

IS THERE A LAWYER IN THE LAB?

Juraj Malcho

ESET spol. s.r.o., Aupark Tower, 16th floor,
Einsteinova 24, 851 01 Bratislava, Slovakia

Email malcho@eset.sk

ABSTRACT

With the broadening possibilities and the ever-growing number of computer users, many applications are being developed that have hidden or fraudulent intentions, or which are at best of doubtful usefulness. The motivation behind these applications is financial profit and they typically target the technically low-skilled members of the population. Many such applications are not the typical malware used in cybercrime nowadays (like bots or spyware trojans), but rather potentially unsafe or unwanted applications. However, this dubious software is often associated with groups responsible for malware dissemination, and is often distributed using unfair practices such as spam campaigns or push-installations performed by malware.

When AV labs note these practices and add detection of such applications to their products, this causes a conflict of interests between AV software vendors and the suppliers of such potentially unwanted software. These conflicts sometimes result in legal battles, dragging many people into the decision-making process, including the legal department, and consuming a significant amount of a company's human and financial resources. The decision to detect such software is in many cases made even more difficult by the users themselves: different individuals, social groups and even nations have very different desires and opinions.

This paper explores the topics mentioned above and considers the boundary between legitimate and illegitimate applications. The problems are explained with reference to several case studies documenting our experiences with such software. Based on our records of such incidents we will outline the rising trend of complaints and legal cases over time.

MALWARE IN CURRENT CYBERCRIME

It has been quite a long time since the first personal computers hit the market, during which time many serious vulnerabilities and design faults have been discovered, and many things have changed. Mankind has slowly got used to the fact that every new technology can be misused, or rather, we can be fairly sure that someone will try to misuse it, whether merely to prove the concept of misuse, or to initiate a serious threat against people and/or the infrastructure. The design of new devices and technology must therefore take into account the securing of the data, dataflow, and any communication in general. However, the systems that are being developed today are more and more complex, so even though huge effort is invested in security, faults are quite often introduced during either the design or the implementation stage. The growing number of technologies and devices broadens the attack surface available to the attackers who try to make profits by exploiting existing security flaws. And that's exactly the domain of computer infiltrations.

Nowadays a vast amount of malicious or unwanted code is financially motivated. We could even say that there are only trace amounts of infiltration which exist only to demonstrate the presumed ability of the author (whether maliciously motivated or not). Proof-of-Concept (PoC) virus writing is not as popular as it used to be. In fact, if a security researcher nowadays hears the term PoC the first image that comes to mind is a chronic, even pathological search for security vulnerabilities and exploits programming. And yet often the underlying motivation is far from altruistic service or efforts to improve software reliability and security. On the contrary, new security vulnerabilities are now very much in demand on the black market, and present great opportunities for illegal income. That is the reason why PoC code and vulnerabilities tend to gravitate more easily towards malware authors than to the respective software developers.

And that's how we get to the typical malware of today, which takes advantage of some type of vulnerability – whether a technical or a human one. The decision about whether malice is intended and threat classification is very straightforward and unambiguous in this case. For an AV company the main problem here is implementing detection. The protection schemes in modern malware tend to be complicated, new variants are coming out in huge volumes and the professional groups on the other side work deliberately on evading detection. The income of these criminal groups is mostly derived from trading stolen credentials or any data stolen from compromised computers, or by renting botnet services, such as adware push-installations, advertisement and spam delivery or DDoS attacks.

THE GREY ZONE – ADWARE, SPYWARE, POTENTIALLY UNWANTED APPLICATIONS

Let's leave the clearly defined malicious code aside and focus more on greyware – the software from the grey zone. The complications with these applications are not usually inherent in code complexity, code protection/obfuscation, or in implementing detection. The problem lies in the decision as to whether the software is or is not malicious, or if it's actually useful somehow. Of course, one will automatically assume that the decision criteria have to be subjective and possibly ambiguous to some extent – every user could have a different opinion or different desires. So the boundary between good and evil, usefulness and uselessness is unclear. Even different AV companies might have different views on various issues and the philosophy might differ somewhat, leading to disagreements even among the experts.

