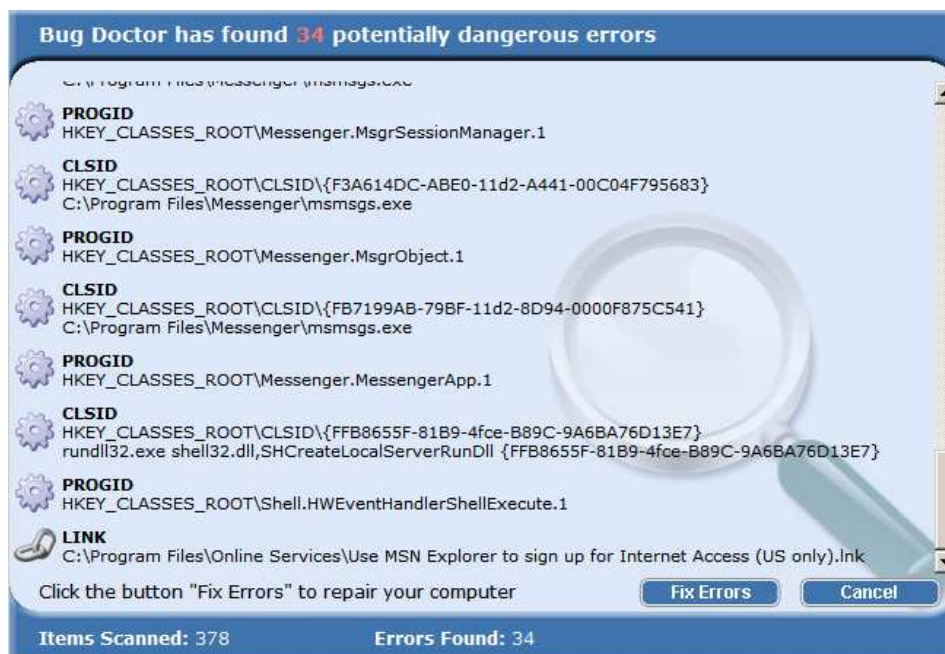
This article's objective is to illuminate if and how the forming of a strategic basis of detection criteria could benefit from using derivatives of existing legislation and directives, and to explore if and how the existing consumer protective legislation could be strengthened by the input or experiences of the anti-spyware/anti-virus industry.

Applications in the Twilight Zone

Assume that an application, or the vendor behind an application, is stating that it can fix bugs, errors and illegitimate/corrupt registry information on Windows operating systems. Scanning for such objects is a fairly common practice and a multitude of

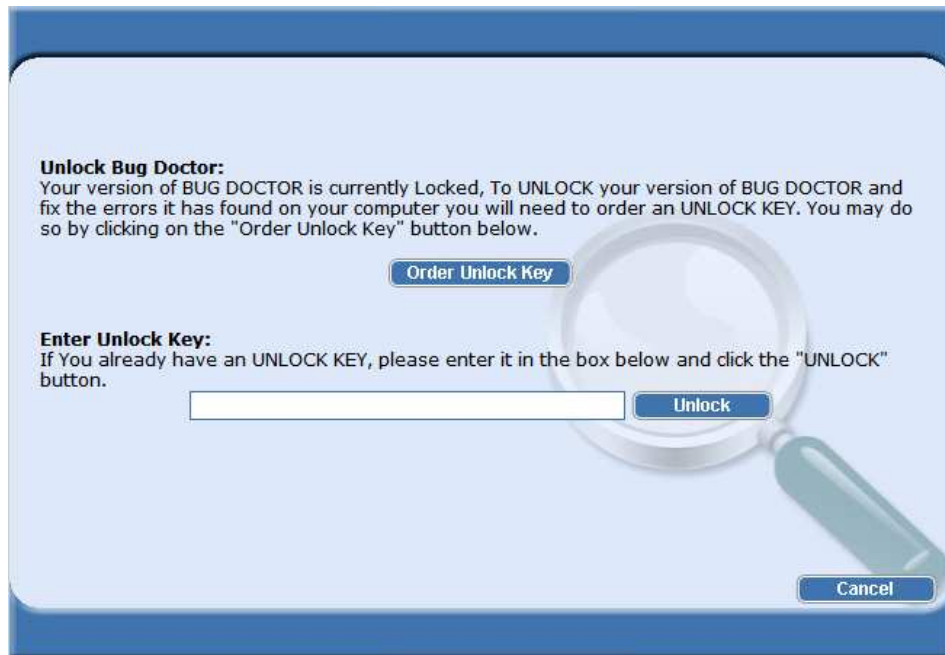
registry scanners/fixers/optimizers are available on the market both as freeware and commercial versions. A majority of PCs have some remnants in the registry from uninstalled applications or broken or invalid shortcuts. This means that a registry scanner/fixer most likely would find something, especially on the first scan. These issues, though, do not pose an immediate threat or danger to the system or its main operability.

