Malware, Marketing and Education: Soundbites or Sound Practice?

David Harley BA CISSP FBCS CITP

Director of Malware Intelligence, ESET LLC

Randy Abrams

Director of Technical Education, ESET LLC

This paper was presented at the 12th Association of anti Virus Asia Researchers International Conference (AVAR 2009) in Kyoto, and was published in the Conference Proceedings.

Abstract

What are the cornerstones of success in the anti-malware industry? Sound technology, of course. Sound marketing, too: a good product is of little use if no-one knows enough to go out and buy it. There are other factors too: sound after-sales and support service, for instance, influences the deployment, maintenance and efficacy of a product or service. Is this enough?

Commercial viability is paramount, but this industry has not generally been driven solely by profit. Many researchers believe that we have a responsibility to the community to contribute to making the online world a safer place. We try to do this not only by promoting our own products, but by raising general awareness of current threat and anti-threat trends and issues, the need for self protection, and ways in which our services fit into a wider scheme of community education and awareness.

In this paper, we look in detail at educational mechanisms such as inter-organizational community initiatives like AMTSO, security company blogging, and various forms of informational literature. Drawing on our experience as educationalists both inside and beyond the vendor community, we consider the practical, strategic and ethical issues that arise when a security company augments its marketing role with recognition of its civic responsibilities.

Introduction

Let's not be naive about this: while both individual anti-malware researchers and security companies as corporate entities have invested heavily in pro bono publico initiatives (and we'll consider some of those in due course), mainstream anti-malware is a commercial venture: product developers and researchers generally have to make a living like anyone else, and commercial success enables them, and the many co-workers who support their core activities, to eat.

What are the cornerstones of success in the anti-malware industry? Sound technology, of course, and in a purist sense good technology might be seen as its own reward. Certainly there are many people in the security industry who seem to see commercial success as a secondary consideration, sometimes as a factor that only becomes a target comparatively late in the project. Often, perhaps, this reflects a growing realization that lack of revenue stream is limiting the potential of a promising security potential, and a product that originated in academia or as an open source product or service acquires a for-fee version and a full-blown marketing operation. Not that this at all negates the value of those who use their commercial acumen to spot a niche for a new product and go all out to make money from filling it: there are many ways in which a useful product may come into being.

At some point, however, it becomes clear that sound marketing has become a necessity: a good product is of little use if no-one knows enough to go out and buy it. In fact, even a free product is generally marketed, and we're not only referring to trial versions, or to other free products that are made available with limited functionality compared to the full-strength "industrial" version but are free to eligible groups (home users, for instance). These have a clear altruistic purpose: they enhance the security of the community as a whole, while reducing the vulnerability of groups that aren't primarily seen as potential customers. However, they may also have an (entirely legitimate) commercial agenda, in that they build trust in the brand name, as well as acting as a freely available demonstration of the core technology.

Products and services that don't have an overt association with a commercial venture are also likely to arise from a more complex set of motivational factors than pure altruism: for instance, scientific curiosity, ego gratification, the desire to demonstrate competence as a precursor to finding paid employment in the industry, the urge to prove a concept technically before developing it as a commercial venture, or to attract funding for an academic project.

There are other factors too: sound after-sales and support service, for instance, influences the deployment, maintenance and efficacy of a product or service, but it doesn't come cheap, and there may come a point in a product's development cycle where hard decisions have to be made to keep the cost of unlimited support from rendering the product uneconomic to maintain. Commercial viability is, therefore, paramount, at least for a commercial product, where a small core development team may be supported by a huge global infrastructure.

However, this industry has not generally been driven solely by profit, and it's naive to assume that the effectiveness of researchers in the industry is compromised by the need to eat. Should we assume that a doctor or policeman is only to trustworthy if his income is independent of his chosen profession? Or, come to that, is it really safe to assume that research and/or development in the absence of an overt commercial agenda is necessarily more altruistic let alone more effective? We could (but won't) name software that has, however pure the intentions of their developers, done as much harm as good because the users of that software didn't realize

the limitations implicit in its development, purpose, implementation or support. We can, of course, also name free programs whose contribution to the welfare of the community has been considerable. However, many of these have either made the transition into full commercial products, or ceased development as it became impractical to continue support on a voluntary basis.

