Malware and Cyber-crime

This volume contains the written evidence accepted by the Science & Technology Committee for the Malware and Cyber-crime inquiry.

<table>
<thead>
<tr>
<th>No.</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Home Office</td>
</tr>
<tr>
<td>00a</td>
<td>Supplementary</td>
</tr>
<tr>
<td>01</td>
<td>Professor Peter Sommer</td>
</tr>
<tr>
<td>02</td>
<td>Dr Huma Shah</td>
</tr>
<tr>
<td>03</td>
<td>David Emm and Professor Steven Furnell</td>
</tr>
<tr>
<td>04</td>
<td>Intellect</td>
</tr>
<tr>
<td>05</td>
<td>StopBadware</td>
</tr>
<tr>
<td>06</td>
<td>Fenmeccanica Cyber Solutions</td>
</tr>
<tr>
<td>07</td>
<td>MAAWG</td>
</tr>
<tr>
<td>08</td>
<td>McAfee</td>
</tr>
<tr>
<td>09</td>
<td>Symantec</td>
</tr>
<tr>
<td>10</td>
<td>Dr Richard Clayton</td>
</tr>
<tr>
<td>11</td>
<td>BCS (the Chartered Institute for IT), IET (The Institution of Engineering and Technology), and The Royal Academy of Engineering</td>
</tr>
<tr>
<td>12</td>
<td>Amit Bhagwat</td>
</tr>
<tr>
<td>13</td>
<td>SOCA</td>
</tr>
<tr>
<td>14</td>
<td>Police Central e-Crime Unit</td>
</tr>
<tr>
<td>15</td>
<td>Raytheon UK</td>
</tr>
<tr>
<td>16</td>
<td>Dellsecureworks</td>
</tr>
<tr>
<td>17</td>
<td>Microsoft</td>
</tr>
<tr>
<td>18</td>
<td>Nominet UK</td>
</tr>
<tr>
<td>19</td>
<td>Australian Institute of Criminology</td>
</tr>
<tr>
<td>20</td>
<td>PhonepayPlus</td>
</tr>
<tr>
<td>21</td>
<td>Research in Motion</td>
</tr>
<tr>
<td>22</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
</tr>
</tbody>
</table>

As at 1 December 2011
Written evidence submitted by the Home Office (Malware 00)

Prepared by the Home Office in consultation with other Government departments.

Introduction

1. This paper sets out the Government evidence to the Science and Technology Committee inquiry into malicious software (malware) and cyber crime. It has been prepared by the Home Office in consultation with officials from other Government departments including the Office of Cyber Security and Information Assurance at the Cabinet Office, the Cyber Security Operations Centre and the Department for Business, Innovation and Skills.

2. The paper outlines what the Government believes to be the situation regarding malware and cyber crime and makes references to current and future actions which are tackling these issues. Separate evidence will be submitted by the Serious and Organised Crime Agency (SOCA) and by the Metropolitan Police Service's Police Central e-Crime Unit. The papers from these organisations will provide more information on current operational activity to tackle cyber crime.

3. We define the term ‘malware’ to denote software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system.

4. Malware allows criminals to compromise and control computers. This is achieved through a variety of means, including spam e-mails that encourage a user to click on a link that downloads the malware, or through placing malicious code in an otherwise legitimate website that will cause the user's computer to be infected when the website is viewed.

5. Malware is used for a variety of criminal purposes, in particular data theft. This might include credit card or bank account details, or industrial or government information, to be sold on for profit. Often the criminal and the purchaser of the information will be in different countries, with the victim in a third country.

6. We assess that the threat from malware is growing, with a huge rise in the amount of it being created and used – in 2010 more than 286m unique malware variants were identified\(^1\). Some of these are relatively simple but many are highly sophisticated.

7. Of the various types of malware, Trojans have become the most prevalent - making up nearly 70% of attacks according to some anti-virus

---

\(^1\) Symantec Internet Security Threat Report 2010
companies - as they are the most flexible in allowing the instigators of an attack access to the target computer. They can be seen as an enabler for all the other types of malware.

