Security Software & Rogue Economics: New Technology or New Marketing?

David Harley CITP FBCS CISSP
ESET North America

About Author

David Harley CITP FBCS CISSP is CEO of security consultancy Small Blue-Green World and Senior Research Fellow at antivirus company ESET LLC. He also runs the Mac Virus web site, and is Chief Operations Office at AVIEN. He has been working in anti-malware research for over 20 years. He has authored, edited and otherwise contributed to over a dozen books on security, including «Viruses Revealed» and the «AVIEN Malware Defense Guide» as well as far too many articles and papers.

His previous roles included systems and network administration and support at what is now Cancer Research UK, management of the UK National Health Service's Threat Assessment Centre, and NHS messaging security.

He has been obsessed with psychosocial aspects of security, testing and evaluation since the early 1990s, and currently serves on the Board of Directors at AMTSO. He spends his barely-existent free time on photography, country walking, and the guitar.

Keywords

Free AV, Rogue AV, Rogue Applications, Social Engineering, User Behaviour, Behaviour Analysis, Criminal Behaviour, Rogue Services, Product Evaluation, User Psychology, Marketing, Multi-Disciplinary Teams, Support Scams, Sales, Support

Security Software & Rogue Economics: New Technology or New Marketing?

Abstract

A highlight of the 2009 Virus Bulletin Conference was a panel session on "Free AV vs paid-for AV; Rogue AVs", chaired by Paul Ducklin. As the title indicates, the discussion was clearly divided into two loosely related topics, but it was perhaps the first indication of a dawning awareness that the security industry has a problem that is only now being acknowledged.

Why is it so hard for the general public to distinguish between the legitimate AV marketing model and the rogue marketing approach used by rogue (fake) security software? Is it because the purveyors of rogue services are so fiendishly clever? Is it simply because the public is dumb? Is it, as many journalists would claim, the difficulty of discriminating between "legitimate" and criminal flavours of FUD (Fear, Uncertainty, Doubt)? Is the AV marketing model fundamentally flawed? In any case, the security industry needs to do a better job of explaining its business models in a way that clarifies the differences between real and fake anti-malware, and the way in which marketing models follow product architecture.

This doesn't just mean declining to mimic rogue AV marketing techniques, bad though they are for the industry and for the consumer: it's an educational initiative, and it involves educating the business user, the end-user, and the people who market and sell products. A security solution is far more than a scanner: it's a whole process that ranges from technical research and development, through marketing and sales, to post-sales support. But so is a security threat, and rogue applications involve a wide range of skills: not just the technical range associated with a Stuxnet-like, multi-disciplinary tiger team, but the broad skills ranging from development to search engine optimization, to the psychologies of evaluation and ergonomics, to identity and brand theft, to call centre operations that are hard to tell apart from legitimate support schemes, for the technically unsophisticated customer. A complex problem requires a complex and comprehensive solution, incorporating techniques and technologies that take into account the vulnerabilities inherent in the behaviour of criminals, end-users and even prospective customers, rather than focusing entirely on technologies for the detection of malicious binaries.

This paper contrasts existing malicious and legitimate technology and marketing, but also looks at ways in which holistic integration of multi-layered security packages might truly reduce the impact of the current wave of fake applications and services.

Introduction

"How much should we say at this point?" "I don't think it matters. We've never been able to protect ourselves from idle speculation." (Mankel, 1997)

A highlight of the 2009 Virus Bulletin Conference was a panel session on "Free AV vs paid-for AV; Rogue AVs" (Virus Bulletin, 2009).As the title indicates, the discussion was clearly divided into two loosely related topics. In fact, the connection between the two is less tenuous than it might seem, and the anti-malware industry will, sooner or later, have to come to terms with that fact rather more frankly than it has up to now.

The continued success of rogue marketing in its various forms and in various marketplaces convincingly demonstrates that the internet community continues to find it difficult to distinguish between legitimate marketing – also described by some outside the industry as FUD (Fear, Uncertainty, Doubt) marketing – and the "rogue" marketing approach used by fake AV. (Not for nothing is it often referred to as scareware.)