Naturally, these companies cooperate closely (and not only in order to evade similarly conflicting situations). Over the years several projects and organizations have been established in order to introduce generally respected rules and best practices that have been developed and discussed within the community. One of the goals is to create a stable reference point which can be used in discussions of controversial issues. Let's mention a few of the initiatives that are most related to the topic of this article: the Anti-Virus Product Developers Consortium (AVPD), the Anti-Spyware Coalition (ASC) and the Anti-Malware Testing Standards Organization (AMTSO). AVPD [1] was formed to provide an open forum in which developers could work toward common goals such as product testing, product certification, surveys, studies and market research. ASC [2] is a group dedicated to building a consensus about

definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. And finally, AMTISO [3] was founded in May 2008 as an international non-profit association that focuses on addressing the global need for improvement in objectivity, quality and relevance of anti-malware testing methodologies. More information about these organizations and initiatives can be found on their web pages.

SPECIFICS OF THE GREY ZONE SOFTWARE

Let's have a closer look at the previously mentioned problematic software where the decision-making process about its malicious intent or legitimacy is complicated and tricky. What kind of software is it? Well, put very simply – it's the software that is, in fact, completely useless and doesn't provide any real value. Or, in other words, if the software is actually paid for, then the only party that gets any genuine benefit from it is the author/company that develops it. That's a very simple and elegant definition, right? But in the real world, endless discussions could be held regarding the usefulness or legitimacy of these kinds of software. What's worse, sometimes it even leads to lawsuits. It happens more and more often that after a lengthy analysis an AV company decides to detect some application and a few months later the developers complain about unjustified detection and request that the false positive (FP) be fixed. The rounds of decisions and considerations that follow are usually very uneasy due to the collision of interests. There are many factors that need to be taken into account – not only the software itself, but also the user base, and it is necessary to verify the company's credibility and to analyse the distribution channels that are used.

The distribution channels themselves can easily turn a legitimate application into an unwanted one. Basically we have two reasons to flag an application as potentially unsafe or unwanted: the application is being misused by some malware, or the distribution model constitutes direct incitements to illegal profit. In the first case you could think of countless system tools that are often misused by malware to enhance its features. Some examples are the system tools from *SysInternals/Microsoft*, various password crackers/password recovery tools, using remote administrator tools to implement backdoors, and so on. In the second case (the use of dubious distribution channels) we're talking about a pay-per-install business model where the distributor earns a small cut of the profit for every successful installation of the software. This effectively means that the software is often spread by malware and automatically installed on a victim's PC, or offered in spam campaigns.

A very important piece of information is the incentive for detection itself. Often it comes in the form of a request from the customers who notice strange and unexpected behaviour on the part of their PCs. Rogue companies and their products (rogue anti-virus, rogue anti-spyware) have their fraud fine-tuned to every little detail – the product and their website has a professional look, and often they are inspired by real anti-virus software. The websites are full of fake FAQ lists, along with lots of forged positive reactions and testimonies from non-existent users, etc. Even if we base our decisions on relatively clear rules and recommendations such as those made by the ASC, the decision is difficult and time consuming to make. An in-depth analysis can take hours and

days before a good reason for detection is found. That's where the AV companies expend a lot of resources nowadays.

It is beyond the scope of this article to talk in detail about the ASC rules and best practices: the relevant documents are available on the ASC website. In the following text we will focus on several concrete examples from history, through which we will illustrate the problems that AV companies encounter every day in regard to grey zone software.

ZLOB. THE EASY STUFF...

One of the first problematic cases is the notorious devastator of *Windows* boxes – Win32/TrojanDownloader.Zlob. The first variants appeared in autumn 2005. As with other new unknown families, it wasn't immediately clear how big this issue would become, whether it would be just one of many generic trojan downloaders, or whether it would become a long-term systematic project. That's why the first detections carried names like Win32/TrojanDownloader.Agent.NCW (*ESET*) or Trojan-Downloader.Win32.Agent.uz (*Kaspersky*). But shortly after, thanks to the activity of the group behind it, the family earned its unique identification – Zlob. As time went by new variants that were fine-tuned to evade detection by specific AV products started to appear on a daily basis. It was one of the first cases of one-on-one fights between a criminal group and AV companies where financially motivated malware was involved. But the other party became bored after some time and tried a new trick – they complained about the detection and requested that we cancel it (Figure 1).

```
From: support [mailto:support@emediacodec.com]
Sent: Wednesday, April 12, 2006 4:28 PM
To: xxx
Subject:
```

Hello xxx.