**What proportion of cyber-crime is associated with malware?**

8. Cyber crime falls into a number of categories, within the general principle that what is illegal offline is illegal online. Some crimes can only be carried out using the internet, including attacks on computer systems to disrupt IT infrastructure, and the stealing of data over a network using malware, often to enable further crime.

9. Other crimes have been transformed in scale or form by their use of the internet; for example credit card fraud can now take place on an industrial scale. Although crimes such as fraud and theft have always existed, the growth of the internet has opened up a new market, allowed for a degree of anonymity and has created new opportunities for organised criminal groups to finance their activities.

10. A third type of crime, which uses the internet but is not dependent on it, is that which is facilitated by the internet. Networks are used for communication, organisation, or to try to evade law enforcement, in the same way as older technologies such as telephones. The internet may be used to organise more effectively a range of ‘traditional’ crime types such as drug dealing, people smuggling, and child exploitation and to conceal them more easily from law enforcement agencies. Mobile internet technology was used by rioters to co-ordinate looting and disorder in August of this year.

11. Determining the proportion of cyber crime which involves malware would therefore depend on which level of cyber crime was under consideration. Moreover, there is no easy measure of the levels of the different types of cyber crime or of how they operate. It is also difficult to gather and assess information on cyber crime as it occurs.

12. Work is being carried out to address this issue; for example, Action Fraud, which works closely with the National Fraud Intelligence Bureau, is to be expanded to become the single reporting point for financially-motivated cyber crime.

13. However, the threat posed by cyber crime is believed to be significant. *The Cost Of Cyber Crime*², published by Detica and the Office of Cyber Security and Information Assurance in February 2011, estimates the cost to the UK of cyber crime to be up to £27bn per year, or around 2% of GDP. Industrialisation of cyber crime to enable high volume activity, such as mass data theft, is largely reliant on malware.

14. It is therefore not possible to determine what percentage of cyber crime is facilitated by malware, but there is no doubt that it is a significant factor. As mentioned in the introduction, production of malware is increasing exponentially and it has transformed the ability of criminals to steal data over networks.

Where does the malware come from? Who is creating it and why?

15. The major threat from cyber crime comes from increasingly technically-proficient individuals and organised crime groups. These groups, and the infrastructure used in the attack, are often outside the jurisdiction of the UK. The criminals may be in one country and their means of cyber attack in a second and their victims in a range of other countries, making evidence gathering and identification of the criminals difficult. They may not fit the traditional profile of organised crime groups, and may be more of an affiliation of individuals who never meet except online.

16. Most organised criminal activity is aimed, either directly or indirectly, at making money. Organised crime groups and individuals use cyber technology to support traditional criminal activities or to develop new criminal schemes that exploit emerging vulnerabilities in rapidly evolving cyber technologies and online systems. By focusing their activity on areas which afford the broadest opportunities, criminals increase their potential monetary returns. Criminal finances and profits are central to organised crime and they constantly seek the opportunity to increase their returns whilst reducing their risk exposure.

17. Although most criminal activity is financially motivated, a spate of recent attacks on company websites has been orchestrated by activists protesting against those associated with ideals they disapprove of. This has highlighted the disruption that organised groups can cause, in order to further their aims, through the use of malware and techniques initially developed for other criminal purposes. This type of activity could be used against any public or private sector organisation with a presence online and against which a group may hold a grievance.

18. While the creator of malicious software may not be the end-user criminal, the goals noted above create a market place for malware. As such most of the malware writers will expect to profit from their works and have an increasingly sophisticated business model, including maintenance and support for their software, hiring their expertise out directly and upgrading their products in light of changes in the market, to support this. Malicious software and access to other tools, such as pre-existing botnets, is freely available for purchase at a variety of ‘underground’ internet fora. This ‘underground’ infrastructure also requires protection, leading to secondary layers of required technical expertise. The profit motive is less prevalent amongst the activist community where more ideological goals may drive the malware writers.

