MICROSOFT ANTI-VIRUS – EXTORTION, EXPEDIENCE OR THE EXTINCTION OF THE AV INDUSTRY?
Randy Abrams
ESET LLC, USA

Email abrams@eset.com

The views and opinions presented are strictly those of the author and do not reflect the views and opinions of his employer or Virus Bulletin.

ABSTRACT
In 1993 Microsoft released MSDOS 6.0, which included Microsoft Anti-Virus, a re-branded and ill-conceived entry into the anti-virus industry. In 2003 Microsoft announced the acquisition of RAV anti-virus, and in late 2004 the acquisition of Giant anti-spyware.

From 2003 it was obvious that Microsoft would become a player in the anti-virus industry at some level. Many comments were made at the time about Microsoft’s previous debacle in the industry, and of course diehard Micro-haters cite this as a predication of the quality of the new product.

Having worked with Microsoft security professionals for several years, as well as with the developers of RAV for a couple of years prior to the acquisition, I have my own views as to the predicted performance of the offering.

This paper will take a look at the product that was acquired, the changes in the corporate culture at Microsoft between 1993 and today, and the effect on the product Microsoft is bringing to market. I left Microsoft in June 2005 to join ESET, an anti-virus company. Should I be concerned about the longevity of my job? What about the diversity of choices of anti-virus software available today – will there be any left? Will the new Microsoft product leave users in worse, or very little better, shape than they were before, as the old MSAV arguably did?

INTRODUCTION
In March 1993 Microsoft released MSDOS® 6.0, which included utilities that had not previously been included in the operating system, one of which was Microsoft Anti-Virus (MSAV). MSAV was a stripped down version of Central Point Anti-Virus, arguably a weak performer in the young anti-virus field.

In April 1993 Microsoft hired Randy Abrams, who promptly replaced MSAV internally with an anti-virus product suitable for use on the PCs in the duplication facility. The most significant problems with MSAV were that Microsoft licensed the product and so was apparently unable to improve it, and that it was very difficult to find out how to update the signatures. To add insult to injury, no significant effort was made on the part of Microsoft to teach users that updates were required.

As was easy to predict, MSAV quickly became a favourite target for virus writers, and several viruses attacked users of the product successfully. Although I am not in possession of any statistical information, anecdotally I have been told that there was a short-term impact on the sales of anti-virus software.

Today, Microsoft is back in the anti-virus space. Any person who believes that the new offering from Microsoft will be of the same quality as MSAV from DOS 6 is advised to leave the room now in order to acquire an aluminum (or aluminium) foil hat. The foil hat may not help, but such people are bound to believe it does!

There is one interesting parallel between the old MSAV and the new product offering; both are ‘bundled’ as utilities. MSAV was not available as a product separate from DOS 6, and as of this writing, the new Microsoft anti-virus is available only as a suite – called Windows Live OneCare – which includes anti-virus, anti-spyware, a firewall, backup, hard disk defragmentation, and also offers removal of ‘unnecessary files that can clog your PC’.

EXTORTION
Before continuing with my opinions of the product and predictions for the future, I would like to present the reason for the question ‘Is MSAV extortion?’, and the answer.

When Microsoft announced plans for a consumer anti-virus offering, some people – with an obvious and disingenuous agenda – labelled the offering ‘extortion’. To answer the question of whether MSAV is extortion we need a functional definition of the word. Fortunately, several resources are available to help us with this task. Looking back in history the definition has not changed significantly, so those who do not know what extortion is simply lack some education. In 1913 the Webster’s dictionary gave the following definition [1]:

Extortion
1. The act of extorting; the act or practice of wresting anything from a person by force, by threats, or by any undue exercise of power; undue exaction; overcharge.
2. (Law) The offense committed by an officer who corruptly claims and takes, as his fee, money, or other thing of value, that is not due, or more than is due, or before it is due.

Law.com offers the following definition:

Extortion
n. obtaining money or property by threat to a victim’s property or loved ones, intimidation, or false claim of a right (such as pretending to be an IRS agent). It is a felony in all states, except that a direct threat to harm the victim is usually treated as the crime of robbery. Blackmail is a form of extortion in which the threat is to expose embarrassing, damaging information to family, friends or the public.

