Might Governments Clean-up Malware?

Richard Clayton
Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, UK.
richard.clayton@cl.cam.ac.uk

Abstract

End-user computers that have become infected with malware are a danger to their owners and to the Internet as a whole. Effective action to clean-up these computers would be extremely desirable, yet the incentives conspire to dissuade ISPs (and others) from acting. This paper proposes a role for government in subsidising the cost of clean-up. The organisations that tender for the government contract will factor in not only the costs of the clean-up, but also the profits they can make from their new consumer relationships. A model is proposed for what the tender price should be – and, by plugging in plausible values, it is shown that the cost to the tax payer of a government scheme could be less than a dollar per person per year; well in line with other public health initiatives.

1 Introduction

This paper looks at the problem of dealing with end-user computers that have, in a variety of ways, become infected with malware. This can sometimes be a serious security issue for the owner of the computer in that malware is often capable of copying confidential files, stealing online banking credentials, or of fraudulently redirecting traffic for financial gain [15]. Additionally, it is almost invariably a security issue for the rest of the Internet, because the infected computer can be combined with others into a 'botnet' which is then used for a large range of criminal activity, from distributed denial of service attacks, through click fraud, to the bulk sending of email spam [13].

Quite clearly, for the Internet to be safer for everyone, 'something must be done' to clean-up the infected computers, but there are a number of barriers to this – mainly to do with incentives. Since the incremental effect is small, no-one may be interested in collating lists of botnet members and submitting reports to ISP 'abuse' desks. The ISPs, who must be involved to map IP addresses to customer identities, gain little from handling the reports. They risk alienating customers by simultaneously threatening disconnection and refusing to provide free technical help to deal with the problem. If the report does reach the customer they may not appreciate the need to act and, indeed if the malware does not steal data from them, inaction makes little difference to their Internet experience. Furthermore, removal of malware costs time and/or money that the end-user may feel that they can put to rather better use.

May 21, 2010

The cost of cleaning up malware is obviously a key issue – and the perception of it being a complex task, with expert help expensive and essential, goes a long way to explaining why customers delay malware removal and why ISPs are generally so reluctant to offer assistance. Of course some malware is trivial to remove, but effective clean-up may be difficult, it may need specialist knowledge, and hence it can indeed be rather costly.

This paper suggests that there might be a role here for governments to step in and subsidise the clean-up – with the analogy being with their role in protecting public health. We believe that such a subsidy will go a long way towards improving the incentive issues – it will no longer be quite such an expensive nuisance for an ISP, or their customer, to learn of a malware problem. Furthermore, by reducing the cost of clean-up to the end-user, it would also make it fairer (and more politically acceptable) to introduce regulations to compel ISPs and customers to ensure that malware is removed in a timely manner.

Clearly, by bulk purchase of clean-up services through a tendering system, a government will be able to reduce the cost of their subsidy. Additionally, since the suppliers should be able to sell further products (anti-virus software would be an obvious example), they should be treating the referrals as a valuable 'sales lead', and tendering lower for the contract as a result. Hence, we argue in this paper, tax-payers will end up with a rather smaller bill than might initially have been expected.

Lest it be thought that this proposal is completely speculative, the Luxembourg Ministry of Economics is currently evaluating a policy initiative, based on an early version of this paper, to operate a state-subsidised malware cleaning scheme. If they decide to go ahead and the scheme is successful, then this would make a compelling case for rolling out similar initiatives in other countries – with a consequent improvement of Internet security for all.

The rest of the paper is arranged as follows. In Section 2 we discuss the nature of malware in more detail, and outline existing initiatives for malware removal. In Section 3 we set out how a government sponsored scheme would work, and in Section 4 we model the costs and set out the basis for our belief that it will not be as expensive as it might initially seem; and then in Section 5 we conclude.

2 Malware

One of the most important ways that criminals make use of the Internet is by employing malware (malicious software). Ordinary consumers are tricked into running these programs on their computers, and the malware will compromise online banking sessions, steal passwords for email accounts so they can be exploited for sending spam; and almost invariably cause the computer to join a 'botnet'. The botnet is the 'swiss army knife' of Internet wickedness, allowing criminals to command the individual botnet members to send email spam, participate in advertising 'click fraud', take part in denial of service attacks, or assist in hosting illegal web content.