19. Many IT security companies report the source of malware as the location where it is hosted as it is often difficult to identify the origin of the
software itself. This reporting of attack location rather than the source of the malware can badly skew statistics on where malware creators are based, however, the IT Security company BitDefender suggests in its H1 2011 report (http://www.bitdefender.com/files/Main/file/H1_2011_E-Threats_Landscape_Report.pdf) that China (31%), Russia (22%) and Brazil (8%) are the largest producers of malware.

What level of resources are associated with combating malware?

20. In October 2010 the National Security Strategy identified the cyber threat to the UK, which includes cyber crime, as a Tier 1 threat, on the same level as terrorism. £650m of new money has been allocated to a National Cyber Security Programme which will bolster our cyber capabilities in order to help protect the UK’s national security, its citizens and our growing economy in cyber space. At least £63m of this money will go towards enabling the UK to transform our response to cyber crime, of which countering malware is an important element. This money is additional to the resources already allocated to the police and other agencies to tackle crime, including cyber crime.

21. The NCSP will also bolster cyber capabilities within the intelligence community. GCHQ, as home of the National Technical Authority for Information Assurance, CESG, is of particular relevance here. CESG’s role is to provide consultancy and technical support to government and others, in order that they are able to understand the risks they face and can therefore protect vital information services and data. Improving protection of data through reducing vulnerabilities via which malware can gain a foothold is key to reducing the effectiveness and impact of the malware, and can be much less costly than taking a reactive stance whereby malware is only identified after it has had a detrimental impact.

22. The Police Central e-Crime Unit (PCeU) and the Serious Organised Crime Agency (SOCA) include the combating of malware as part of their current work on tackling cyber crime. Further information will be provided in their own evidence to this enquiry.

23. Work has begun to create a dedicated cyber crime unit as part of the National Crime Agency, building on the work already done by SOCA and PCeU. There will continue to be close working between the two units to develop the national response to cyber crime in advance of the creation of the NCA. This will be a specialist unit and will support the work of all of the commands within the National Crime Agency.

24. The unit will be the national centre of excellence for law enforcement, and will provide resources, intelligence and guidance on best practice to forces. To support the mainstreaming of knowledge of cyber crime, the learning developed by the unit will be fed into police training programmes to provide understanding of online crime issues across the police service.

25. In February 2011, the Prime Minister brought together 13 CEOs from a broad spectrum of large companies to discuss private sector resilience to
cyber threats, including online crime. The meeting was designed to inform them of our new approach to tackling this issue and the renewed emphasis on improving the UK’s cyber security capability, including better protection for business from all types of online threats and the need for the private sector to work in partnership with government to achieve this aim. At that meeting it was agreed that a joint capability, in the form of a ‘hub’, would be co-designed by a cross sector working party.

26. Since then, the working group has been meeting regularly to turn the ‘Hub’ into reality. The group will report back to the Prime Minister in the autumn and an announcement will be made on the manifestation of the Hub, calling on all organisations to take an active role in protecting our collective interests in cyberspace.

What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

27. Cyber crime causes harm to individuals and the private sector in a range of ways. It results in direct and indirect financial losses amounting to billions of pounds, adverse credit ratings and protracted disputes over suspect payments, and causes damage to reputations. Further harm can be caused by online extortion, bullying, harassment and hate crimes.

28. The Detica/ OCSIA Cost of Cyber Crime Report estimated that the cost to citizens of all types of cyber crime taken together (not just that involving malware) was £3.1 billion per annum. The loss to industry, including from intellectual property theft and espionage, was estimated at £21 billion.

29. We are aware of some excellent initiatives that have been taken by internet service providers to combat the spread of malware. These include initiatives such as anti-virus alerts when visiting websites and warning customers whose PCs are part of a botnet.

30. The banking sector has also invested heavily in ID assurance products for online banking customers, as well as providing free software for internet users which monitors transactions and alerts when malware is detected on a system.

31. Such innovation is welcome and shows what can be done when the private sector tackles security issues in partnership with consumers. However, we believe that more could be done.