Rogue Mail

Why is it so hard? Is it because the purveyors of rogue services are so fiendishly clever? Diabolical criminal masterminds, like computer superbugs, are as scarce in real life as they're common in popular culture. For every Moriarty (Wikipedia, 2011a), Karla (Wikipedia, 2010) or Blofeld (Wikipedia, 2011b), there are multitudes of workaday criminals who make a living through the application of their practical knowledge of what makes a victim tick to social engineering, or through their ability to produce malicious code which is good enough to survive long enough to ensnare some victims before detection. And lower on the food chain, there are even more skiddies (Wikipedia, 2011c) and wannabe hackers who may get lucky.

Dumb and Dumber

So is it simply because the public is dumb? The psychology of victimology (Wikipedia, 2011d) and social engineering (Harley, 2008) is, perhaps, rather too broad and too far out of scope for this paper, but the mechanisms exploited by cybercriminals owe more to the "madness of crowds" (Mackay, 1841) and illustrate a failure of crowd intelligence (Wikipedia, 2011e) rather than "the wisdom of crowds" (Surowiecki, 2004). Not that this necessarily invalidates Surowiecki's central hypothesis: it's perfectly possible to argue that susceptibility to malicious social engineering, especially in a poorly understood field like malware and anti-malware, is a likely consequence of a problem with one or more of the key criteria that characterize a "wise crowd":

- Diversity of opinion
- Independence of opinion
- Specialization, access to local knowledge
- A mechanism for aggregating independent opinion into a collective decision.

Discussion

Many pundits would claim that the central issue here is the difficulty of discriminating between "legitimate" and criminal flavours of FUD (Fear, Uncertainty, Doubt), though this could very easily be viewed as a special case of the criteria problem outlined above.

Fear Pressure, Peer Pressure

In a very broad sense, of course, most marketing is based on the "fear" of the consequences of failing to respond to sales pressure, which itself is likely to exploit other pressures such as peer pressure. So we buy iGadgets in order to avoid appearing "uncool", medical insurance in order to avoid unnecessary pain or death, security software so as to escape the impact of destructive Trojans, or leakage of our sensitive personal or financial data. The border between advertising (or marketing, sales or PR) and social engineering (in the sense of the malicious psychological manipulation that is normally characterized by the term nowadays, rather than the more general sense in which it is used in social and political science (Harley, 1998) is sometimes very fuzzy indeed. Does this mean, then, that the AV marketing model is fundamentally flawed in that no-one would buy it if they weren't frightened of the consequences of infection by malware? If that's not the case, how is the security industry to explain its business models in a way that clarifies the differences between real and fake anti-malware, and the way in which marketing models follow product architecture?

If rogue AV marketing mimics the techniques used in legitimate marketing of legitimate security products, then it can't be enough for legitimate companies to decline to follow Rosenberger's "suggestion" (Rosenberger, 2010) that they might mimic rogue AV marketing techniques, bad though such techniques are for the industry and for the consumer.

The situation calls for an educational initiative, an exercise in social engineering (in a non-pejorative sense) on a grand scale, and it involves educating the business user, the end-user, and the people who market and sell products.

A security solution is far more than a scanner: it's a whole process that ranges from technical research and development, through marketing and sales, to post-sales support. But so is a security threat, and rogue applications involve a wide range of skills: not just the technical range associated with a Stuxnet-like, multi-disciplinary tiger team, but the broad skills ranging from development to search engine optimization, to the psychologies of evaluation and ergonomics, to identity and brand theft, to call centre operations that are hard to tell apart from legitimate support schemes, for the technically unsophisticated customer. A complex problem requires a complex and comprehensive solution, incorporating techniques and technologies that take into account the vulnerabilities inherent in the behaviour of criminals, end-users and even prospective customers, rather than focusing entirely on technologies for the detection of malicious binaries.

How Free is Free?

Free antivirus is not automatically considered a Bad Thing (Wikipedia, 2011f) by the security industry, even by those of us who earn their living from that industry and therefore need products that generate a revenue stream. In fact, free versions of commercial products do have a significant marketing function, as well as benefiting the user community (Mac Virus, 2010). This is the case whether they're free-for-personal-use scanners with limited functionality and support, or online scanners that give instant access to an up-to-date engine (again, with limited functionality and support), or fully-featured evaluation copies.