It was once useful to distinguish different types of malware: 'worms' were self-replicating programs that spread from computer to computer without user intervention; 'viruses' attach themselves to genuine programs or emails, and run only when the user requests this; and a 'trojan' was a program that claimed to do something useful and secretly did something wicked.

These days, these distinctions are of limited value – and the categories have blurred considerably. The main vector of infection at present is visiting websites which contain malware, either because they have been specifically constructed that way, or because they were insecure and someone has broken in to plant the malware.

2.1 Malware infection

The user will become infected either because they deliberately install software from the website (they may be persuaded that a video will not play because their system needs to have extra components installed) [17], or the site will just automatically download content that exploits flaws in system components such as media players (so-called 'drive by' infection [16]).

Users can improve their protection against malware by keeping the programs on their computer up-to-date and by never installing software from untrustworthy sites. It is also useful to run anti-virus software, with a current list of threats to scan for; although technical advances by the malware writers mean that a great deal of malware now completely fails to be detected by these programs. Using a firewall, or as most consumers will, connecting to the Internet via a network address translation (NAT) device, has value in protecting against 'worms', albeit these are an unusual type of threat nowadays.

Even with a totally secure and up-to-date system, and impeccable online behaviour, consumers can still become infected with malware through no real fault of their own; perhaps by visiting a reputable site that has been recently compromised, having their browser automatically download malicious content, and thereby falling victim to a '0-day exploit', for which no countermeasure yet exists.

2.2 Malware detection

Consumers become aware that their computer is infected with malware in two main ways. The first is by running a detector on their computer; the second is by being told of the problem by someone else who has noticed that their computer is behaving inappropriately.

It is often the case that newer versions of anti-virus software will detect malware that has been present on a computer for some time. If a particular malware program is widespread enough, the anti-virus vendors will ensure that their products are able to detect and remove it. However, malware will often arrange for anti-virus updating to fail, so that the anti-virus software continues to run with outdated information of what is to be detected. The user will therefore have a false sense of security – and will continue to operate a compromised computer.

The other major system for malware detection is Microsoft's monthly 'Windows Update' arrangements, into which is incorporated their 'Malicious Software Removal Tool' (MSRT).[1] Microsoft will take steps to detect and deal with malware if it is especially widespread, and/or when there is particular disruption being caused by the botnets that the malware makes possible.

When the user does not themselves notice that their computer is infected with malware, this may come to light because the bad things which it is doing are detected elsewhere on the Internet. Occasionally a researcher will be able to enumerate all members of a botnet, or a spam email may be sent to a special 'trap' address which is unused, so that any incoming email must be unsolicited. Whatever the mechanism, the report will be made to the user's ISP, who is then expected to deal with their customer.

The reason that reports have to be made to the ISP is that for consumers and small businesses there is no publicly available directory to map the IP address of the misbehaving computer into a contact address for its owner. Provided that the correct technical details are given to the ISP, it can use its own private records to work out which customer is causing the problem, and can then communicate with that customer. By convention [6], the email address used to reach the ISP is `abuse@ispdomain` and the personnel who deal with this mailbox are called the ISP abuse team.

2.3 Malware removal

Once the user is aware that they have malware on their computer then they should always wish to remove it, and if well-enough informed they will generally do so. This is not only because they want to be good Internet-citizens, but also for self-protection – because so much malware has keylogger functionality, important information, such as online banking credentials, is at risk. Once the user has removed the malware, they must then immediately change all of their passwords (and indeed their password recovery questions as well, to prevent the criminals changing the password straight back).

Some malware is relatively easy to remove – the Microsoft MSRT program is very effective for the malware it targets; and anti-virus companies provide removal software as well as detection software. However, where a custom removal tool is not available, then generic techniques will be needed, and these can be extremely complicated.