Given the two primary definitions of extortion, we need to consider two questions:
1. Is Microsoft exacting payment from customers by threatening harm?
2. Is Microsoft overcharging?

The answer to the first question, ‘Is Microsoft exacting payment from customers by threatening harm?’ is obviously ‘no’. Microsoft does not deliberately create security vulnerabilities to sell security software. Microsoft is not threatening to write viruses. There probably are very naïve or unduly paranoid people in the world who believe otherwise, but the obvious truth is no, Microsoft does not engage in such practices.
Is Microsoft overcharging for Windows Live OneCare? At just less than US$50 for coverage of three computers, Microsoft is charging less for the OneCare suite than most vendors have been charging for standalone anti-virus solutions. When the entire suite of OneCare is considered it is obvious that Microsoft is not overcharging.

The only logical and honest answer to the question ‘Is Microsoft Anti-Virus extortion?’ is ‘no’. It is extremely disappointing that some otherwise credible reporters have abandoned journalistic integrity, adopted a self-serving agenda, and stooped well below sub-tabloid standards in referring to Microsoft’s re-entry into the anti-virus arena as ‘extortion’.

EXPEDIENCE

The second part of the topic involves the question of expedience. Is it expedient for Microsoft to provide anti-virus protection? That depends on whether we are talking about Microsoft, the anti-virus industry, or the users.

For Microsoft, this is probably an expedient move. There is a high likelihood of financial success from the endeavour and there is a significant chance that some users who do not already use anti-virus software will start to use it. It is unclear how large this number of users will be.

For the anti-virus industry, the expedience will probably depend upon the individual companies, with smaller companies potentially enjoying more success. Large companies, such as Symantec, McAfee, Trend Micro and CA will probably lose some market share to Microsoft. Initially the loss will be in the consumer and small business space, but when Microsoft Forefront comes to market, medium and large businesses are likely to be adopters at some level as well.

As far as the expedience for users goes, it is too early to provide a definitive answer. The long-term answer will depend on how well Microsoft anti-virus is able to help protect its customers. This speaks directly to the quality of both the product and technical support.

With the original MSAV, customer service was almost unheard of. This is not a situation that Microsoft is likely to repeat. Microsoft has been offering free anti-virus support for several years now, through 1-800-PCSAFETY, and has been building expertise in the field. Microsoft’s product support, once loathed, has made tremendous strides and is now garnering predominantly favourable feedback from consumers who use it. Technical account managers are largely very respected by the organizations they support as well. Quality service has been a serious goal of the corporation and its employees for several years.

As for the quality of the product, as of this writing it is not looking particularly good for OneCare users. Despite Windows Defender having been a released product (Giant Anti-Spyware), and after being acquired spending a couple of years in beta, anti-spyware is not installed by default in OneCare and has no Checkmark certification for spyware detection. Several anti-virus companies were able to integrate spyware detection into their product and achieve spyware detection certification much more quickly than this.

On 16 June 2006, a zero-day vulnerability in Excel was disclosed. On 18 June, OneCare was unable to detect one of two exploit samples where seven other anti-virus companies were already protecting their users.

Still, I do expect the quality of Microsoft’s offering to improve. To understand why I expect the quality of the product and support to be competitive it is useful to have a glimpse into the Microsoft ‘psyche’. Having worked at Microsoft for over a dozen years, I feel qualified to help provide some insight.

John Thompson, CEO of Symantec (apparently a Larry Ellison wannabe) was quoted by ZDNet in May 2006 as saying: ‘Our strategy is to out-innovate Microsoft. We know more about security than they ever will.’ [2]

I have news for Mr Thompson: Symantec doesn’t know anything about security – in fact, no company does. A company is a legal entity and it is the people who hold the knowledge. Microsoft has people who are every bit the equals of security experts in any other company.

The strategy of Symantec out-innovating Microsoft does not appear to be rooted in Symantec’s corporate history. Symantec has not yet been able to keep pace with the technical innovations of small companies like ESET, Norman and BitDefender.