In the commercial world, however, many researchers believe that we have a responsibility to the community to contribute to making the online world a safer place. Promotion of our own products is not the only way in which we try to do this (though most of us would not be doing what we do if we didn't believe those products do make a valid contribution). We also aim to raise general awareness of current threat and anti-threat trends and issues, the need for self protection (in a general sense: there are few researchers in the anti-virus world today who wouldn't advocate multi-layered protection rather than reliance on an AV product, even their own) , and ways in which our services fit into a wider scheme of community education and awareness.

Community Initiatives

What do we mean by the community? Well, that depends on context of course. Security researchers, especially in the anti-malware industry, have a reputation (not always undeserved) for being clannish, exclusive and introverted, self-defensive, and hostile to anyone who tries to break into the inner circle uninvited. To some extent this is a reaction to the realities of the malware/anti-malware war of attrition: today, more than ever, the black hats watch the white hats as carefully as we watch them, and keeping secrets (and maintaining a "web of trust") is critical to maintaining some sort of balance of power.

Certainly, though, there's a degree of cooperation between researchers within the anti-malware industry, the wider security industry, and voluntary groups on the fringes of the industry that the media and the public are often unaware of. However, this cooperation (in terms of sharing of information and resources) is not purely self-interested – law enforcement groups, for example, are not primarily interested in maintaining the wellbeing of anti-virus companies. Rather, this community should be seen as a coalition of interested (and yes, to some extent self-interested) groups pooling expertise and resources in the interests of the wider community of legitimate users of computers and the Internet. Sometimes these activities result in publicly visible initiatives such as the Conficker Working Group, but this particular community more often resembles the proverbial swan, doing a great deal of invisible paddling under the surface of the water.

However, in this paper we aim to consider more public initiatives: primarily, educational mechanisms such as inter-organizational community initiatives like AMTSO (Anti-Malware Testing Standards Organization)and APWG (Anti-Phishing Working Group), wider community initiatives such as "Securing our eCity", corporate blogging as carried out by security companies, and various forms of informational literature such as white papers and conference papers, and their relationship to overt promotional literature. Drawing on our experience as educationalists both inside and beyond the vendor community, we consider the practical, strategic and ethical issues that arise when a security company augments its marketing role with recognition of its civic responsibilities.

Industry Alliances

There have been a number of industry alliances over the years: AVAR (Association of anti Virus Asia Researchers), of course, is a notable example, while EICAR (formerly the European Institute for Computer Antivirus Research) and CARO (Computer Anti-virus Research

Organization) also have missions targeting wider communities. They are commonly associated with conferences and workshops (and sometimes other initiatives such as the CARO naming scheme and EICAR working groups) that have an impact outside the “inner circle” of members.

Virus Bulletin [1] (both the magazine and the conference) is slightly different in that it derives from a community-oriented project initiated by a single vendor: however, it provides services such as product testing and the yearly conference that not only have wide impact, but also represent cooperation between many vendors and other groups, effected as sponsorship, subscriptions, contribution of technical material and so on.

AVIEN is different again, in that it originated in a desire to improve networking between researchers in the independent and customer communities, rather than within the industry, but quickly widened to provide a common meeting ground between the industry and its more knowledgeable customers. AVIEN’s future is under discussion at the moment, and probably lies in a more service-oriented incarnation, but in the past the organization has initiated a number of community-facing projects such as online conferences and a major book. [2]

The WildList Organization originated in a desire to track the impact of In-the-Wild replicative malware [3], and developed into a major resource for anti-malware testers and certification specialists. Unusually, it has never worked on a direct subscription model, perhaps reflecting the need for trusted individuals as reporters rather than primary corporate representation: when its existence was threatened by limited resources, the way out turned out to be absorption by independent testing organization ICSALabs, now part of Verizon [4].

AMTSO (the Anti-Malware Testing Standards Organization), while intended from its inception as a major information resource in the field of product testing, went straight for not-for-profit status, but on the basis of a corporate-sized subscription that would allow it to meet its ambitious aims. The organization stands out in that its main focus is explicitly educational and informative. The Anti-Phishing Working Group is also subscription-based: unlike AMTSO, however, it works on the basis of a wide range of subscription/sponsorship options that offer different degrees of participation and access to resources.

AMTSO and APWG differ from some of the organizations mentioned earlier in that they cover a range of participants that goes beyond the security industry. At present AMTSO tends to attract a range of vendors, testers, and advisors from academia and elsewhere. APWG similarly attracts interested parties from vendors to financial institutions to law enforcement, reflecting the range of activities the organization has initiated: again, while much of its activity is based on information sharing, it also has a strong educational focus.