To remove malware, the basic steps are to find all running copies of the program and stop them; remove all system start-up instructions that would cause the malware to run at the next reboot; and delete all copies of the malware on the computer's disk, perhaps disentangling it from legitimate files to which it has become attached. Once the malware is gone, the computer may need to be reconfigured because the malware may have disabled the anti-virus system or messed with the firewall settings. In extreme cases it can be simpler to reinstall the entire operating system from scratch, and indeed to avoid lingering problems the super-cautious will do this as a matter of course.

[1] `http://www.microsoft.com/security/malwareremove/`

2.4 The economics of dealing with malware

Because malware can be so difficult for consumers to deal with, they will look for help in cleaning up their computers. The main sources of such help are friends and family (amongst whom may be a technically skilled person); computer shops, especially the one from which they bought their computer; and their ISP.

Customers tend to have a strong expectation that their ISP will help them deal with problems whose origin was on the Internet; especially if it was their ISP who relayed the report that they had a malware problem in the first place.

However, ISPs are not usually set up to do generic technical support, and because their support is offered over the phone and by email, removing malware is especially difficult for them. Therefore, their response to customers is either to point at 'how to' documents on the Internet, or to suggest contacting the shop where they bought their computer. This can leave customers upset, and they may erroneously conclude that if their ISP does not seem to care whether they remove the malware, then they need not care either.

ISPs are not just extremely reluctant to offer technical support in dealing with malware, but they may be reluctant to handle incoming malware reports either. The provision of Internet access to consumers has become a commodity, and ISPs find it essential to compete on price. To keep prices low, they have to eliminate costs from their organisations, and one of the areas where it is very tempting to attempt to save money is within the abuse team. Processing incoming reports, determining which customer is involved and then talking to that customer is expensive – it is often claimed that communicating with a customer just once eats up the profits on that customer for the year. [2]

In principle, the market should deal with ISPs who skimp on abuse team activity. Their customers will be added to third party blacklists. As the number of entries grows, those blacklists will add larger and larger blocks of the ISP's address space. Because these blacklists are used by many spam blocking systems, this will impact the ability of the rest of the ISP's customers to

[2] The cost of communicating with customers is widely claimed to be comparable with the annual profit they generate, but substantiating this figure turns out to be difficult. The Help Desk Institute (HDI), a membership/certification organisation for technical support professionals, hosts a 2003 white paper [19] which discusses the complexities of determining what the cost of a call might be, concluding "Industry average for cost per call (fully burdened) within the help desk industry is $20–$40." It might be thought that this could be on the low side for calls relating to malware, and of course costs may have risen, some 7 years later.

For the other part of the equation, profit per ISP customer is hard to assess since many major ISPs also bundle television or telephone services, or provide dial-up services (where the cost base is different from broadband). Earthlink's 2010 Q1 figures [7] show a net profit of 25.7 million USD, and that broadband revenue was 59% of their revenue. Assuming (and it is an assumption) that broadband has the same profit margin as dialup then their 900 000 customers provide a profit per annum of 67 USD per customer.

As another data point, McPherson, in a detailed 2007 blog post [12] on just this issue – the cost to ISPs in communicating with customers about botnet membership – estimated the profit per annum to be 60 USD and the cost of a support call to be 50 USD.

This evidence shows that the "profits for a year" claim is excessive, albeit not greatly so.

have their email delivered, and the general impression of uncleanliness may reduce the amount of free peering that the ISP can negotiate.

However, the impact of these measures is relatively small, the process slow, and there is a considerable asymmetry to them – a large ISP suffers little loss from blocking a small ISP, whereas the small ISP would lose considerably by blocking the large ISP [18]. Hence one cannot look to the market to ensure optimal expenditure on abuse teams, except over very long timescales.

2.5 Malware removal today

In an effort to improve the situation, a number of initiatives are currently underway. In the United States the largest cable provider, Comcast, has unilaterally decided to act [4]. In Australia [10], the Netherlands [9] and Germany [8], the ISPs have mutually agreed to deal with botnets; this mutual action means that all ISPs will incur similar costs. In the United Kingdom, an influential all-party Parliamentary group has recently recommended that the UK ISPs come to a similar mutual agreement [1].