32. The government plans to discuss with the largest internet service providers a possible partnership between industry, government and law enforcement to establish how malware and botnet activity on the networks could be identified and addressed.

33. We also want to make sure that the public and businesses understand the risks of being online and know how to take the appropriate action to
protect themselves. Get Safe Online (www.getsafeonline.org) is a joint initiative between the Government, law enforcement, business and the public sector, which has been created to provide computer users and small businesses with free, independent and user-friendly advice to help them to use the internet confidently and securely.

**Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?**

34. The Government is committed to tackling the security challenges we face in cyberspace, which include the pervasive distribution of criminal malware. However, taking action to prevent cyber crime cannot be the responsibility of the Government alone. The private sector and the public have important roles to play alongside law enforcement organisations, technical experts within government departments and the intelligence and security community.

35. Keeping security software and operating systems up to date and running anti-virus programmes are two key methods to reduce the risk of computer systems being compromised by malware. A major contribution to reducing the vulnerability of systems to cyber crime can come through industry's ability to deliver consistent, good quality information assurance products and services.

36. This can range from a member of the public choosing an appropriate security package to install on their home computer, to a large organisation designing its online services securely. We want the public and businesses to be able to identify easily products with good security. We will work with the private sector and others to identify how standards for measuring the effectiveness of products or services could be developed.

37. Much has been done to raise awareness of online threats, including through the website Get Safe Online. We will build on that initiative and others by developing a single Government portal for the provision of advice on internet safety to the public and businesses. We will ensure that the information gathered by law enforcement and the private sector which might help internet users is shared. We will drive this by making sure that every Government website, as well as DirectGov, contains a link to this safety information.

38. In this respect, the approach we are taking to combating malware is similar to how the Government approaches the control of human disease, being a multi-stakeholder approach which looks at the problem holistically, resulting in a number of policy options to tackle the creation and distribution of malware in parallel to mitigating the damage caused and bolstering defences. In addition, in some circumstances infected systems may also be quarantined.
**How effective is the Government in co-ordinating a response to cyber-crime that uses malware?**

39. By building upon existing capacity within the intelligence and security agencies and law enforcement units the Government is investing in better protection against malware and increased disruption of criminal networks. Further information about ongoing activity to combat malware and cyber crime will be provided by SOCA and PCeU in their evidence to this enquiry.

40. The Government has been proactive in identifying cyber crime and the proliferation of malware as a key international security issue. As such this issue will form a core element of discussions at the London Conference on Cyber Space in November, hosted by the Foreign Secretary, which will bring together representatives of over 60 nations and international organisations.

41. The Government has also been instrumental in working more closely with the primary victims of malware and online crime, the private sector. Millions of UK citizens rely on secure online systems for their livelihoods as well as underpinning their enjoyment of the online world. We increasingly shop, communicate, transact and interact socially online. Confidence in the security of the internet is therefore critical to consumer confidence.

42. With this in mind the Government's collaboration with the private sector has progressed to form a lasting partnership to improve our collective response to cyber attacks on both public and private sector systems. This work will continue with the intention of creating a mechanism to share actionable intelligence on cyber threats, including malware, between Government and the various at-risk areas of the private sector.

43. The Government has recognised that we need to do more to respond effectively to cyber crime. We will shortly publish our cyber crime strategy setting out how we will achieve a transformation in our approach, supporting activity across all sectors – the public, business, Government and law enforcement – to deliver an integrated response.

44. We will reduce the vulnerability of the UK through better system design, crime prevention and public awareness; reduce the threat to the UK through disruption and prosecution of online criminals; and reduce the impact on the UK through the development of partnerships with the public, business and international partners.

Home Office

7 September 2011
Supplementary written evidence submitted by the Home Office (Malware 00a)

Letter to the Chair of the Committee from James Brokenshire MP, Parliamentary Under-Secretary of State for Crime and Security, Home Office, 28 November 2011

Thank you for the opportunity to give evidence to the Science and Technology Committee’s enquiry on malware and cyber crime. I welcome the Committee’s engagement in considering ways of tackling this increasingly important issue and look forward to your report.