We are eMediaCodec support team. we would like to know why your software NOD32 detects our codec as virus "Win32/TrojanDownloader.Zlob.II".

Our emediocodec is provided with Terms and Conditions located at <http://www.emediocodec.com/terms.html> where we describe in details what is the codec itself. We do tell surfers about what being installed on their computers.

We would very appreciate if you remove our eMediaCodec from your virus list.

Thanks

Figure 1: emediocodec.com complaint.

Of course, however unprofessional this letter might look, it raises doubts and some uncertainty and forces one to verify the issue. There's a curious link to their website where you can, allegedly, find all the information about the codec. Well, as far as I remember, apart from installing other malware and advertisement delivery there was never any real all-playing codec functionality. More complaints followed and were repeated a few times, but eventually the group behind Zlob started generating such massive new waves of these trojans that they realized there wasn't the slightest chance of success in this direction. The number of files belonging to the Zlob family reached the thousands, endless numbers of computers have been infected to date, and the trojan itself has undergone a turbulent evolution. Nowadays, a PC infected with the Zlob trojan will end up with a rogue anti-virus or spyware on the system (among other things). Despite all the troubles, good

news arrived from the malware authors in January 2009 when they left a message for *Microsoft* employees in one of their most recent trojans (Figure 2):

```
For Windows Defender's Team:

I saw your post in the blog (10-Oct-2008) about my
previous message.

Just want to say 'Hello' from Russia.

You are really good guys. It was a surprise for me
that Microsoft can respond on threats so fast.

I can't sign here now (he-he, sorry), how it was
some years ago for more seriously vulnerability for
all Windows ;)

Happy New Year, guys, and good luck!

P.S. BTW, we are closing soon. Not because of your
work. :-))

So, you will not see some of my great ;) ideas in
that family of software.

Try to search in exploits/shellcodes and rootkits.

Also, it is funny (probably for you), but Microsoft
offered me a job to help improve some of Vista's
protection. It's not interesting for me, just a
life's irony.
```

Figure 2: Message from Zlob author(s) to Microsoft.

It seems that at least the original authors of the trojan plan to abandon the project. However, this family is already so full-blown and developed that we cannot say for certain that this will be the final end of Zlob. On the contrary, it's very likely some other group will continue to operate and improve it.

ROGUE ANTI-VIRUS/ANTI-SPYWARE. THINGS GET TRICKY...

The topic of fake/rogue anti-virus or anti-spyware products has been touched upon already in the section on Zlob. Briefly summarized, this is software that pretends to be a legitimate anti-virus solution, fools users into believing that non-existent malware was found on the system, and usually also offers the possibility of removal of the imaginary infiltrations. The goal of this fraudulent theatre is to force the user to buy the full product that allegedly removes the malware even more effectively than the evaluation version, which itself got installed onto the PC via illegitimate channels. The victim, in fact, pays for a graphical bubble, which is sitting on the system tray, consumes the system resources and, what's more, risks having his/her payment card details compromised or stolen.

This category of potentially unwanted software or spyware is a good candidate for close examination of the means of distribution and for demonstrating the differences in classification of the various software components that partake in the process of computer infection. It all usually starts in a pretty uncompromising manner, an unequivocal infection by a code that nobody would have a problem defining as malware. The typical scenario involves a security vulnerability, usually built into an automated exploit pack, hosted somewhere on the Internet. It's not unusual to see legitimate websites being compromised, having iframe redirects inserted into their HTML code. The iframes point to an attacker's server, which serves the malicious code. The installers/downloaders have all the typical features of trojans, so everything is pretty clear so far and there's no need to spend too much time deciding about the classification. Usually these codes fall into the trojan or trojan downloader categories.