Agreeing to handle abuse reports and pass them on to customers is only one part of the solution, because it is also necessary for the customers to have their computers cleaned up, and as just discussed, ISPs are not going to be enthusiastic about doing this. The most likely mechanism will be partnerships with third parties – Comcast has formed a partnership with McAfee for online assistance; and if the computer needs to be worked on by a skilled technician the user will be charged 89.95 USD for this service. Similarly, one of the Luxembourg ISPs recommends a local home visit service that charges Euro 18.95 per quarter hour.[3]

How users actually deal with malware problems is not widely studied. One of the few reliable datapoints we have is the 2006 Consumer Reports 'State of the net' survey of two thousand US households which found that 39% of those surveyed had a problem with a "virus" in the previous 2 years. Of these, 34% dealt with the problem by reformatting their hard drives, and 8% replaced their computers [5].

Purchasing a new computer might at first sight appear like a waste of money – but for many users it may well cost little more to purchase a new computer (which will be faster and better) than spend a fair proportion of the price in cleaning up the old one. Since the new computer will come with a modern operating system (better able to resist infections), and 'free' anti-virus and anti-spyware products, it is perhaps surprising that the figure was as low as 8%.

3 A government-funded scheme for malware removal?

It is envisaged that a government subsidised scheme for cleaning up computers infected with malware would work as follows:

[3]This sounds especially cheap, but the technicians are alleged to be under strict instructions that they are never to be so quick as to avoid charging for less than half an hour. Hence the price is more realistically portrayed as Euro 37.90, approximately 52 USD.

- The ISP abuse team receives a report that one of their customers has a computer that is a member of a botnet, that is sending spam, or has some other indication of malware infection.

- The ISP identifies the customer and informs them of their problem. The customer is provided with links to educational material (why their computer might be infected, and why this matters); some self-help data for the particular problem they seem to have (e.g. a Conficker-infected customer would be given links to the Conficker Working Group website[4]). They are also told the details of the government sponsored clean-up scheme, which they are entitled to use if they wish.

- Ideally, the customer uses freely available tools to clean-up their computer themselves. This will often be the best and most effective thing to do. Large businesses, with in-house IT Departments, are also likely to choose to deal with the problem internally.

- If the customer does not have success with these tools, then a technician will visit their home (or at lower price, the end-user can visit a local shop). Their computer will then be cleaned up for them. There will be a charge for this service, to prevent the 'moral hazard' of consumers deciding not to take any precautions at all, but this charge will be nominal (perhaps 20 USD, or 30 USD for a home visit) with the government paying for the rest of the service.

- The consumer is strongly encouraged to follow 'best practice' advice in installing anti-virus software and ensuring that their software is entirely up-to-date (using programs such as Secunia's 'Personal Software Inspector'[5]). The consumer will also be advised to change their online passwords (and password recovery questions), and to keep an eye on their bank and credit card statements for suspicious transactions.

If this scheme works as described then there are clear benefits.

There is of course the reduction of infected computers, albeit this action in one country may not be significant on a global scale. More important will be the reduction in data loss by citizens – malware usually includes a keylogger, so the quicker that a computer is cleaned up, the less likely that passwords will reach the criminals, and the smaller the time window they will have to exploit them.

Perhaps most importantly of all, the rapid, and hopefully painless, correction of the malware infection should prevent any loss of confidence in using the Internet. Most governments are now looking to the Internet as a way of cutting their own costs in communicating with citizens, and for benefits to the wider economy from having an online population. Keeping confidence in the Internet high is an essential prerequisite to tempting people online, and keeping them there.

[4] `http://www.confickerworkinggroup.org`

[5] `http://secunia.com/vulnerability_scanning/personal/`

Last, but by no means least, if the scheme is effective then other countries will look to implement their own version – this means that early adopters will find their international standing enhanced, and their views will carry more weight in this policy area.