“Securing our eCity” [5] is very much a community-facing project aimed at helping the whole spectrum of end-users to be better-prepared to face the perils of the 21st century threatscape. It has also attracted a range of contributors and sponsors, from inside and outside the security industry, and merits a mention here in that it is showing signs of growing from a local initiative to a national and even international venture.

Whiter Than White Papers

What exactly is a white paper? Well, the concept has travelled a long way from its parliamentary origins to mean, in this industry at any rate, almost any informational paper. Looking at almost any security industry white paper library, we find a mixture of styles, formats and content that can include conference paper reprints, journal and magazine reprints, high gloss marketing literature, product documentation, highly technical papers looking at a single topic in depth, short overview

papers, comparative test data, and so on. Well, it's all, hopefully, information (rather than misinformation). Clearly there are issues that have to be borne in mind with any published material, however transient it might seen, and papers often have a life as hard copy as well as being soft copy.

Clearly, any form of documentation on a corporate site will be seen as the responsibility of the site owner as well as (or even rather than) that of the individual author, and there need to be clear policies and guidelines on how to present written material for which the company bears that responsibility. Here are some legal issues that are particularly pertinent, though it's likely that however comprehensive we make this section, there will always be some eventuality we haven't thought of. Presenting content that is not illegal or litigable (bearing in mind that state and national borders mean a lot less on the Internet) may sometimes be more of a challenge than it might seem.

- Four letter words and innuendo may be funny in some contexts, offensive or even illegal in others. It's likely that a security site will, at some time or other, feel the need to comment on grimmer aspects of 21st century life such as physical violence, various forms of pornography, child abuse and so on, and content that addresses these issues must be very carefully and sensitively executed in order to avoid setting off a legal landmine somewhere in the world. Clearly, you wouldn't want to illustrate a point about paedophilia with an image taken from a site offering child pornography that would match some form of culpability metric such as the Copine Scale [6] It might be less obvious, though, that a verbal description of such content might also be seen as illegal in some contexts and jurisdictions.
- We could (and sometimes do) make fun of extreme Political Correctitude, but in many countries, some forms of un-PC behaviour such as racism and sexism are actually illegal: it's fair enough to remark on such issues in an appropriate context, but you might not want to give the impression that you actually condone it.
- Libel is another legal minefield that should *always* be kept in mind. Remember that writing truthfully is not always enough: sometimes you may have to prove that you're right. It's for this reason that journalists tend to use words like "claim" and "allege" even in contexts that you might think quite uncontentious.
- Respect the copyright and Intellectual property (IP) rights of others (Do As You Would Be Done By)…As Tom Lehrer suggested [7] there is sometimes a fine line between research and plagiarism. We'd like to be able to be able to provide you with authoritative guidelines on what is and isn't "fair use" of someone else's material but better-qualified authors than ourselves have pointed out that there are "no mathematical formulas" for that. [8]. Almost as importantly, respect the IPR of your own company. Respect confidentiality, too: it can be surprising easy to breach a non-disclosure agreement inadvertently, even by an indirect reference to something that isn't in the public domain. Dealings with law enforcement agencies, national security agencies, even past employers, may all have grounds for complaint if you make direct use of privileged information.

There are other sensitive areas, of course: regard for accuracy, professional presentation, conformance with company policies and guidelines, targeting and relevance of topics, and so on. Particular sensitivity is required when responding to material published by competitors. If a competitor is knocking your product and making invalid claims, it's likely that you'll want to address such content, but the risks of bad press, flame wars and even litigation are considerable.

It's likely that as such content continues to move away from "electronic paper" towards more multimedia-based formats, that such issues will become more complex, as well as inspiring questions about secure, portable, bandwidth-friendly formatting.

Blogjammed

Corporate blogs are primarily used, indirectly at least, for promotional purposes (marketing, branding or public relations) [9]. This doesn't mean that they aren't community-oriented, but they are usually required to conform to corporate strategy and protocols, and if they are maintained on company time, to be seen as benefiting and promoting the organization in some way. In fact, while there are many private blogs that have no overt commercial agenda, there are also many that have a community focus but are subsidized by some form of pop-up advertising, so the border between a corporate blog page with discreet static links and a page with multiple sponsors may be fuzzier than you might think.

Corporate blogs (and microblogs, come to that) may, nonetheless, have more than one focus: for example, as a mechanism for distributing press releases. The ESET blog that the authors are most often associated with is multifunctional. While this paper is not intended to be all about us, perhaps we can make some general points about what we consider to be best practice by going into some detail about the way we operate. We don't, of course, claim that our approach is right for all contexts!