The use of free-for-personal use scanners *does* mean that more people (i.e. some of those who wouldn't *buy* AV) are protected by a near-commercial grade AV, even if functionality and/or support are limited, as is normally the case (Raywood, 2010). This is always the case, of course: the cost of producing mainstream AV has to be offset somewhere (Schrott, 2010), and it's usually underwritten by income from a for-fee, expanded-functionality version. Even open-source apps have to go this route eventually (or at least charge for documentation and support), and it's naive to assume (or at any rate suggest) that for-fee products are a "rip-off", as some reviewers have done (Edwards, 2007). This is, perhaps understandable in that consumer magazines cater for an audience that doesn't always understand the need for AV, doesn't want to pay for it if it can be helped, and is, like the business sector, far more forgiving towards what it doesn't pay for (Harley, 2006). [] According to a number of sources (Townsend, 2010; Retterbush, 2010; Morgan Stanley, 2010) 46% of consumers are reliant on free security software and that number is accelerating, while one report (OESIS 2010) suggests that "Though it might not be expected, companies that offer free products represent a majority of the market." (Harley, 2010a)

Goblin Market

However, the economics of the marketplace dictate that the consumer market isn't particularly profitable. It generally costs more than companies can afford to support non-paying customers, measured against the profit margin that keeps them afloat. (That, of course, is why some companies make single-user licences so expensive compared to their corporate deals.) So for many years, the deal with free AV has been a trade-off: fewer bells and whistles and in some cases less comprehensive detection and disinfection, and restricted support (for example, there may be support forums, but no one-to-one telephone support). (Townsend, 2010; Harley, 2009a)

Purveyors of rogue AV and fake support services understand these economic models very well – and are pretty good at counterfeiting them – but are even better at exploiting the fact that many people are naive enough to think that a free product is likely to resemble a for-fee product in all respects. They've even been known to borrow such principles as trial versions and offer support centre facilities (which may, admittedly, largely focus on sales issues and answering questions like "how do I uninstall an AV product that keeps flagging your product as malware?" (Harley, 2010b) Others claim (falsely) to have industry standard certifications for their "products," introduce rudimentary "real" detection into the product, slander vendor reputations in public security forums and even the vendor's own support forums, and threaten legal action against real security vendors and others who might expose them for what they are. Others sponsor links to what appear to be versions of legitimate security software, but are actually malware, fake security software, "possibly unwanted" or greyware. Somewhat more unusually, we've seen sites passed off as vendor sites offering downloads that appear to be security programs, but are actually NSIS scripts sending short codes to premium-rate texting services. And more recently, "rogueware" programs that actually borrow the identity of a genuine AV program, though not its "look and feel" (Response, 2011). In many respects, attacks like this are as much directed against the security community as they are against end users.

"TANSTAAFL economics" is a topic apparently (9-12 Project, 2009) far less well understood by the public at large, or even the media, which may award points for "value for money" (and so on) in comparative reviews in ways that sometimes confuse the issue. For instance, by skating over problems with a free product that would be flagged more dramatically with a for-fee product., or by failing to explain the restrictions on the availability of a free product for use outside the home. For example, the use of a free version is not usually permitted in a commercial environment – even a SOHO (Small Office, Home Office) environment – though there are one or two exceptions in that case.

Marketing with a Dull FUD

Mainstream anti-malware companies expend a significant proportion of their laboratory resources on the detection of so-called rogue security programs, which has become harder since the bad guys started to expend some of *their* resources on countering our detection by lab-testing *our* products in order to find ways of making our detection less effective.

Of course, the more successful a security company gets, the more likely it is to be attacked, using fuzzing, reverse-engineering and so on to stress-test security products, then using the results to generate better obfuscation wrappers and other defensive measures. To add insult to injury, where they used to use sites like Virus Total to check the effectiveness of their obfuscation against the latest scanner versions, they now use an in-house equivalent, or a "black" third-party equivalent.

Nowadays, a lot more people are already very aware of rogue security programs. But they may not be aware of how pervasive the organizational infrastructure that underlies them really is, or the variety of forms that such attacks are beginning to take.

False Profits

One of the main drivers here is obviously profit: after all, that's true of nearly all malware authoring nowadays. But this isn't just an attack on the credit cards of the consumers who are directly targeted. It's also an attack on the credibility and effectiveness of the security industry. There may be many who don’t believe that the security industry has too much of either, but bear with me: or at least consider the possibility that overall, we do more good than harm.