3.1 Who will do the cleaning up?

There are a number of candidates for the task of cleaning up computers (since it will clearly not be done by the politicians or the civil servants!):

- Computer retailers – small computer shops have long been set up for computer repair, and larger companies have increasingly turned to this as a new source of revenue. The large retailers often offer on-site installation and repair, using brands such as 'Geek Squad'.
- Community groups – many countries provide free computer services for their citizens through local government initiatives, based around councils or communes. These institutions could extend their activities to include malware removal services.
- Utility companies – the utilities (electric, gas etc) have moved away from just maintaining their own infrastructure and now provide a range of consumer services such as emergency plumbers, central heating servicing, etc. Training some of their existing operatives to deal not only with gas boilers and leaky taps, but also with the relatively narrow field of malware removal is not entirely far-fetched.

3.2 Possible objections to the scheme

Cleaning up malware infected computers cannot be anything other than a good thing – hence provided that the work is of sufficient technical quality, there is no apparent downside to having it done.

However, it is far from obvious that ISPs will be delighted to pass their customers' details on to a third party (the clean-up company) with whom they cannot directly negotiate contractual safeguards. Suppose that third party not only removed malware, but – to receive an introduction fee – they persuaded the customer to move to another ISP. It will clearly be appropriate to identify this type of commercial concern early on and to place restrictions on the marketing of directly competitive services, lest ISPs decide that they will not co-operate.

The co-operation of the ISPs is of course essential, because they must handle the initial reports about malware infestation, and must make an initial communication with their customer. The scheme is designed to try and make this as easy as possible, and to allow them to automate almost all of their tasks. An IETF working document written by Comcast engineers [11] considers nine different ways of communicating with a user – their deployed system currently arranges for the user to see a warning in their web browser.[4]

Naturally, governments could take themselves out of the loop altogether, and invite companies to set up malware cleaning schemes themselves. Quite clearly, if these companies charge a

sufficiently high price to the users for their service then this will be profitable and computers will be cleaned. However, the risk is that the overall approach is far less likely to be successful, and not just because of a lower take-up caused by the non-subsidised price. The involvement of the government makes it easier to cajole ISPs into doing their part, and provides important assurance to citizens that the scheme is bona fide and that quality controls will be in place.

Of course, individual political philosophies differ significantly – so some would see any role at all for government as an anathema. It is only necessary to look around the world at the different approaches that were taken to handling the recent influenza epidemic to see these different philosophies at work.

Even where governments have an interventionist approach to dealing with public health problems (and dealing with malware is much the same sort of issue), many have a lamentable record of purchasing IT services, and that might be felt to doom the proposed scheme from the start. However, the government's task within the proposed scheme is restricted to picking out the low tender(s) that are consistent with appropriate quality controls; and this is not dissimilar to their role in other sectors where they manage to be reasonably effective.

Another doubt would be whether a government-sponsored scheme for cleaning up malware might reduce the market for technical innovations that would make the scheme unnecessary. Since the government's subsidy is fairly limited (the calculations below suggest that it will be less than a sixth of the total cost), this distortion of the market is not substantial, but it might nevertheless mean that some people will reject the scheme on philosophical grounds.

4 Likely costs of the scheme

In this section we build a model for the costs of the malware removal scheme and make some estimates for what these costs are likely to be. As will be seen, many of the cost estimates are extremely rough. It would be possible to pin some of them down by means of consumer surveys or pilot implementations, and doubtless a government considering this scheme as a policy option would promptly perform such investigations.

4.1 The model

The scheme being proposed involves costs for set-up, publicity, monitoring, audit and a wide range of other incidentals. These are not considered here. What is modelled and estimated covers what is likely to be the bulk of the money involved – the costs incurred per reported malware incident.

The model is that a malware report reaches an ISP who passes it on to their customer. Some customers will choose to deal with it themselves, whereas others will take advantage of the government subsidised clean-up scheme. If they choose the scheme then they pay a nominal amount for the service, with the remainder of the cost paid by the government.

Using variables for the various values we have:

A proportion, s, of reports cause the scheme to be used.

Hence $(1-s)$ of reports are dealt with 'for free'.

The cost per clean-up event is C, with the end-user paying e and the government $(C-e)$.

Hence the naïve view of operating the scheme means that the government puts it out for tender, the various organisations who wish to operate it calculate what they expect C to be (including an element of profit), and they put in a tender for $(C-e)$ and hope to be the low bidder.