But this isn't true of the software that actually gets downloaded by the trojan downloader – this one is classified as adware, spyware or an unwanted application. Why? Because even though its installation is forced, usually there is an End-User Licence Agreement (EULA) which explains all aspects regarding the rogue software, and to which the user actually confirms his agreement. So the software has actually been installed with the user's consent. Of course, the EULA says nothing about the means of distribution and the software vendors themselves disclaim involvement with the distribution channels. They are more or less successful in this, depending on the case. Anyway, this is the time when it's necessary to investigate any subtle features and details about the software, for example those mentioned in the ASC documents. The most important attributes are its invasiveness, its impact on system stability, security and integrity, the extent to which the authors are trying to obfuscate the code and evade detection and so on. These days we register hundreds of families of such rogue applications, and the level of pretended legitimacy and their quality varies from childish trivial attempts to solutions that look seriously professional.

The birth and first indications of the spreading of these applications date back to 2005, when families like WinAntivirus¹ appeared. Again, the first steps in its evolution were very similar to the case of Zlob, and even here we received complaints (Figure 3) about detecting this incredibly useful software.

```
Subject: NOD32 detects our products as malware
Date: 21 Aug 2006 10:21:51 -0500
From: xxx@winsoftware.com
To: xxx
```

```
I am contacting you on behalf of WinSoftware
Company.
Recently our Quality Assurance Department discovered
that parts of our product,
WinAntiVirus Pro 2006, were added to your anti-
malware database, and are currently being detected
as malware.
WinSoftware believes this may have been done
inadvertently; nevertheless this has a big impact
on our Company's reputation and on customer
satisfaction level. WinSoftware, therefore, requests
that you remove these product from your base no
later than fourteen (14) days from receipt of this
notification.
Please confirm receipt of this message.
```

```
Best regards,
xxx
Senior Vice-President, Legal Compliance
WinSoftware Ltd.
```

Figure 3: winsoftware.com complaint.

It has to be noted that, compared to the Zlob complaints we received, this one looks immeasurably more professional and serious. We see a stronger choice of words, they mention damage to the company's reputation and the request to remove the detection is followed by a 14-day deadline. Furthermore, during the installation the user agrees to a EULA, putting himself/herself fully into the hands of the creators of this alleged anti-virus. Of course, for any serious AV company such an application cannot be tolerated on the customers' PCs: therefore WinAntivirus, along with tens and hundreds of other families of rogue applications, stayed in the

¹ The names of rogue applications (especially AVs) starting with the words Win- or Antivirus- have, for obvious reasons, become very popular.

malware databases. But compared to Zlob there's a significant difference – fake AVs are not classified as trojans, but are rather put into the adware/spyware category, which means that they belong to extended sets of virus definitions². Simply, they lack the necessary level of aggressiveness and invasiveness that would clearly make them a trojan³.

Finally, we need to mention that nowadays the rogue AVs are being distributed along with other malware that is directly related to botnets: what's more, they're often being distributed by worms. Considering the obvious similarities in the protecting packers and obfuscation techniques, it's clear that behind the scenes there are always the same group(s), so there is no doubt about their illegitimate intentions.

ADWARE – DELIVERING (UNSOLICITED?) ADVERTISEMENTS. THE EASY PART

What about generic adware – software primarily specializing in the delivery of unsolicited advertisements? Software falling into this category is extremely diverse and, from the malware/adware/spyware classification point of view, there are examples that fall into all of the categories, from trojans through adware to potentially unwanted applications. The more aggressive the software⁴, the easier it is to make the decision about its classification. On the other hand, with rising aggressiveness the complexity of detection implementation also grows proportionally.

As has been said already, the decision process is often much more time consuming than the process of creating detection patterns. In fact, the genuine anti-virus and the problematic malware are two pieces of software standing against each other, having their existence in the system approved by EULAs, which the user has (often unknowingly and without reading) agreed to. And to prove that the vendors of this dubious software really mean it, we've seen several legal cases in the past, such as this one. In 2007, a company named Zango (also known as 180Solutions), notorious as an adware provider, made a charge against *Kaspersky Lab*, complaining that it was unjustly blocking software that Zango provides. In doing so, Zango alleged that *Kaspersky* was damaging its reputation and preventing it from doing business. The initial decision of the court sounded quite positive, as it basically stated that an interactive computer service provider (in the context of content filtering) has the right to block material that he or his customers consider objectionable. Still, it wasn't the end of the story, and further appeals followed. However, the final good news came in April 2009 when Zango announced that it was going out of business.