It’s not a coincidence that rogue products sometimes impersonate real products and services (Patanwala, 2010; Harley, 2011). We see legitimate brands, web sites and even malware descriptions misappropriated by fake AV companies.

Not so long ago, this author passed on information to a competitor about spam linking to a site claiming to be offering a new version of their product. It might even be true, up to a point: that operation, rather than being a straightforwardly fake and clearly malicious site, seems to specialize in charging its customers for access to software that’s available free from other sources (Harley, 2010c), and the competitor in question does indeed offer a free version of its scanner. However, this particular group has also offered access to a product known to be rogue, so the service that they’re offering is clearly not extravagantly fussy about the quality and legitimacy of the products it promotes, even if it has no direct alignment with the fake AV industry.

Fake Product, Fake Support

Many rogue products incorporate an “online support” button (Brulez, 2010), allowing the gang to escalate the victim’s engagement from free product to free (but very short term) trial product to remove the “infections” to customer satisfaction survey. This is nicely integrated into traditional approach, where “blackhat SEO” (Search Engine Optimization) is used to poison Google searches, driving potential victims to a malicious site where pop-ups flag “viruses” and demand money. And indeed, Innovative Marketing, an operation formerly responsible for a huge catalogue of rogue scumware, is somewhat celebrated for the size of its support infrastructure, though apparently its support staff were mostly dealing with enquiries such as: “I’m trying to install your product, but my antivirus keeps blocking it: how can I get it installed?”

Send in the (Fake) SAAS

In the past year or two, the author (Harley, 2010d) has become aware of a “service” whereby people are cold-called to let them know that they “have a problem” with malware infection, and were being offered a different as a replacement for their current “inadequate“ anti-virus. (Harley, 2010a)

Ongoing commentary and investigation (Harley, 2010e) has shown this attack to be characteristic of a group of sites in India offering dubious software and support services, and not only in the UK (Harley, Schrott & Zeleznak, 2010). Other companies have also reported this kind of scam: for instance, Symantec’s Orla Cox (2010) took up the theme, and Paul Ducklin (2010) blogged on it more recently at Sophos.

Low-Hanging Fruit in the Walled Garden

Ducklin made the useful point that as more ISPs start to consider the walled garden approach, by which a customer’s access to the Internet is conditional on the clean state of their machine, more of those customers will be conditioned into finding credibility in phone calls from remote call centres advising them of malware problems. While this aspect of the problem has particular local significance in Australia, the legal ramifications in other jurisdictions have been remarked elsewhere (Harley, Schrott & Zeleznak, 2010; Harley, 2011).

Blurring the Borders

Real anti-malware developers are harassed by legal threats when they detect fake security programs (and certain greyware) as malware, and that's not the only way in which they use our own weapons against us. Rob Rosenberger, an inveterate but often entertaining critic of the security industry, has long suggested that the AV industry has groomed the customer to accept the improbabilities of fake security marketing with its own marketing models (Harley, 2010f)). He's not altogether right, but he has a point: there's been a disturbing trend recently to escalating hype and fear-mongering in some corners of the industry, using techniques that seem modeled on rogue AV marketing. AV researchers have always been sticklers for ethics: if industry marketing becomes indistinguishable from that of the bad guys, companies don't just lose credibility with their customers, but with the experts who maintain the product backbone behind the marketing.

Faking IT

Criminals have long been misusing Search Engine Optimization (Black Hat SEO) to attract potential victims to web sites that trick them into thinking their machines are infested with viruses or spyware, and offering fake security software to "fix" problems that don't exist, or which they themselves have caused. For instance, by corrupting or encrypting files and then charging a fee to "recover" them.