There is of course going to be some significant price sensitivity, in that higher values of e lead to lower values of s – that is end-users may eschew an expensive scheme in favour of a do-it-yourself solution. Also, if e is the same as C (or higher) then the tenders submitted should all be zero (or negative, viz: organisations compete as to how much they are willing to pay for the contract).

However, there is potentially a lot more going on here than the initial naïve approach would suggest. Recall the US survey (8% of computers are replaced when there is a problem), and it can be seen that a certain proportion of end-users will not pay e at all, but will instead spend a considerable amount on a new computer, giving a profit of N to whoever supplied it. Clearly, the higher the value of e, the more likely this is to occur.

Furthermore, it will be possible to persuade a sizeable proportion of the end-users who stick with their old computer that, once it has been cleaned up, they should enhance it by the purchase of anti-virus software (or even just a new mouse). Looking further ahead, making sure that everyone who is dealt with is added to appropriate marketing lists should make it more likely in future that they can be sold new products (after all, they will be buying from those nice people who were so good at fixing their computer last year).

All of these opportunities to profit from the supply of goods to the end-user mean that an organisation that thinks themselves capable of doing this type of selling should lower their tender amount to ensure that they get the contract.

Expressing these further items as variables we have:

A proportion, n, choose a new computer, each yielding a profit of N.

A proportion, v, purchase anti-virus (etc), each yielding a profit of V.

A proportion, f, will purchase in the future, for a (net present value) profit of F.

Putting all of this together:

Those who choose a new computer bring in a profit of $n \times N$.

The others will incur a cost of $(1-n) \times (C-e)$.

The profit from selling anti-virus etc is $(1-n) \times (v \times V)$. [6]

The profit from future business is $f \times F$.

Hence the tender can be as low as: $(1-n) \times (C-e-(v \times V)) - (n \times N) - (f \times F)$.

[6] Note that new computers come bundled with anti-virus.

4.2 Putting some numbers into the model

It is possible to make some plausible estimates of the numbers in the model, in order to see what sort of tenders might be made.

We start by assuming that C (the clean-up cost) is 70 USD and that e (the amount to be paid by the end-user) is to be 30 USD.

Objections might reasonably be raised as to where these numbers come from. The examples given above were from the USA (89.95 USD) and Luxembourg (52 USD[7]). Arbitrarily, the mid-point of these two values has been chosen – dubious readers are at liberty to plug in their own favourite value. Similarly, a reasonable case can be made for e being anywhere between 20 USD (much lower and perceptions of moral hazard might make the scheme politically unworkable) and 40 USD (any higher and the scheme hardly involves a subsidy any more). Once again the midpoint (30 USD) has been chosen.

It's also worth observing at this point that C is nothing like constant, and for any company doing significant volumes of work (as they might expect to do, having been awarded a government contract for an entire country) there is ample scope for automation and cost-saving. In particular, the reports flowing through the ISPs are likely to be for large numbers of instances of small numbers of particular malware variants – viz: with a little preparation clean-up can be made very simple for the vast majority of cases.

We know from the US that with e in the 90 USD region then n (the proportion of end-users purchasing a new computer) is 0.08 and N (the profit from such a sale) will be around 100 USD. It's hard to say how elastic demand for a new computer might be, but let us assume that with $e = 30$ USD then n is 0.05.

The end-user price of commercial anti-virus products is highly variable and there are many discounts. It is plausible to assume a list price of 70 USD and a profit margin of 42 USD (that's 60% trade discount). Hence V is 42, and we will assume that, given the circumstances of the sale, there will be a sale in 50% of cases (ie: $v = 0.5$). Note that if it was an anti-virus manufacturer offering the service then the discount could be almost 100% rather than 60%.

Finally, we have to estimate the likely future profit from the customer relationship ($f \times F$). This isn't easy, but the going price in Google Adwords for 'new laptop' is estimated at 1 to 4 USD. It might be assumed that appropriate relationship management would yield just as good a result as buying the most expensive clicks, so we will put this value in at 4 USD.