A blog published on a corporate website does market the corporate brand, and must therefore present the company in the best possible light, demonstrating core values such as professionalism, expertise, and ethical grounding. Get the content right, and readers will say "Hey, these guys really know their stuff." And, hopefully, there will be a long-term marketing advantage. Get it wrong, though, and the comments will be along the lines of "Those guys know nothing," or "This blog is just advertising fluff," or even "Get me my lawyer!"

Of course, all the legal and quasi-legal strictures mentioned previously in the context of paper writing will also apply to some extent in a blogging context. The Electronic Frontier Foundation have done some very useful work in the context of blogging within the law [10], among other relevant issues: while some of that work is heavily focused on "lone bloggers", we recommend that *any* blogger find time to go through it.

We will certainly include PR material where appropriate (that is, we believe that it will benefit and/or interest our perceived audience). However we don't such material as our primary focus, since regular bloggers on the team are either members of the Research team based in San Diego, or colleagues on other ESET sites working in similar areas. While we work closely with our marketing teams, we believe that gratuitous content that is intended purely to stimulate product sales can actually be counterproductive in terms of attracting traffic – at least in terms of our audience. We aim to produce material that conforms to a number of strict criteria.

Accuracy

As researchers in an industry that demands high ethical standards, we have a responsibility not to compromise on the quality of information we transmit. While we may not have the latitude that an independent researcher has, we consider ourselves fortunate to be allowed to be true to the ethical standards expected of us. Furthermore, as information security professionals, people expect us to know our subject. While no-one knows everything about everything, we consider it necessary to be honest and accurate, to correct errors of fact that *do* creep in, and be upfront and say so when there's a topic we're not best qualified to deal with.

Informational content

As a small team, we can't compete with major media outlets in terms of all-round security coverage, especially as we all have many other jobs to do, though we are considering ways of increasing our coverage of security alerts, for example. What we do try to do is focus on as many of the most important issues around we can and provide useful commentary, rather than simply recycling other content by simply summarizing other people's posts and articles. In fact, it sometimes seems to us that some of the "there's an interesting article at http://xxxx on XYZ" content that characterized many early blogs has largely moved over to micro-blogging sites like Twitter.

This is positive in that micro-blogs have an immediacy and portability that many people find useful, and don't require the high maintenance that a list of links invariably does in a highly dynamic web environment. There is a corresponding drawback, however, in that this very immediacy also means that specific links become more transitory (Twitter is a better place for capturing breaking news than long-life information), and more easily overlooked than a long list of links ordered by topic.

We don't really have time and space here to go into micro-blogging in general and tweeting in particular to the extent it really deserves. However, we recently happened upon [11] an excellent resource from an unlikely source. [12] Neil, Williams, Head of Corporate Digital Channels at the UK government's Department for Business, Innovation and Skills put together a template Twitter strategy document for government departments.

While some of the content is fairly specific to government concerns and the UK in particular, it does provide a well-thought out and comprehensive starting point for considering the implications and strategic thinking behind a corporate micro-blog, and many of those principles will apply to "real" blogs as well. (Indeed, one of the sections included is on leveraging existing web content, including blog posts, while the "Content Principles" section addresses similar principles to those we list here.)

It also follows that somewhat similar "Web 2.0" sites such as Facebook and LinkedIn will also require special consideration and specific guidelines in a corporate context, whether you're in the public or private sector.

Education

While information-sharing is sometimes hard to separate from education, we also see it education as a discrete function. So some topics are, so to speak, less topical and more educational: for instance, ten ways to reduce your exposure to phishing attack, or FAQ-type material. These can be aimed at home users, corporate end users, even system administrators: the amount of hard-core technical content will depend on the issue, the context and the author. The sad fact is that such posts tend not to gain the sort of viral dissemination that hot-off-the-press news items do –though it is also slightly sad to see hundreds of security bloggers chasing the same story in a news media feeding frenzy. Our experience is, though that the inclusion of such material *is* appreciated by a significant proportion of our readers, but that the proportion of such interest is harder to measure than media interest, which can be measured in URLs and column inches. It also constitutes a valuable adjunct to community projects such as those described above.

Professionalism

One of the ways in which professional presentation in documentation can be encouraged is by the introduction of a formal review process. For conference papers and journals, this process is usually part of the acceptance process by the conference or publisher. For blogging, at the other extreme, the need for immediacy often renders a formal review impractical, but for papers, where the deadlines may be more flexible, a formal review is often a useful quality control measure. Even when writing a short, simple email or blog, it's all too easy for the writer to overlook logical, syntactical or grammatical errors that they would have no trouble spotting in someone else's text. With extended documentation, it's even more true that the toughest proofreading tasks, even for a practiced proofreader or editor, centre around reading your own documents, perhaps because you are likelier to "read" what you meant to say rather than the wording you actually used.