Perhaps I misinterpreted the word ‘innovate’, though. Symantec bought Norton anti-virus and the IBM ‘Digital Immune System’. Symantec bought IMLogic to protect IM systems. Symantec bought Sygate and Safeweb, and a host of other companies. Microsoft is well versed in acquisitions as well. Despite the ability to buy technology there has been no demonstrable ability for either Microsoft or Symantec to detect malicious software proactively at any significant rate. The prevention, rather than clean up, of infections is where innovation is most sorely needed.

It is the people at Microsoft who will determine the quality of the product and the support. Microsoft Corporation employs in excess of 50,000 employees. Like any large corporation, Microsoft has some bad apples, but the vast majority of employees are smart, hard-working individuals who take pride in their work. Most employees are front-line product support for their friends and families. It is embarrassing to these people when there are problems with Microsoft products. Microsoft employees generally are very passionate about the work they do. The love of technology has resulted in some really cool, but insecure products in the past, but with security at the forefront now – especially being forced down marketing’s proverbial throat – these people are working on developing new technologies with security in mind.

Obviously there have been numerous problems with the security of Microsoft’s products in the past, however it is doubtful that many, if any, other products could withstand the scrutiny that Microsoft products receive and come out faring any better while providing anything close to comparable functionality and ease of use.

Microsoft nurtures a tremendous culture that encourages respectful disagreement. Within the company there are a myriad of mailing lists that deal with a variety of topics. One such mailing list that deals with information for testers is virtually an online classroom and support centre. Even though my job title and background were not in testing (at least not formally), I joined the testing information mailing list. The sharing of information on that list enhanced the knowledge of all who participated.

This type of knowledge sharing is a huge and valuable resource for Microsoft and results in improved product and
employee productivity. One need not be a tester to participate in the list and people from a variety of job functions make meaningful contributions to the list.

A different list dealing with product security and privacy issues in general is not only a source of information and education, but a lively forum where many diverse viewpoints and opinions on these issues are argued.

Veheement disagreement with Microsoft policies and plans were, and I suspect still are, commonplace on this list. Anyone who has participated on this list must understand how far the Microsoft environment is from an ideological monoculture. Microsoft's executive management is intelligent enough to understand that disagreement with policies and decision is not disloyal, rather it demonstrates passion and genuine caring. Microsoft's management is also smart enough to know it is better to be aware of what people think than to participate in stifling dissent.

Once, while working at Microsoft, I obtained potential vulnerability information that I passed along to the Microsoft Security Response Center (MSRC). The reply I received stated that the issue was not a vulnerability. Convinced that it was, I provided arguments and a harmless example of the problem to demonstrate my reasoning. After ensuing discussions, internal to the MSRC, it was decided that the issues did either constitute a vulnerability or at least a problem that required resolution. The problem was later fixed. I was not a tester, a programmer, a member of a security team, or in any position of authority. Security response was not my job. At no time (that I am aware of) was I criticized for intruding into someone else’s job, nor were my views and opinions dismissed as irrelevant due to my background or job duties.

The fact that people at Microsoft are willing to accept information and diverse views, generally very openly, is a huge benefit to the company. Microsoft employees are encouraged to contribute their skills, knowledge and opinions on any issue they feel passionate about. Companies who do not actively foster this type of environment waste valuable resources and put themselves at a serious competitive disadvantage to Microsoft.

For those interested in another employee’s insight into what it is like to work at Microsoft, I would refer them to [3].

The combination of the work environment, the dedication of employees, and the hiring of experienced anti-virus professionals leave me with no doubt that Microsoft will be a serious contender based upon the merits of its product.

After Microsoft announced that it had acquired GeCad RAV, Nick FitzGerald posted thoughts about the acquisition on alt.comp.virus. In June 2003, when discussing why Microsoft had made this decision, Nick posted:

‘Having a steady supply of users connecting to the Redmond mother ship every day for what has come (due to the AV industry’s “success”) to be seen as “needed updates” may boost either or both of MS’s desires for pushing more patches to more users (who may normally be rather hesitant, if not outright resistant to visit WindowsUpdate) and/or as the “natural” means to start a “paid for updates” service. Not only has the AV industry enjoyed unparalleled access to its users’ computers to install updates almost unquestioned, _but_ its users enjoy this so much they _pay_ for the “privilege”.