Plugging these values into the model we find that the naïve tender value ($C-e$) would be 40 USD and the more sophisticated one, taking account of all the other factors, would be 11.05 USD.

Quick inspection shows that the most significant contribution to the lowering of the price is the sale of anti-virus software, which is reducing the tender price by 19.95 USD all on its own. Hence there's significant sensitivity here to both the sale price and the conversion ratio: if v was only 33% then the tender price should be 17.70 USD. Quite clearly, this high dependency on the sales

[7] In fact this should be 47 USD because there's a kickback of 10% to the ISP for every customer they refer.

of extra products alongside the clean-up service means that any organisation contemplating a low tender will have to implement an effective plan to train their technical operatives to be competent at end-user selling.

The final calculation worth doing would be the government's costs. Assuming that an organisation was indeed prepared to tender 11.05 USD per clean-up, what should the government budget to spend?

Estimates of malware infection vary considerably from a few percent of the online population,[8] up to scare-mongering 25% plus values.[9] Some of the most reliable data comes from the Microsoft MSRT programme, which expresses infection rates in CCM (computers cleaned per thousand runs of their scanning software). The CCM values are also very variable, but are typically under 10 for first world countries – the USA is 8.6, the UK 4.9 and Finland 2.3. Converting CCM values to overall infection rates is complex, but it does suggest that about 1% of the computer population will need the clean-up service per month.[10]

Assuming that s (the proportion of malware infected computers that are dealt with by the service) is 0.5 this means that about one in 200 computers will be using the service each month at a cost to the government of 11.05 USD. ie: the annual cost per computer will be about 66 cents. The total cost clearly depends on the number of actively used computers in the country, which will be roughly equal to the population. Putting this in context, this amount is rather less than the cost of water fluoridisation [3] of about 92 cents per person (in today's money), and debates about that public health policy are seldom about the cost.

It might finally be noted that there are potential financial assistance opportunities for early adopters – for example within the European Union, a successful scheme in one Member State is very likely to lead on to deployment elsewhere. It might therefore be possible to seek money for prototyping from central EU funds, particularly if this speeded up any aspect of deployment.

[8] Panda Security provide per country information, which distinguishes types of malware. Presently about 3.1% of UK computers have a serious problem (as do 7.3% of US computers). `http://www.pandasecurity.com/img/enc/infection.htm`

[9] The 2008 OECD report on Malware [14] contained the sentence "Furthermore, it is estimated that 59 million users in the US have spyware or other types of malware on their computers." News outlets picked up on this, e.g. The Sydney Morning Herald [20] who divided the 59 million figure into the US population, and then concluded that around a quarter of US computers were infected (assuming that each person owned one computer). The OECD published a correction in the online copy of the report a few days later. They were actually quoting PEW Internet research on adware/spyware (which is a subtly different threat) from 2005 (which was a while earlier than 2008). The sentence should have read "After hearing descriptions of 'spyware' and 'adware', 43% of internet users, or about 59 million American adults, say they have had one of these programs on their home computer." Of such errors in understanding the meaning of data is misinformation made.

[10] Microsoft's general approach is to tackle widespread malware infections – viz: the high volume events. The work left over, which needs to be dealt with by the clean-up system, will concern a minority of people who have failed to enable the Microsoft tool, and malware with lower populations. Hence, assuming that Microsoft have already dealt with half the problem is a reasonable working estimate.

5 Conclusions

It has long been obvious that there are no effective schemes in place for ensuring that end-users who are infected with malware have their computers cleaned up.

Some countries are now beginning to see agreements being brokered between ISPs to deal with the problem – addressing some of the negative incentives by agreeing to act in a consistent and, sometimes, collaborative manner. However, there are considerable externalities to malware infection, and hence strong arguments have been made for regulatory action to compel effective malware removal [2].

This paper has suggested an intermediate scheme – short of compulsion – which involves a government subsidy for clean-up schemes. Some political philosophies will of course dismiss this out-of-hand, but there are clear analogies with government initiatives for improving public health, which is often seen as an entirely appropriate milieu for government action.