Why do we call this rogue AV? (Harley, 2010b) While they do a good enough job of impersonating the AV industry to fool their victims, these aren't rogue AV developers: they're criminals, trying to confuse their victims by making it more difficult to distinguish between the disease and the cure. Some rogue AV may be have no direct destructive impact "worse" than the useless tonics and placebos of an old-time medicine show – a minor hit on the victim's bank book and a potentially dangerous sense of false security – but it can be worse. When a victim is tricked into giving out sensitive information, there are many ways in which it may be misused, apart from the original "sting" (Harley, 2010g)

Conclusion

So, naturalists observe, a flea
Has smaller fleas that on him prey;
And these have smaller still to bite 'em,
And so proceed ad infinitum. (Swift, 1733)

There's nothing new about fake security software (and other utilities); indeed, passing off malware as anti-virus is a way of tricking the victim into running it that goes back to the Black Baron (Harley, Slade, & Gattiker, 2001), and earlier. However, variations on the ways of exploiting the security-related fears of potential victims are, it seems, infinite. Gangs pushing rogue AV have shown energy and ingenuity in driving victims towards sites salted with fake AV, where they can take full advantage of those fears. Just as the real AV industry is accused of doing.

However, there is a distinct difference between meeting a demand that originates in a reasonable fear of a genuine threat (AV, insurance, flak jackets), and creating a demand that originates in ruthless exploitation of the fear of a threat that doesn't exist (fake AV, garlic and silver bullets), and offers little or no protection against real threats (malware, injury, shrapnel). Whether you like it or not (and lots of people outside the security industry seem to dislike it), the former is legitimate marketing. The latter is unequivocally fraudulent. The question remains: how does the average user learn to distinguish between the two? These "smaller fleas" are uncomfortable enough for the security industry, but constitute greater potential dangers than a fleabite to its customers.

Invitation to a Free Lunch

Let's start with an easier question: why shouldn't you use free antivirus? (Harley, 2009b) As already stated, the AV industry doesn't actually disapprove of free AV: most companies have free evaluation versions, and several have free online scanners, though the evaluation copy only functions for the evaluation period, and an online scanner has limited functionality, but completely free versions also have limitations. The message is, though, that anyone wanting to use a free version of a for-fee product needs to be sure that:

- They meet the eligibility criteria for using a free version. Vendors who make a free version of a commercial product available usually intend it to be available to home users or for evaluation only, not for multi-seat commercial offices.
- That the free product itself meets all their needs. Most free AV is limited to detection (and, in some cases, removal). Some free products don't detect the full range of malware, and don't usually have all the capabilities of a full-blown security product. (Schrott, 2010)

Free protection is in some senses better than no protection, as long as people don't expect more from it than it can actually offer. However, even the best "pure" anti-virus scanner in no way equates to comprehensive protection – by which I mean reasonably effective multi-layering, not 100% infallibility! – at home or in a commercial environment (Townsend, 2010). In fact, it could be said that with the possible exceptions of the occasional hobbyist programmer or teams of open source enthusiasts with no solid connection to the mainstream AV industry, the free-for-personal-use scanner is the last refuge of the pure anti-virus scanner. And even those free-for-personal-use editions aren't, of course, limited to the detection of self-replicating malware any more.

However, none of this is particularly helpful to the victim lured by Black Hat SEO or social media spam to a malicious site that pushes fake alerts leading to fake warnings. There have been approaches to making the distinction clearer at several levels, however.

Selling Education

Vendor-specific approaches have included including access to educational material built into a scanner sales package, such as access to a "tips" web site, informational newsletters and so on. These seem to be useful in that they can bring customers to resources that they would not have accessed otherwise, as long as those resources are security-centred rather than marketing-focused. (That isn't to say that informational resources should never include any sort of marketing agenda, of course: that might be ideal, but would hardly be realistic.)

Behave Yourself!

One possible approach was suggested in a 2009 paper for the Virus Bulletin Conference on using the behaviour of the user *as well as* that of malware to train both the software and the user to be more effective at defending a system (Debrosse & Harley, 2009). Of course, behavioural analysis is a standard tool for today's anti-malware, but analysing the behaviour of the user as well as (if not instead of) that of the program is a dramatically different approach to incorporating education into marketing.

However, these approaches have one major flaw in the context of this topic: they involve an element of preaching to the choir. That is, they are most likely to benefit someone who has already bought a product, and is therefore less likely to fall for a fake alert (though it's by no means unknown). While there's no absolute answer to that objection, at least a partial answer is for vendors (individually and as an industry) to think more holistically about their position as suppliers not only of products and services, but also of education, through blogs and white papers, and through participation in multi-disciplinary forums and informational initiatives in the public interest.