The application shown below, PC Bug Doctor, is one example. The application presents the user with a list of findings under the header, "Bug Doctor has found 34 Potentially Dangerous Errors."



The above image shows the result of scanning a "normal" Windows XP Pro Operating System with the PC Bug Doctor application (BugDoctorSetup.exe version 5.0.2.4 with the md5 value of 0e3bdb05e4a239a119d4daod6fb48654). The test system was fully operational showing no noticeable lag due to the "Potentially Dangerous Errors" detected.

When users attempt to fix the errors, they are prompted to license the application by paying a fee.



The above image shows the result of pressing the "Fix Errors" button presented in the previous image.

Users are thereby urged to license the application in order to be able to fix the "potentially dangerous errors". Such marketing tactics could scare computer users, especially novice ones, into paying for the application. This tactic could be referred to as "marketing by fear".

Marketing by fear is not an uncommon practice. These tactics are often used by rogue applications where users are urged, or more or less forced, to install such applications. These applications are often easier to index due to other evidence of improper/malicious behavior (such as a high number of false positives or fake objects detected) that can help form a basis for categorization. The situation gets trickier when the application in question has a functional scan and the marketing tactics may constitute the only criteria for the indexing/categorization.

It can be argued that such borderline applications are becoming more prevalent. A shift from forced installations, or other clear rogue behavior, towards a direction where the rogue application may be harder to spot and pinpoint would pose new challenges for the anti-spyware/anti-virus industry. Rogue anti-spyware/anti-virus or "fixer"

applications that are marketed on increasingly professional and legitimate-looking websites could be able to trick even the most experienced users. These programs are often accompanied by highly positive user testimonials, like the examples shown below.

What was a last ditch attempt in 'saving' my PC turned into a life-saving exercise - I had the dreaded 'blue-screen' brought about by the MS Professional Office loop message conflict - which on at least one occasion also turned red - much to my major frustration and helplessness.

THANK YOU Bug Doctor - not only is my 'conflict' resolved, my PC runs like a dream and I once again have faith in human nature.

Hello! I have been using Bug Doctor for a few years now, and would not be without it! I love it because it truly does work. I recently had to reformat my hard drive and after a few days I noticed something was not right, it was sluggish and just not the way it should be.

So I thought well how could there be any problems after reformatting, I mean sure maybe something little, well what a surprise when I ran the Bug Doctor it found over 100 things wrong in almost every category. So I click on fix and viola! all done and believe me it ran better than ever!

This is no gimmick! I run it once or so a week and even though it doesn't find anything wrong every time, I'm sure if there is a problem it will find and fix it for me. Oh ya can I say that it is easy to use even if you're not a computer wiz? If you don't have it, you will be amazed like me!

I am a lifetime customer since 2/27/05. There are four programs I think every computer should have. A virus scanner, firewall, spyware scanner, and Bug Doctor. Bug Doctor is a must have and well worth the price, it will save you time and headache fixing your computer and it does it very fast. Well done Bug Doctor.

The Bug Doctor is awesome! Goodbye PC repairman. My PC is a lot faster now too. Thank you. Thank you

The above images show examples of highly positive user testimonials that may or may not own buoyancy.¹

Highly positive user testimonials may be the turning factor that pushes users into buying the software. The image, below, shows a customer response that was sent to the Malware Labs at Lavasoft (on 2009-02-03) by a user who discovered that the purchased Bug Doctor application was detected by Ad-Aware.

I have just downloaded Ad-Aware Pro on trial and on the first scan it has identified the programme Bug Doctor, which I purchased last week, as a potential scam programme.

Can you provide more information on Bug Doctor as it came with an impressive list of testimonials (albeit they could be fake).

Your unbiased advice would be appreciated.

The Bug Doctor setup file, "BugdoctorSetup.exe" version 5.0.2.4, was detected as a fraud tool by many security vendors – for example, Avira AntiVir, F-Secure and Kaspersky scanners (represented at the Hispasec Sistemas service VirusTotal.com).²

The use of ad services, such as Google or Reuters ad services, for advertising rogues is another tactic used in order to increase the market exposure of rogue applications.³⁴ Users are thereby drawn to the rogue sites where massive positive propaganda lures them to not just take the bait, but to swallow it hook, line, and sinker. Users that download and install these new types of rogue applications may not even know that they are being scammed. The application may be somewhat functional, but the extent of its functionality is often hard to pinpoint for novice users that have fallen for the trap.

¹ Retrieved from the www.pcbugdoctor.com website on 2009-02-12.