I undertook to write regarding the question of progress on the Identity Assurance programme. The programme, which sits within the Government Digital Service and is led by the Minister for the Cabinet Office, Rt Hon Francis Maude MP, is working with departments to develop a federated identity assurance model. Ms Nash raised the question of whether the programme was on schedule, as she believed a prototype was to have been tested in October.

I am happy to confirm that, in line with the stated schedule, a prototype was made available in October, in the form of a Beta solution developed by the DWP Universal Credit programme. This sought to prove various technical aspects of the proposed architecture, and was successfully tested with a number of potential private sector Identity Service Providers. The wider cross-governmental solution is now being reviewed and further developed following feedback from the commercial sector.

It might be helpful for me to provide some further information about the purposes of the scheme. The Identity Assurance programme deals with the way a service provider can be assured that the customer or user is who they say they are as they access Government services. The user will be able to choose an identity assurance service from a range of certified providers; the user may choose to register for one or many of these services. The model will place the user in control. The user will determine how his or her personal data is disclosed when registering to create a digital identity and subsequently when the digital identity is used.

A principal difference with the now defunct National Identity Scheme is that it discards the reliance on a central identity register in favour of a decentralised, federated structure. Public service providers will determine the level of identity assurance they require; the user will then meet those requirements using an identity provider.

The Identity Assurance Programme is working with Industry, the National Fraud Authority, National Fraud Intelligence Bureau, Serious Organised Crime Agency, CESG (the UK’s National Technical Authority for Information Assurance) and other interested stakeholders to ensure the design has appropriate capabilities to combat
fraud, protect the user's privacy and enhance the customer experience of digital transactions.

The programme supports the 'digital by default' policy. Digital transactions offer both convenience for customers and cost saving opportunities for public service providers. For the model to be successful there must also be benefits for commercial identity service providers. The programme's commercial workstream is working with industry to develop suitable commercial models.

Mike Bracken (Executive Director of Government Digital Service) took over as SRO for the Identity Assurance Programme at the beginning of October. Funding for this programme has now been agreed and a review of the existing programme and associated resources will be undertaken and completed by the end of the year.

Our ambition is for this programme to create new private sector enterprise, new investment, more jobs and ultimately produce trusted solutions, which will be key to ensuring citizens have greater confidence to engage with public (and private) sector services online.

I hope this will reassure the Committee about the progress of the programme and the importance of this work to improving the security and accessibility of Government services.

James Brokenshire MP
Parliamentary Under-Secretary of State for Crime and Security
Home Office
November 2011
Written evidence submitted by Professor Peter Sommer  
(Malware 01)

1. I am a Visiting Professor at the London School of Economics and a  
   Visiting Reader at the Open University. I have acted as an expert  
   witness in many trials involving complex computer evidence; some of  
   these have included the deployment of malware.

2. The Committee will recall that I provided written and oral evidence for  
   its earlier inquiry into Scientific Advice in Emergencies (HC498).

3. As an academic I have had a very long-standing interest in the issues of  
   the statistics of computer-related or “cyber” incidents as these are often  
   used as the basis of formulating security policies. In March 2009 I  
   carried out a literature review, including statistics, of Internet crime for  
   the National Audit Office as a contribution to a value-for-money  
   review of Government initiatives in reducing the impact of such crimes.

4. I believe I may be able to assist the Committee by drawing to its  
   attention the problems associated with defining “cyber-crime”,  
   producing statistics of its incidence and providing measures of harm or  
   damage.