Explanation is Education

Security companies are going to have to do a better job of explaining their business models in order to make clearer the difference between the rogue approach to marketing and provision, and the legitimate approach. And that means a lot more than mimicking rogue AV's FUD marketing: it's an educational initiative, and it involves educating the business user, the end-user, and the people who market and sell products. Every time someone tries to sell a product using quasi-rogue approaches , they trade a short-term possible economic advantage for a long-term drop in the industry's credibility. That's bad for the industry, of course, but it's also bad for the consumer. It exposes him to further confusion between rogue and legitimate, and he'll tend to go for what sounds like the better (something for nothing) deal.

The Common Computing Security Standards Consortium has a list of "trusted vendors" at http://www.ccssforum.org/trusted-vendors.php. It lists vendors by name and includes various items of information, perhaps most usefully, the main URLs for those vendors. While there are many informational sites that include URLs for security vendors, this one has an advantage in that its list was compiled during extensive discussions on an associated mailing list of the definitions of trusted and the entire fake AV problem, so there was a certain informal filtering of company names based on an existing web of trust. Unfortunately, it isn't clear that this list or initiative is being maintained. However, the approach is valid and a similar initiative could be helpful – though no panacea – and could indeed be extended, for instance, to develop a joint code of conduct for the marketing of security products, to make it harder for purveyors of fake products and services to mimic and pervert legitimate practices.

References

9-12 Project (2009). TANSTAAFL: The FIRST (and most important) Rule of Economics. Retrieved 1st February, 2011, from http://www.educatetheelectorate.com/index.php?option=com_content&view=article&id=110:tanstaafl&catid=44:basics&Itemid=114.

Brulez, N. (2010). Technical support – they're not always the good guys. Retrieved 1st February, 2011, from http://www.net-security.org/malware_news.php?id=1402.

Cox, O. (2010). Technical Support Phone Scams. Retrieved 1st February, 2011, from http://www.symantec.com/connect/blogs/technical-support-phone-scams.

Debrosse, J. & Harley, D. (2009). Malice Through the Looking Glass: Behaviour Analysis for the Next Decade. Virus Bulletin Conference Proceedings. Retrieved 1st February, 2011, from http://www.eset.com/resources/white-papers/Harley-Debrosse-VB2009.pdf.

Ducklin, P. (2010). Sick of call centres? Don't worry, it gets worse. Retrieved 1st February, 2011, from http://nakedsecurity.sophos.com/2010/11/04/sick-of-call-centres/.

Edwards, S. (2007). The Great Anti-Virus Rip-Off. Computer Shopper, pp 125-131, Dennis Publishing.

Harley, D., Schrott, U., Zeleznak, J. (2010). Hanging On The Telephone: Antivirus Cold-Calling Support Scams. (In press)

Harley, D., Slade, R., Gattiker, U. (2001). Viruses Revealed: Osborne.

Harley, D. (1998). Re-Floating the Titanic: Dealing with Social Engineering Attacks. EICAR Conference Proceedings. Retrieved 1st February, 2011, from http://smallbluegreenblog.wordpress.com/2010/04/16/re-floating-the-titanic-social-engineering-paper/.

Harley, D. (2006). I'm OK, You're Not OK, Virus Bulletin. Retrieved 1st February, 2011, from http://www.virusbtn.com/virusbulletin/archive/2006/11/vb200611-OK.

Harley, D. (2009a). Microsoft AV Revisited. Retrieved 1st February, 2011, from http://blog.eset.com/2009/06/23/microsoft-av-revisited.

Harley, D. (2009b).More Free Lunches. Retrieved 1st February, 2011, from http://blog.eset.com/2009/08/03/more-free-lunches.

Harley, D. (2010a). Fake AV, Fake Support. Security Week. Retrieved 1st February, 2011, from http://www.securityweek.com/fake-av-fake-support.

Harley, D. (2010b). Security Zone: Faking IT Support. Retrieved 1st February, 2011, from http://www.computerweekly.com/Articles/2010/10/04/243165/Security-Zone-Faking-IT-support.htm

Harley, D. (2010c). Limewire, free software, and for-fee membership. Retrieved 1st February, 2011, from http://blog.eset.com/2010/10/27/limewire-free-software-and-for-fee-membership.

Harley, D. (2010d). Fake AV Support Scams. Retrieved 1st February, 2011, from http://blog.eset.com/2010/07/20/fake-av-support-scams.