² VirusTotal.com. Scan results of the BugDoctor installer file "BugdoctorSetup.exe". <http://www.virustotal.com/analysis/3006a5ad14f95734ed2fdd00945acfdb>. Retrieved on 2009-02-12.

³ Tdaxp. "Malware on Reuters website?", <http://www.tdaxp.com/archive/2009/02/06/malware-on-reuters-website.html>. Retrieved on 2009-02-10.

⁴ Maximumpc. "Why is Google Running Ads for Known Malware Sites?", http://www.maximumpc.com/article/news/why_google_running_ads_known_malware_sites. Retrieved on 2009-02-10.

The rogue application may have even been purchased second hand from the creators, and the new owner may act as an administrator for his/her “business” – answering e-mails and/or phone calls and providing an update now and then. The owners/administrators of such scam projects may even send complaints to the anti-spyware/anti-virus vendors that have their application in detection, requesting re-evaluations and urging for redress. The analysis of such cases requires in-depth analysis and review by the anti-spyware/anti-virus vendor, encompassing the website, marketing strategies, incoming user reports and testimonials, promises that are made to users and how these promises are fulfilled, and validity of presented user testimonials. Such thorough analysis could, therefore, take up much valuable time and effort. In spite of that, all cases must be treated in the same just manner and a decision to put an application into detection has to be backed up with adequate evidence.

Legislation Derivatives – Swedish National Legislation

According to Konsumentverket, The Swedish Consumer Agency, traders may not use marketing methods that mislead consumers. Misleading, in this case, means using false claims or other representation which are deceptive in terms of the trader's own, or someone else's, business. According to Konsumentverket, the Swedish Markets Court has, in many cases, taken a position on what misleading advertising actually means. A starting point for assessment is the overall impression the petition gives the consumer at a fleeting contact. The tenth paragraph of the marketing law states that material information cannot be omitted in the marketing so that the petition is misleading. If the information provided is unclear, incomprehensible or ambiguous, it is equated with omitting information. The marketing law provides several examples of what is considered to be misleading practice and the examples provided are derived from the European Union's (EU's) Directive of Unfair Commercial Practices. The main objective is that if a method of marketing is to be considered unfair in accordance with the tenth paragraph of the marketing law, the marketing has to have commercial effect. This means that the marketing affects the recipient's ability to make informed business decisions. Violations of the marketing law can lead to a market disruption fee.⁵

⁵ Konsumentverket. “Vilseledande marknadsföring”, <http://www.konsumentratt.konsumentverket.se/mallar/sv/artikel.asp?lngCategoryId=495&lngArticleId=1896>. Retrieved on 2009-02-10.

Legislation Derivatives – EU Legislation

The EU Unfair Commercial Practices Directive was formally adopted in May 2005 (Directive 2005/29/EC on Unfair Commercial Practices) and the directive was updated with new rules on December 12, 2007. The updated directive outlines “sharp practices”, for example aggressive and misleading marketing, that is prohibited throughout the EU. The directive was also “future-proofed” by issuing a general ban on unfair commercial practices. The rules of the directive are to be enforced via national courts and national consumer protection authorities, such as Sweden’s Konsumentverket.⁶

The Unfair Commercial Practices Directive is supposed to reduce the differences in the consumer protection laws between different countries while keeping a good level of consumer protection. The directive is to protect consumers from marketing methods that impair the consumer’s ability to make an informed and efficient decision or choice; it applies to commercial practices that harm consumers’ economic interests. The directive further states that,

“It provides protection for consumers where there is no specific sectoral legislation at community level and prohibits traders from creating a false impression of the nature of products. This is particularly important for complex products with high levels of risk to consumers...”⁷

The directive states that information provided in order to help the customer make an informed and efficient transactional decision has to be disclosed when the trader makes an invitation to purchase. This means that such information will not have to be disclosed in all advertisements, but only when the trader makes an invitation to purchase. The directive also prohibits the promotion of products that look similar to other products if the resemblance confuses customers as to the commercial origin of the product in question. This would apply to several rogue applications that try to mimic the look of legitimate anti-spyware/anti-virus programs. Using such consumer-

⁶ European Commission, Consumer Affairs. “The Unfair Commercial Practices Directive”. http://ec.europa.eu/consumers/rights/index_en.htm. Retrieved on 2009-02-10.

⁷ Official Journal of the European Union. “DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005”. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EN:PDF>. Retrieved on 2009-02-10.

confusing strategies is considered to be misleading. Commercial practices that significantly impair the consumer's freedom of choice (for example, via harassment, coercion and undue influence) are considered to be aggressive commercial practices and are therefore prohibited.⁵ This may also apply to several rogue applications that constantly urge or nag users to license the rogue, thus hindering users from operating their systems in a normal manner. Some rogues use coercive tactics and undue influence in order to steer users to specific actions or locations, which takes away users' freedom of choice.