‘MS has never come close to this level or form of user “dedication”, and may now see this as the route forward for increasing “revenue opportunities”.’

I was not involved in the decision-making process to acquire RAV, but having had discussions with people who were involved, at some level, I believe that Nick is partially on the right track. In a paper by Matthew Braverman entitled ‘Win32/Blaster: a case study from Microsoft’s perspective’ and presented at VB2005 [4], it was reported that more than five months after the Blaster worm had appeared the Windows Blaster Worm Removal Tool cleaned millions of infected computers. Later in Matthew Braverman’s paper it is revealed that, within six months, over 12 million computers were disinfected.

Microsoft realizes that the exploitation of security problems, as well as malware infections that only rely upon user ignorance and gullibility, are harming the Windows brand. By attracting users to Windows Update, and by getting users to run anti-virus software, Microsoft will improve the security of its users. This will help Microsoft protect the Windows brand. The corporate focus on protecting the Windows brand is another reason why I expect both product support and the product itself to be of good quality. From the human side, the testers, developers, and support professionals at Microsoft do sincerely want to help people be more secure. I do not believe that the revenue potential will go unexploited, and I do not believe this was a primary factor in the decision to provide a Microsoft solution.

After the Microsoft Blaster Removal tool, Microsoft released the Microsoft Malicious Software Removal tool. Some statistics around the success of the latter were presented by Jason Garms at the AVAR 2005 conference in Tianjin, China [5]. The billions of executions to date, coupled with a very low incidence of problems with the tool bode well for Microsoft, however it must be noted that there are considerable differences between a fully-fledged anti-virus product and a monthly tool that addresses a small part of the problem. Still, one must recognize the capability of Microsoft engineers to produce a robust security tool.

It would appear from empirical evidence that Windows Live OneCare will be expedient for some users. The major caveat would be that if a user selects Windows Live OneCare over discrete security products providing better protection, the specific user’s security profile will be degraded. For those using inferior products, or none at all, OneCare is good news. Obviously a big part of the quality of the offering is the technology. As Nick FitzGerald noted, Microsoft acquired some ‘pretty good’ anti-virus software. While RAV posted a cumulative record six VB 100% awards out of 25 attempts, it should be noted that RAV achieved VB 100% awards in four of its last six tests and one of the failures was on the Linux
OS. RAV was a product with an increasing level of quality and very bright developers. Several of these developers came to Microsoft in the acquisition of RAV. Unlike the days of DOS 6, Microsoft has a significant and competent test and development team working on the anti-virus product.

Microsoft invests billions of dollars each year in its research department. The funding is for pure research, much like Park Xerox used to do. I would expect that some of the ideas coming from Microsoft research will eventually add significant heuristic capabilities to the product; however that is far from guaranteed. Companies such as McAfee and Symantec have significantly greater resources, but have been unable to approach the heuristic capabilities of NOD32 – the product of ESET, a small Slovakian company – or Norman Virus Control from Norwegian company Norman, or BitDefender from Romanian company SOFTWIN.

EXTINCTION OF THE AV INDUSTRY?

So, given that Microsoft is not extorting users, and will very likely have a very competitive product soon if not already, what does this mean to the anti-virus industry? Will we see another IE vs. Netscape scenario? Leave it to Nick FitzGerald to provide some prescient insight into this topic in the same 2003 alt.comp.virus post.

‘And does MS really think it can (in the short term) take over enough of the AV industry to dominate? Remember, in the “browser wars” against Netscape, it was really two__emerging__products fighting not only for market share but to shape the vision and direction of what that market was. Here we have MS swallowing up a small player in a very well-established sub-industry niche – quite a different kettle of fish if you ask me...’

Before this alt.comp.virus thread ZDNet ran an interview with Bill Gates [6], in which David Coursey reported the following:

‘When asked why Microsoft isn’t in the anti-virus business and more heavily into desktop security, to my surprise Gates just sort of smiled and said some issues remain to be resolved. I think companies in those spaces should consider that a warning.’