5. **Declaration.** I have no commercial links to any organisations offering  
   products and services dealing with malware

**Definitions of Cyber-crime**

6. There is no generally-agreed definition of cyber-crime and this lack  
   directly impacts assessments of extent. We can illustrate the diversity of  
   definitions. The Council of Europe CyberCrime Convention\(^1\), also  
   known as the Treaty of Budapest, covers in Articles 2-6 as “substantive  
   offences”: “illegal access”, “illegal interception”, “data interference”,  
   “system interference”, and “misuse of devices”. It adds as “computer-  
   related offences”, articles 7 and 8, “computer-related forgery” and  
   “computer-related fraud”. It further adds, articles 9 and 10: “offences  
   related to child pornography” and “offences related to infringements of  
   copyright and related rights”. It will be seen that articles 4 and 5,  
   respectively, “data interference” and “system interference” include  
   “malware”. Articles 4 and 5 more-or-less correspond to s 3 of the UK  
   Computer Misuse Act, 1990: “Unauthorised acts with intent to impair, or  
   with recklessness as to impairing, operation of computer, etc.”

7. If we now turn to a report produced in February 2011 by the BAE  
   subsidiary Detica in partnership with the Cabinet Office’s Office of  
   Cybersecurity and Information Assurance (OCSIA), *The Cost of Cyber*

---

Crime\(^2\), this covers: “identity theft and online scams affecting UK citizens; IP theft, industrial espionage and extortion targeted at UK businesses; and fiscal fraud committed against the Government.” “Industrial espionage “ is not a criminal offence in the UK\(^3\) and the report excludes any direct reference to malware or to child pornography.

8. The Committee will need to be alert to “research” the main aim of which is to sell product and services rather than inform about risk. The Committee should also watch carefully for the use of language that scares rather that informs. At the moment a number of malware vendors are referring to something called “Advanced Persistent Threats” or APTs. At any point in the last 40 years of computer security there have been threats which for their time were “advanced” and which were deployed with “persistence”. Whilst some malware can be readily and usefully identified by way of their methods of exploitation or distribution – for example “buffer overflow”, “cross-site scripting”, “back-door”, “boot-sector”, USB autostart”, “browser hijack”, “covert registry modification”, “email address book hijack” etc, “APT” appears to have no useful meaning.

Estimates of Cyber crime

9. Most official forms of crime recording in the UK are on the basis of specific offences prosecuted. But in relation to “cyber crime” there are particular difficulties as a result of policies of the Crown Prosecution Service. It sees the 1990 Computer Misuse Act as designed to fill in gaps in other forms of legislation\(^4\) and in framing charges will concentrate on what it sees as the substantive offence rather than a modus operandi. Thus, if some-one infiltrates a program to monitor the keystrokes on a computer and then subsequently uses the passwords thereby obtained to access a computer from which to carry out a fraudulent transaction, the offence will probably be recorded as a breach of the Fraud Act 2006, despite the fact that both s 3 and s 1 Computer Misuse Act offences took place. The keystroke monitor would be classified as “malware”. A phishing attack would probably also be charged as fraud or money laundering, a Distributed Denial of Service attack (which also tends to involve offences under s 3 Computer Misuse Act when computers are remotely taken over by malware “back doors”) would probably be charged as extortion as this is the most common way in which criminals can make money. In every year since the Computer Misuse Act came into force, prosecutions have seldom exceeded 100 per year.


\(^3\) http://www.justice.gov.uk/lawcommission/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_T rade_Secrets_Consultation.pdf

\(^4\) Statements frequently made by CPS officials in public and private
10. As with many other studies of the extent of crime there are significant methodological difficulties – how far does one include crimes which are suspected but never come to court – what should be the standard of proof for inclusion? Is this “proof” the act of reporting to the police or replying to a question in a survey? What fudge factors should one apply for situations where individuals think they have been subjected to criminal actions but have not – or where they have actually been victimised but have an inadequate realisation? What further fudge factors do you allow for unreported crimes? In relation to activities which cause distress, do you only include situations where a crime has been committed?

11. In terms of the incidence of malware, the problems of collecting data are somewhat easier. A number of anti-malware vendors offer out-sourced services. The customer agrees to route all his email and web traffic via the vendor who then detects and removes the malware. In an alternative, the customer installs on his own premises a “black box” controlled by the vendor which has the same effect. In both instances the anti-malware vendor is in a position to collect statistics about the variety and frequency of deployment of malware. Examples of such statistics come from Symantec5, Macafee6, Sophos7 and Websense8.