The ANNEX I of the directive provides 23 examples of misleading commercial practices and eight examples of aggressive commercial practices. Selected examples of each practice are shown below.⁵

Misleading Commercial Practices

1. Claiming to be a signatory to a code of conduct when the trader is not.
2. Displaying a trust mark, quality mark or equivalent without having obtained the necessary authorization.
3. Claiming that a code of conduct has an endorsement from a public or other body which it does not have.
12. Making a materially inaccurate claim concerning the nature and extent of the risk to the personal security of the consumer or his family if the consumer does not purchase the product.
13. Promoting a product similar to a product made by a particular manufacturer in such a manner as deliberately to mislead the consumer into believing that the product is made by that same manufacturer when it is not.
18. Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favorable than normal market conditions.
20. Describing a product as 'gratis', 'free', 'without charge' or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item.

Aggressive Commercial Practices

24. Creating the impression that the consumer cannot leave the premises until a contract is formed.

Concluding Thoughts

The directives associated with commercial practices, listed in ANNEX I, are also applicable to software applications. However, it is unclear if certain statements, like “risk to the personal security of the consumer”, also apply to the virtual extension of a person, such as a consumer making online purchases or installing software applications for evaluation. It could be argued that the virtual extension of a person should be considered an interface into the real world; experiences and events in the virtual world also tend to cause reactions in the real world and/or within the physical person behind the computer screen.

The fact that the new Unfair Commercial Practices Directive is built upon former legislation shows that, in order to be effective, laws and directives have to adapt to the current context, taking into account that new ways of trade and new marketing methods may emerge. Legislation and directives have to be efficient in the context that they are supposed to regulate.

The EU has even tried to future-proof the current legislation by issuing a general ban on unfair commercial practices.

Participants of the anti-spyware/anti-virus industry have the possibility to form rules or codes of conduct that can be elevated further – if adopted and approved by a majority and the state – to legislation and directives. The elevation process could be described as a dialectic spiral where the final formalization of adopted rules represents a merging of different opinions. Such elevated/formalized rule bases undergo a significant increase of efficiency or strength when adopted by a large majority. This is how laws and legislation are born.

The anti-spyware/anti-virus industry could be looked at as a choir, a buildup of different voices and characters that, in a joint effort, could generate fantastic tunes in harmony while still preserving unique nuances and individuality. The fantastic and harmonic tunes, in this case, refer to the joint power and efficiency of cooperating vendors in the

anti-spyware/anti-virus industry – a cooperative effort that would give more bite to the protection against unfair commercial practices in a digital context.

One of the objectives of the Unfair Commercial Practices Directive was and is to reduce the differences in the consumer protection laws between different countries. It could be argued that the plethora of different “strategic bases of detection criteria” within the anti-spyware/anti-virus industry, to some extent, reflect the scattered image of the Unfair Commercial Practices legislation that existed prior to the updated EU directive. (This is not to say, however, that the directive is a definitive solution).

Legislative efforts such as the Unfair Commercial Practices Directive and its derivatives could form a good basis for the formulation of a common “strategic basis of detection criteria” within the anti-spyware/anti-virus industry applicable especially for twilight zone applications that balance on the line between light (of legitimate applications) and darkness (of rogue applications).

A greater resemblance between the formulated strategic detection criteria and contextual legislation may very well be beneficial for the anti-spyware/anti-virus industry, giving needed leverage to combat borderline applications. It would be possible to develop a symbiotic relationship between legislators and the anti-spyware/anti-virus industry that could be mutually beneficial.

The efforts, experiences and expertise derived from the anti-spyware/anti-virus industries’ ongoing fight against current threats are a valuable information asset for legislators that, in many cases, lack that kind of in-depth knowledge. A closer cooperation between the anti-spyware/anti-virus industry and legislative authorities would help to enforce and extend consumer protective legislation that is striving to regulate commercial practices, including global networks.

The EU’s Unfair Commercial Practices Directive is set to be reviewed in 2011. The European Commission will conduct a comprehensive analysis on the application of the directive. The resulting report from that analysis shall be accompanied, if it is found to be necessary, by a revision proposal.⁵ This means that it is possible to influence legislators into taking into account possible extensions of the legislation – extensions that could be derived from the experiences of security professionals within the anti-spyware/anti-virus industry. Harmonizing the strategic basis of detection criteria with

the current legislation would give the strategic basis of detection criteria a closer resemblance to the legislation, such as the EU's Unfair Commercial Practices Directive, and possibly even increase its general acceptance. Such harmonization could also spare members of the anti-spyware/anti-virus industry the negative experience of having to sing "I fought the law and the law won" after a court session due to a vendor dispute.