It's often useful to implement a peer review to check the accuracy and quality of content, obvious logical and spelling errors and offer suggestions (sensitively) where some improvement in terms of editing (additional or removed content) might be made. Minefields like localization, corporate tone, formatting guidelines, and conformance with authorities such as the Oxford University Press or the Chicago Manual of Style are often better explored by professionals. Experience even with highly respected international publishers suggests, however, that it's all too easy for a copy editor without specialist knowledge of the field to introduce "cosmetic" changes that actually change emphasis or even reverse meaning so as to damage the credibility of the piece, so making changes without actually flagging them is a definite No-No.

Comment Handling

Responding to comments can be as time-consuming as writing the original blog, and requires similar sensitivity. Even those inventive blog spammers who manage to circumvent "blam" filters can impose a significant time-penalty where the blogger is forced to spend time deciding whether or not to approve their comments. We are unsurprised and sympathetic to those bloggers who decide not to support commenting, though by doing so they miss out on a seriously useful feedback mechanism which may provide fruitful discussion and even generate further blogs (though we tend to find that finding *time* to blog is much more of a challenge than finding *topics* on which to blog).

Conclusion

We have both worked in one sector or another of the anti-malware research community for many years, and remember with occasional regret the days when mainstream vendors were community-oriented enough to include links on their own informational web sites to those of other vendors, so that if you couldn't find the information you needed on a specific threat at one site, it was easy to check another. Inevitably, the need to maintain marketing advantage by keeping potential customers on your site for as long as possible has overridden that particular practice, though perhaps the plethora of community-oriented projects, some of which we described above, is sufficient compensation for that.

We do regret that it seems to be less common to give credit to other papers, bloggers and other resources where it's due: we understand that it's not always advantageous to the company to provide links and references to competitors, but such meanspiritedness can disadvantage the end-user or customer as well as the competitor, and we try not to fall into that trap. Of course, formal papers, articles and chapters encourage the copious use of attributed references (indeed, some publishers actually specify a minimum number of references to be included with book

chapters), but more overtly commercially-oriented papers are not always as scrupulous. We are reminded of some books where the author and publisher either assume that you will learn everything you will ever need to know from that book and give no further resources or references at all, or else have an explicit policy of only referencing works from that specific publishing house.

However, we consider ourselves privileged to be able to share the benefit of our prejudices with others, and strive to do so in an ethical, informative but entertaining fashion, and hope that “newercomers” to document provision and the blogosphere will find our observations useful.

References

[1] Virus Bulletin; http://www.virusbtn.com

[2] Anti-Virus Information Exchange Organization; http://www.avien.org; AVIEN Malware Defense Guide for the Enterprise; http://www.smallblue-greenworld.co.uk/Avien.html

[3] The WildList Organization International; http://www.wildlist.org

[4] David Harley & Andrew Lee: "Antimalware Evaluation and Testing", in The AVIEN Malware Defense Guide for the Enterprise, ed. Harley, Syngress 2007; http://www.smallblue-greenworld.co.uk/Avien.html

[5] Securing Our eCity; http://securingourecity.com/

[6] Sentencing Advisory Panel: The Panel's Advice To The Court Of Appeal On Offences Involving Child Pornography, 2002**;** http://www.sentencing-guidelines.gov.uk/docs/advice_child_porn.pdf

[7] Tom Lehrer: Lobachevsky, from the LP "Songs by Tom Lehrer"; see http://en.wikipedia.org/wiki/Songs_by_Tom_Lehrer

[8] Lloyd J. Jassin & Steven C. Schechter: The Copyright Permission and Libel Handbook, Wiley, 1998

[9] Wikipedia; http://en.wikipedia.org/wiki/Blog

[10] Electronic Frontier Foundation: Legal Guide for Bloggers; http://www.eff.org/issues/bloggers/legal

[11] David Harley: Twitter and the Corridors of Power; http://www.eset.com/threat-center/blog/2009/08/07/twitter-and-the-corridors-of-power

[12] Neil Williams: Template Twitter strategy for Government Departments; http://blogs.cabinetoffice.gov.uk/digitalengagement/post/2009/07/21/Template-Twitter-strategy-for-Government-Departments.aspx