As we can see, adware detection and classification quite often involves walking on thin ice (see also the next section) and subtle details can make a huge difference. Any detection that turns out to be unjustified (at least in the eyes of the law) can cost an AV company a great deal in terms of resources and time. But it's the mission of an AV company to listen to the requests of its customers and to protect their computers from undesired software. Generally, nobody⁵ wants to have any

² This has, of course, evolved over time and the organization of malware databases and collections may have changed from company to company, which could have led to reclassification.

³ Well, we could hold a long discussion on this topic.

⁴ Some good examples would be Win32/TrojanDownloader.Swizzor or Win32/Adware.Virtumonde.

⁵ Even though Zango claimed the opposite.



Figure 4: An example of a green software site.

adware on their PC unless they aren't aware of the implications and of how ineffective and unstable it will make their PC. But is this really true?

EVER HEARD OF ADWARE IN CHINA? OH MY...

Let's find out. Putting aside all other problems with China as one of the world's greatest malware producers, the Chinese are very talented in many areas, from cultural to technological. China is known for its problem with piracy, as well as with software that, even though having some other specific functionality, displays various advertisements. This adware (dare I call it this in front of Chinese PC users?) is, day after day, becoming a nightmare for every virus analyst. But deeper investigation reveals that the adware phenomenon is just one of the results of the complicated software situation in China. One part of the problem is 'green' software. If you think this term is somehow related to initiatives related to writing environment-friendly code then you're totally wrong. As mentioned above, China is different and the word 'green' is no exception.

'Green' software usually means a standalone package, where there's no need to install the program, just download, double click and there's your *Adobe Photoshop CS4* full version (see Figure 4). Of course, before packaging, the software needs to be cracked, modified and 'improved' to fix problems like installing all over the disk, licence activation etc. There's no need to worry about the serial numbers or licence keys: they're very easy to obtain as there are tens and maybe hundreds of sites⁶ that offer these green packages. For some people green software equals free software, and in some cases it's even localized. The green websites have all of their material comprehensively organized so it's very easy to navigate for anybody who wants to get a copy of their favourite application. Also, there are custom OS packages that people go for when buying DIY machines. For example 'Windows XP – XXXX edition' would be a *Windows XP* customization done by XXXX group. Pretty much standard *Windows*, no need of activation of course, possibly with some additional commonly used software pre-installed⁷.

⁶ For example <http://www.onegreen.net/>.

⁷ For example <http://www.shenduxp.com/>.

What's interesting is the fact that these servers closely monitor the quality of the software they provide and make sure they don't offer infected content. There are no noble or altruistic reasons behind this – it's only about money. If the site is safe and trusted it gets positive reviews, more page hits and more downloads are performed and thus they make more money on the online advertisements they display.

So why are we talking about this? As with the known Chinese black-market 'original' CDs and DVDs, it is often very hard to distinguish between the original version and a hack coming from a green site. Thus many people and businesses could unknowingly run illegal software even though they are strictly against it in principle. In such an environment the software vendors are pushed to distribute their software for free but – with some ads inside. And that's how well-known legitimate software vendors actually start to create adware – welcome to the Chinese software business model!

Lots of people in China are well aware of the malware threat and know they are surrounded with these password-stealing trojans and other stuff. They actually feel that if they pay for anti-virus it's going to make them much safer. Having their box protected, they can go on to use the green software which of course isn't generally considered illegal. The AV that they paid for and trust is expected to protect them from possible threats that might be lurking at any of those green websites. And of course, the AV definitely shouldn't block all the good and useful software, green or not, which (even though full of ads) is still considered to be standard and absolutely normal – for the Chinese.

So what about the rest of the world? People are extremely allergic to even the slightest hint of advertising, having all those neat ad-blockers and filters, demanding removal of any applications that would exhibit this behaviour. So what exactly is adware? Does it really matter? To what extent are common computer users able to distinguish between what is and what is not good for them and make the right choice? Are we going to end up with double standards?⁸ This issue really causes heavy headaches in any virus lab around the world.