Harley, D. (2010e). Retrieved 1st February, 2011, from http://blog.eset.com/?s=support+scams.

Harley, D. (2010f). Fake anti-malware blurring the boundaries. Retrieved 1st February, 2011, from http://blog.eset.com/2009/10/24/fake-anti-malware-blurring-the-boundaries

Harley, D. (2010g). Anti-Antimalware: Faking It, Not Really Making It. Retrieved 1st February, 2011, from http://blog.eset.com/2009/02/20/anti-antimalware-faking-it-not-really-making-it.

Harley, D. (2011). AV Company, Heal Thyself. Retrieved 25th March, 2011, from http://www.scmagazineus.com/av-company-heal-thyself/article/199043/.

Mackay, C. (1841). Extraordinary Popular Delusions and the Madness of Crowds, Richard Bentley.

Mac Virus (2010). Sophos Goes AVG. Retrieved 1st February, 2011, from http://macviruscom.wordpress.com/2010/11/02/sophos-goes-avg/.

Mankel, H. (1997). Steget efter (English translation by Ebba Segerberg: *One Step Behind*, 2002): Harvill Secker.

Morgan Stanley (2010). Changing Consumer Security Economics: the Rise of Free. Retrieved 1st February, 2011, from http://www.pandainsight.com/es/wp-content/uploads/2010/06/The-Rise-of-Free-MS-17-May-10.pdf.

OESIS (2010) Worldwide Antivirus Market Share. Retrieved 1st February, 2011, from http://www.oesisok.com/news-resources/reports/worldwide-antivirus-market-share-report%202010.

Patanwala, T. (2010). Imitation is not always the sincerest form of flattery. Retrieved 1st February, 2011, from http://blog.eset.com/2010/10/07/imitation-is-not-always-the-sincerest-form-of-flattery.

Raywood, D. (2010). How savvy are consumers when it comes to anti-virus? SC Magazine. Retrieved 1st February, 2011, from http://www.scmagazineuk.com/how-savvy-are-consumers-when-it-comes-to-anti-virus/article/192457/?DCMP=EMC-SCUK_Newswire.

Response (2011). With great name comes great liability? Retrieved 1st February, 2011, from http://www.f-secure.com/weblog/archives/00002090.html.

Retterbush, T. (2010). Free vs. Paid Anti-Virus Protection. Retrieved 1st February, 2011, from http://tomretterbush.posterous.com/free-vs-paid-anti-virus-protection.

Rosenberger, R. (2010). Zone Alarm Dabbling in "Scareware" Tactics. Retrieved 1st February, 2011, from http://vmyths.com/2010/09/20/zonealarm/.

Schrott, U. (2010). Guest Blog: How Free is Free Antivirus? Retrieved 1st February, 2011, from http://blog.eset.com/2010/04/14/guest-blog-how-free-is-free-antivirus.

Surowiecki, J. (2004). The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations: Doubleday; Anchor.

Swift, J. (1733). On Poetry: a Rhapsody. In The Poems of Jonathan Swift. Retrieved 1st February, 2011, from http://www.gutenberg.org/files/14353/14353-8.txt.

Townsend, K. (2010). Anti-Virus and Anti-Spam: a Technology Update. Retrieved 1st February, 2011, from https://kevtownsend.wordpress.com/2010/12/07/anti-virus-and-anti-spam-a-technology-update-2/.

Virus Bulletin (2009). Panel discussion: Free AV vs paid-for AV, Rogue AVs. Retrieved 1st February, 2011, from http://www.virusbtn.com/conference/vb2009/abstracts/Panel.xml.

Wikipedia (2011a). Professor Moriarty. Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/Professor_Moriarty.

Wikipedia (2010). Karla (fictional character). Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/Karla_(fictional_character).

Wikipedia (2011b). Ernst Stavro Blofeld. Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/Ernst_Stavro_Blofeld.

Wikipedia (2011c). Script Kiddie. Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/Script_kiddie.

Wikipedia (2011d) Victimology. Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/Victimology.

Wikipedia (2011e). The Wisdom of Crowds. Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/The_Wisdom_of_Crowds.

Wikipedia (2011f). 1066 and All That. Retrieved 1st February, 2011, from http://en.wikipedia.org/wiki/1066_and_All_That.