Although subsidies might initially be though to be substantial, modelling the opportunity to sell extra products alongside the main service suggests that with some plausible assumptions the cost to the public purse could be under a dollar per computer per annum – well in line with other public health initiatives.

Given that almost every wickedness on the Internet is underpinned by malware-infected computers – and given the slow and patchy Internet industry response – this is clearly a legitimate area for governments to consider getting involved in, and putting up money to improve.

References

[1] All Party Parliamentary Communications Group: Can we keep our hands off the net? Inquiry Report, 2009. http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf

[2] R. Anderson, R. Boehme, R. Clayton and T. Moore: Security Economics and the Internal Market. European Network and Information Security Agency, Jan 2008.

[3] Centers for Disease Control and Prevention: Recommendations for using fluoride to prevent and control dental caries in the United States. MMWR Recommendation Report 50 (RR-14): pp. 1–42.

[4] Comcast Corporation: Comcast Unveils Comprehensive "Constant Guard" Internet Security Program. Press Release, 8 Oct 2009.

[5] Consumer Reports: State of the net. Sep 2006. http://web.archive.org/web/20060820182702/http://www.consumerreports.org/cro/electronics-computers/online-protection-9-06/overview/0609_online-prot_ov1.htm

[6] D. Crocker: Mailbox Names for Common Services, Roles and Functions, RFC2142, IETF, May 1997.

[7] Earthlink Inc.: EarthLink Announces First Quarter 2010 Results. Apr 2010. http://ir.earthlink.net/releasedetail.cfm?ReleaseID=463674

[8] eco: Anti-Botnet-Projekt des eco – Verband der deutschen Internetwirtschaft mit Unterstützung des BSI. Press Release, 10 Dec 2009. http://www.eco.de/verband/202_7268.htm

[9] G. Evron: Dutch ISPs Sign Anti-Botnet Treaty, Dark Reading, 29 Sep 2009. http://www.darkreading.com/blog/archives/2009/09/dutch_isps_sign.html

[10] J. Hilvert: eSecurity code to protect Australians online. 11 Sep 2009. http://iia.net.au/index.php/section-blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.html

[11] J. Livingood, N. Mody and M. O'Reirdan: Recommendations for the Remediation of Bots in ISP Networks. IETF Internet-Draft, version 8, Apr 2010. http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-08

[12] D. McPherson: ISP Death By A Thousand Duck Bites. Arbor Networks Security Blog, Sep 2007. http://asert.arbornetworks.com/2007/09/isp-death-by-a-thousand-duck-bites/

[13] T. Moore, R. Clayton and R Anderson: The Economics of Online Crime. Journal of Economic Perspectives, 23(3), 2009, pp. 3–20.

[14] Organisation for Economic Co-operation and Development: Malicious Software (Malware): A Security Threat to the Internet Economy. Ministerial Background Report, DSTI/ICCP/REG(2007)5/FINAL, June 2008.

[15] M. Polychronakis, P. Mavrommatis and N. Provos: Ghost turns Zombie: Exploring the Life Cycle of Web-based Malware. 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), Apr 2008, pp. 1–8.

[16] N. Provos, P. Mavrommatis, M.A. Rajab and F. Monrose: All your iFRAMEs point to Us. 17th USENIX Security Symposium, 2008, pp. 1–15.

[17] N. Provos, M.A. Rajab and P. Mavrommatis: Cybercrime 2.0: when the cloud turns dark. Comm. ACM, 52(4), 2009, pp. 42–47.

[18] A. Serjantov and R. Clayton: Modelling Incentives for Email Blocking Strategies. Fourth Annual Workshop on Economics and Information Security (WEIS05), 2005.

[19] K. Sherrill: Cost Per Call: Are we comparing apples to apples? Help Desk Institute Library, 2003. http://www.thinkhdi.com/library/deliverfile.aspx?filecontentid=234

[20] Sydney Morning Herald: A quarter of US PCs infected with malware: OECD. 2 Jun 2008. http://news.smh.com.au/world/zombies-and-botnets-oecd-warns-of-hidden-armies-in-cyber-wars-20080601-2kel.html