In an email to a private mailing list (quoted with permission) Jimmy Kuo addressed the notion of the warning with the following quip:

‘I’ll consider it a warning when MS actually does it. Because that’ll be two tries. And MS succeeds on its third try. :-?’

Perhaps Windows Defender or the Microsoft Malicious Software Removal Tool represents the second try. I believe that OneCare will make a significant impact in the anti-virus industry, but predominantly for the largest players.

To quote yet more of Nick FitzGerald’s alt.com.virus post from 2003:

‘...there’s the existing, very well-established “should I use McAfee or Norton?” mindset in that market sector.’

Unlike Nick, I believe that the McAfee and Norton consumer market is where Microsoft will have a very significant impact. With no disrespect intended to the large players in the industry, I do believe that most of the consumers buying these products do so primarily due to name recognition and marketing. These people generally have neither the skills, nor often the desire, to truly evaluate anti-virus software.

Microsoft carries tremendous name recognition and a world-class marketing organization. It may take some time, but I would expect the detection capabilities of Microsoft’s offering eventually to match Symantec, and there is significant potential for better heuristics. If the incredibly slow nature of Symantec’s anti-virus offering is key to its market dominance then Microsoft will be unbeatable – in Virus Bulletin testing, OneCare is making Symantec look fast! McAfee and Trend Micro will also face a competitor who is their equal or better in marketing prowess and a product that is, or will be, their equal or potentially better as well.

Of course, the companies with the largest market share have the most market share to lose. However, I believe the largest companies will lose a disproportionately high share of consumers initially. I think the smaller companies will see a significantly lower rate of loss of market share. Small companies like ESET, and several others, have customers who already know the names of McAfee, Symantec and Trend Micro. These customers have already been exposed to the marketing machines of these companies, and yet have made a conscious decision to choose the products they use for reasons that clearly extend beyond name recognition. In general, ESET’s customers care about system resource consumption and proactive detection. Microsoft’s offering includes separate engines for anti-virus and anti-spyware and then adds other components. No data, as of this writing, indicates any significant level of heuristics in the Microsoft offering and the scanner is considerably slower than most other anti-virus products.

The one reason why Microsoft may have success in luring customers from smaller companies is the convenience factor of the backup and performance portions of OneCare. This may not prove to be as enticing as it may look at first glance. For customers choosing solutions based upon technology it is reasonable to assume that a significant percentage of these customers also have a favourite backup solution and/or performance product. OneCare will not appeal to the ‘best-of-breed’ buyer in the foreseeable future.

Microsoft will have obstacles to overcome if it is to obtain and maintain significant market share. Not the least of these factors is a hostile media. When a Microsoft product has a fairly low risk vulnerability, the press reports this to a far greater extent than when any other company’s products have more significant problems. Anything negative with Microsoft’s name in the headlines is seen as a marketing opportunity for many media companies. I’m betting it is effective in bringing attendees to a presentation too! A virus that disables Microsoft Anti-Virus as well as a dozen other anti-virus products will be presented as attacking Microsoft. While the negative treatment of Microsoft by the media may be disproportionate, often inaccurate, and unfair, it does happen and it will have some impact on MS.

Microsoft Anti-Virus will be the target of most all of the virus writers. In the past this may have diverted some attacks away from other vendors, but the evolution of malware toward organized crime simply means that Microsoft will be an additional target. It is unlikely that any other vendors will see any reduction in attacks against their products with Microsoft.

Microsoft has a significant and competent test and development team working on the anti-virus product.
entering the field. Having said that, it is still likely that the fewer, but still active, non-profit malware writers will target MSAV specifically for fun or out of spite, and most other vendors will be ignored. The result will be a marginally higher attack rate against Microsoft.

In the past, it was other vendors’ anti-virus products that failed to prevent Windows from becoming infected. The fact that Microsoft’s anti-virus offering will, at times, fail means that it will be Microsoft who failed to protect Windows. I believe that after some market gain by Microsoft, failure to protect its own operating system will eventually cause many users to turn to other anti-virus solutions, restoring some lost market share for other companies. The fact that other companies’ products fail, at times, to protect the Microsoft operating systems will generally not be viewed as harshly as when OneCare fails, regardless of which product does better overall.