AND THERE ARE MORE CONFLICTS OUT THERE

The most problematic applications are those developed by relatively well-established companies that have real customers who seriously make use of their services. The mutual customers of such a company and of an AV solution provider then request that they are allowed to run both of the applications without conflicting or blocking each other. On the other side of the river there is a group of users who are very sensitive about their computers and won't allow the installation of anything that they do not fully trust. Corporate networks and IT systems are very specific environments where many (types of) applications are undesired/unwanted even though probably nobody would object when installing them on a home PC. Quite often these applications might be installed via dubious channels that the users might not be able to control and so the software indeed gets onto the PC as unsolicited content.

The hot topic of today is online casinos. There are vast numbers of people who want to play – and win – as it's real money that gets into the game. These applications can, but

⁸ It actually seems exactly so.

don't have to, deliver advertisements. Quite often they evolve over time from ad-delivering to non-ad-delivering. Their main problem is that they often use the open distribution model of affiliates who get their cut for every successful installation. In our current botnet era this model can be (and is) heavily misused to gain quick and easy money, so it's a common practice for these applications to be distributed by spam or even trojans. This results in more money being poured into the pockets of the criminal groups, and the installation of these applications onto a large number of PCs without the users' consent.

Since these companies do business with online casinos, their relationship with money is very tight and they don't hesitate to attack AV companies with requests to cease detection even at the price of a lawsuit. Thus the work of virus analysts evolved into a new and unexpected dimension, and the resolution of these issues has become extremely time consuming.

THE COMPLAINTS TIMELINE

Let's have a look at what all this has meant to a specific AV company – ESET. Over the last three and a half years we have come across over 20 cases where it was necessary to involve the legal department. Roughly summarized and at a conservative estimate, it cost us more than 1,150 man-hours and involved at least 530 employee interactions (not counting our external consultants or partners). Some of the incidents have been successfully resolved and closed, while many of them are still open and have been causing trouble for months. Typically, the load is not balanced but rather comes in spikes. Figure 5 displays the timeline of the number of employee interactions involved in resolving detection complaints per month.

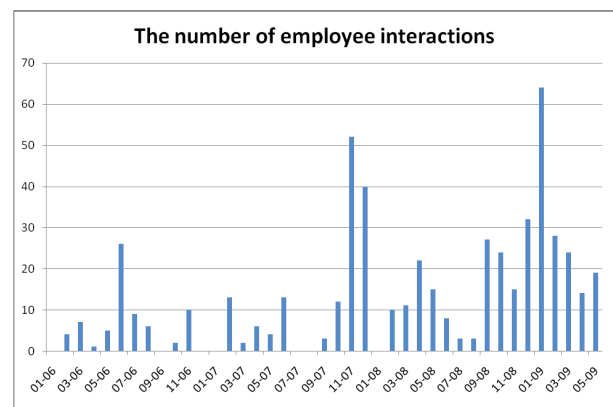


Figure 5: The number of incidents per month where ESET employees were involved in resolving detection complaints.

Of course, not all cases are equally complicated and the amount of time spent varies. Basically, it grows proportionally to the number of people involved and the graph is similar to Figure 5, with only slight differences (Figure 6).

Again, let me remind you that these numbers are rather conservative, as it's hard to determine the exact amount of time that virus analysts had to spend analysing endless numbers of software packages, comparing different versions and variants. Based on the graphs we see that in the last 12 months the average load was 46 man-hours, involving over 21 people per month, as opposed to an average of 16 man-hours/

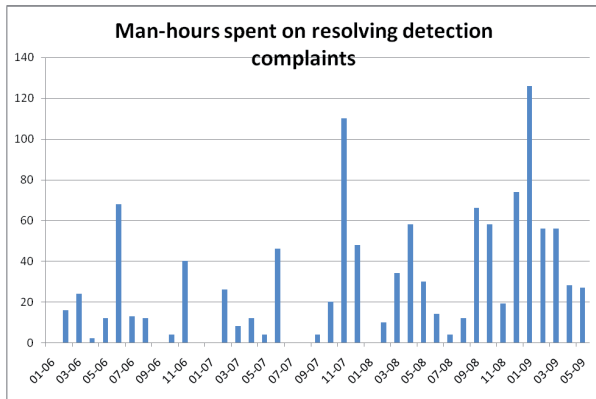


Figure 6: The number of man-hours spent on resolving detection complaints per month.