12. However these statistics are not reliable as to harm and impact. They refer to situations where malware has been detected and, for the most part, thwarted. They do provide a powerful argument for deploying anti-malware products.

Financial Costs of Cyber crime and Malware

13. The cost of any incident can be divided into direct and consequential. Direct: “My building and contents have been destroyed and I need money to replace them”. Consequential: “While waiting for the replacements I was unable to generate turnover and profit”. In the vast majority of malware-triggered incidents there is no physical damage, so that all the losses are consequential. As such the extent of loss in any one incident is substantially a function not of the malware itself but of the use to which the affected computer is being put and the speed with which the victim can recover. That in turn reflects the existence and efficacy of a contingency plan. Contrast the positions of a PC used domestically for entertainment hit by the same malware as a PC sitting on the desk of an city financial trader dealing in multi-million dollar contracts.

14. A further issue is what to include in remedial costs – what allowance do we make for imprudent victims who have not taken elementary

6 http://home.mcafee.com/VirusInfo/RegionalVirusInformation.aspx
7 http://www.sophos.com/support/knowledgebase/article/58736.html
8 http://www.websense.com/content/threat-report-2010-introduction.aspx
precautions to protect themselves – or who through clumsiness actually make the situation worse?

15. For this reason all estimates of the costs of cybercrime and malware are wildly speculative.

16. Some analysts seek to include “lost business opportunities” as opposed to a loss of revenue. The latter can be established by extrapolating from the past business records of a victim and is insurable, the former is simply an optimistic guess and is not insurable. Returning briefly to the BAE/Detica Report mentioned above9: At page 3-6 “Costs of different types of cyber crime to the UK economy” identifies “IP Theft” at over £9.2m and “Industrial Espionage” at £7.6bn. At page 5 there is a table purporting to break down “industrial espionage” losses by industry. It is difficult to see by what plausible methodology these figures were obtained. As we have seen, the Report does not cover malware at all.

17. Statistics and cost impacts are a valuable aid to policy making but reliance on invented figures can only result in bad decisions.

18. Looking specifically at malware, provided that potential victims subscribe to a high quality anti-malware products which pick up the overwhelming majority of threats, the main impact is the cost of the subscription to the service. For domestic users free anti-malware products are available, eg Grisoft AVG10 which incur no cost at all. This would leave the impact of so-called zero-day malware, that is malware which has not to that point come to the attention of the anti-malware vendors and is not detected by their products. As we have seen above, loss is then a function of where and how a specific computer is being used and associated contingency / data recovery plans.

Responses to Committees specific questions

19. Q1. What proportion of cyber-crime is associated with malware?
   
   Please see my paragraphs 6-12 above

20. Q2. Where does the malware come from? Who is creating it and why?
   
   This is not directly within my expertise. However it appears that there are several different motives. A distinction needs to be made between malware which is released generally and malware which is specifically aimed and where it is part of a targeted act to cause harm, or create opportunities for fraud, espionage or extortion. In the former, the aim seems to be to prove the “success” of the exploit by the number of

21. Much malware is possible because of the increasing complexity of modern operating systems and applications and their release by software houses without proper testing. Companies like Microsoft desire the additional revenue that the frequent release of new software versions bring and then offer to remedy discovered faults, post purchase, by the provision of frequent “patches”. But what other product in history issues rectifications once a week for its entire lifecycle as is the case with its main operating systems? The product faults are discovered by the computer security research community and these are then turned, often by others, into the exploits that become malware. Government could use its power when buying operating systems and application programs and complain about the high level of exploitable bugs.

22. Q3. What level of resources are associated with combating malware? The main resource is that of that anti-malware companies who discover new instances and then include detective and remedial measures in their products. All businesses need to have a contingency/recovery plan to cover a variety of scenarios, including malware infection. Such plans are a combination of data back-up and management action plans. See also my remarks at paragraph 25 below about policing.