The most obvious hurdle and perhaps the largest for Microsoft is the perception of not understanding security. Regardless of truth or fairness of this perception, it will slow the rate of adoption of OneCare and will prevent many from ever adopting the Microsoft offering.

One of the concerns I have heard in the anti-virus industry is how Microsoft being a competitor is going to affect the sharing of information. In 1997 Microsoft was exceptionally bad at sharing information that would help the anti-virus industry protect Microsoft users. Over time, Microsoft became better at sharing information. A handful of people at Microsoft worked very hard to make this happen. The group at Microsoft that is responsible for sharing information with the industry is now the group responsible for the security product offerings – an apparent conflict of interest.

Interestingly, this unholy alliance may potentially result in better information sharing than if the duties were separated. Any information that the Microsoft anti-virus product group has about Microsoft software will probably have to be shared in order to prevent legal problems. Because Microsoft is now producing anti-virus software, there will be people in Microsoft requiring the same information that the rest of the anti-virus industry needs. I do not see the competitive aspect as a reason for information sharing to be diminished.

If less information is shared I would expect it to be due to the lack of industry experience of the anti-virus product management at Microsoft. Few people at Microsoft have any significant experience working with the anti-virus industry. I also believe that experienced researchers, such as Adrian Marinescu, have the stature and integrity to insist that Microsoft play fairly with the rest of the industry.

The better Microsoft’s competitors are at protecting Windows users, the stronger the Windows brand will be. This should be exceptionally strong motivation for Microsoft to help the industry as much as possible. A possible problem in acting on this self-serving, but useful motivation is a review system that probably does not take this aspect of the business into consideration.

The absolute numbers of users signed up for OneCare will probably be the review criteria for employees and the absolute good done for the Windows brand name will probably not carry any weight at employee review time. If Microsoft can figure out how to address this potential problem the industry stands to benefit from increasingly better information sharing.

If Microsoft is unable to reward performance that leads to a stronger Windows brand then the industry will struggle for critical information and OneCare will prove to be counterproductive to Microsoft and its customers.

One of the issues I have with Microsoft’s entry into the anti-virus/anti-spyware arena is the blatant corporate hypocrisy of the corporation’s pro-spam and anti-privacy position.

On the surface, Bill Gates and the Microsoft public voice claim to be fighting against spam. The truth is that Microsoft, as a corporation, has supported legislation that allows spam to be sent to users who do not opt out, as opposed to the respectful approach of opt in. Anti-malware professionals know that, increasingly, spam is used to carry malware. The notion that one should opt out of spam is inconsistent with respect for privacy, and flies in the face of intelligent security measures. I would expect that if a survey was conducted amongst Microsoft employees the vast majority would prefer opt-in legislation in the US, yet Microsoft Corporation has completely ignored anything related to decency in its approach to this issue.

I doubt this will have any significant effect on US sales, but I would hope that in other parts of the world, where laws are more supportive of privacy than those in the US, it will be detrimental to sales. It is irresponsible for Microsoft to support a position that requires consumers to validate their email address for spammers in order to try to be removed from a spam list. Microsoft’s opt-out position contributes to the spam problem, and hence to the spread of malware. There is little wonder why the US is one of the biggest spam producers – companies such as Microsoft have openly supported legislation to exacerbate the problem.

The final obstacle for Microsoft is its track record. Microsoft anti-virus does not have any significant track record and Microsoft Defender® has not achieved any certification for spyware detection as of this writing.

The competition has established track records. Many other companies have long histories of consistent certification by the ICSA, Checkmark, and Virus Bulletin. NOD32 is certified by Checkmark Labs, ICSA, and has achieved the Virus Bulletin VB 100% award more times than any other product. NOD32 has been tested by AV-Test.org and AV-Comparatives.org and has consistently been found to have exceptionally better proactive detection than any other product, including products developed by companies, such as Microsoft, with large research and development budgets.

There is a simple measure for Microsoft if they care to try to compete on the technical merits of their product. ESET has set the bar for quality, it remains to be seen how high Microsoft can jump.

REFERENCES