six people per month in 2006, which means triple growth in three years. Also, the spikes reach as high as 130 man-hours per month, which is almost equivalent to a full-time employee. Of course, in reality it is not possible to stay within these mathematically calculated boundaries: every task (not to mention the extra time spent switching between tasks) also takes its own time to manage. With the growing number of dubious software cases and all those people using proven and time-tested methods of deceiving inexperienced, trusting computer users, it's clear that these numbers will increase in the future and the growth will probably not remain linear.

CONCLUSIONS

As we can see in the interactions between AV companies and the providers of various dubious applications, the encounter with the law is starting to be a daily routine. As with any legal case, these issues are quite challenging, as well as time consuming and expensive. Past experience has shown that security failed to keep up with technology; these days we realize that legislation has pretty much the same problem, and it's very hard to deal with all the issues that result from the technological possibilities and opportunities. Parasitism is ruling the world and every now and then a smart guy appears trying to squeeze out some money from society – and of course, it's the law that matters, not morality. This applies to the fraudulent software we have mentioned in this paper, or to applications that target inexperienced, trusting people (for example, the 'I Am Rich' application for iPhones for \$1,000), or even to attempts to make money out of a ridiculous patent. The perfect example could be the case of a company named Information Protection and Authentication of Texas LLC⁹ [7] that is suing pretty much the whole AV industry for patents infringement. But you cannot avoid these things, it's impossible to exhaustively cover our current world with simple comprehensive rules.

In the end, all that's left is morality, and the moral implications of such issues; it may be straightforward to reach a resolution, and it may be really, really difficult. Defining what is and what isn't moral isn't really within the scope of this document but...

For current AV companies morality is a very fundamental issue. One needs to realize that running an AV company isn't

⁹ Paul Roberts really hit the nail on the head in his article [7] saying that this company appears to exist solely for the purpose of exercising its patent ownership rights in court.

just selling a specific piece of software. We are offering a service that allows even technically less adept people to keep their PCs in a relatively good condition, despite the danger that's lurking everywhere in the digital world. In the end, natural evolution has resulted in convergence between AV companies, or IT security specialists generally, and law enforcement. These people cooperate to fight cybercrime worldwide regardless of company boundaries, regardless of working hours and regardless of the missing pages in the law. In these undefined cases there's no other way but to follow one's instincts and morals – which are qualities that are absolutely natural to these folks. So when an AV specialist decides that some piece of software isn't very much to his liking and that it's potentially unsafe/unwanted/problematic, the chances are good that he's right.

REFERENCES

- [1] ICSA Labs Anti-Virus Product Developers Consortium. [https://www.icsalabs.com/icsa/topic.php?tid=fb33\\$17e3028d-905a8eba\\$0310-9492444d](https://www.icsalabs.com/icsa/topic.php?tid=fb33$17e3028d-905a8eba$0310-9492444d).
- [2] Anti-Spyware Coalition. <http://www.antispywarecoalition.org>.
- [3] Anti-Malware Testing Standards Organization. <http://www.amtso.org/>.
- [4] Anti-Spyware Coalition Risk Model Description. <http://www.antispywarecoalition.org/documents/riskmodel.htm>.
- [5] Zlob – best wishes with a hidden message. <http://mad.internetpol.fr/archives/8-Zlob-Best-Wishes-With-A-Hidden-Message.html>.
- [6] US District Court, Western District of Washington at Seattle. Zango, Inc vs. Kaspersky Lab, Inc.; case no. C07-0807-JCC. <http://www.taugh.com/zangokaspersky230ruling.pdf>.
- [7] Roberts, P. Infringement lawsuit blasts security Who's Who on app control. <http://blogs.the451group.com/security/2009/01/07/infringement-lawsuit-blasts-security-whos-who-on-app-control/>.