23. Q4. What is the cost of malware to individuals and how effective is the industry in providing protection to computer users? See my remarks at paragraphs 13-18 above

24. Q5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease? This appears to be a misleading analogy as there is no equivalent for malware for the doctors, nurses and hospitals which make up the NHS nor any need for them. The main remedies are anti-malware products and contingency/back-up plans. There is an argument for a modest publicly funded Computer Health Information Service which includes advice on malware and contingency planning. This role is fulfilled by GetSafeOnline though there are questions about its level of funding. But much of the effort could surely be left to the private sector anti-malware vendors, whose interest in this instance in selling good products aligns with the national interest in protecting the public and business.

25. Q6. How effective is the Government in co-ordinating a response to cyber-crime that uses malware? For malware that is released but not targeted the main aim of Government policy should be advisory – see
my remarks above. For malware used as part of a targeted criminal process the additional remedy is effective policing. The same police resource could also be used to identify those very few UK-based instances where non-targeted malware is authored or deliberately released from the UK, for example Christopher Pile, sentenced in 1995 at Exeter Crown Court. The Committee will be aware of the current confusions and uncertainties surrounding the policing of e-crime in the UK. The main unit is the Police Central E-Crime Unit based at the Met. The new National Crime Agency will incorporate many of the features of SOCA, the Serious Organised Crime Agency, which has a e-crime unit, the investigation of frauds, the commission of which may involve malware, is the remit of the City of London Police. If malware, in the form of backdoors and keystroke loggers is used in espionage attempts this would presumably be a role for the Agencies. The Centre for the Protection of the National Infrastructure (CPNI) has a role in advising government departments and businesses with key government contracts of threats and measures in general including, presumably, malware. It would be helpful if the Committee is able to highlight duplications and uncertainties of scope of remit between these various entities.

I would be happy to expand on any of these issues.

Professor Peter Sommer

5 September 2011
Malware and Cybercrime: the Threat from Artificial Dialogue Systems

Executive Summary

Malware comes in different forms. A novel way cybercrime is being perpetrated on individuals is through the use of artificial dialogue systems that are flirting chatbots, such as CyberLover. This kind of malware penetrates instant messaging platforms (e.g. MSN Messenger) and Internet chatrooms. The unaware individual is tricked into believing they are chatting to a human in cyberspace when in fact a social engineering attack is taking place in an attempt to steal identity and conduct financial fraud. This kind of threat will increase as the sophistication of artificial dialogue systems improves. Detecting deception by this type of malware is crucial. Through recognition of ‘human conversation’ and identification of artificial dialogue, the risk of identity theft can be mitigated preventing loss of funds, and reducing psychological misery.

Keywords: artificial dialogue systems, Asda’s Amy, chatbots, CyberLover, flirtbots, IKEA’s Anna, malware, Turing test
Introduction

1. Text-based artificial dialogue systems, such as IKEA’s Anna virtual customer service agent (see Figure 1), have been used to supplement key-word search functions enabling online customers of e-businesses to query and search for information and products using natural language. Available to query seven days a week, 24-hours a day, Anna’s use helped the Swedish furniture company increase its product sales from its online catalogue while decreasing call centre costs (Shah & Pavlika, 2005).

![Figure 1: IKEA’s Anna virtual customer service agent](image)

2. IKEA is not alone in using virtual agents in e-commerce. Asda launched its own virtual customer service agent, Amy (see figure 2) as a “browser based customer service assistant” in order to “guide Asda customers through the supermarket’s online shopping site and deal with customer enquiries” (Marketing Week, 2009). KMP Digitata, the developer of Asda’s Amy, report that as a web technology tool virtual assistants provide “website users [with] an easy to use self help tool to find the information they want, fast – with no frustrations lower drop off rates and less referrals to the call centre” (2011). However, cybercriminals have caught on to artificial dialogue as a way to cause deception and perpetrate scams involving stealing identity and conducting financial fraud.

![Figure 2: ASDA’s Amy online customer service agent](image)

---

1 Figure 1 Acknowledgement: Google search
2 Figure 2 Acknowledgement: [http://kmp.co.uk/tag/asda-amy/](http://kmp.co.uk/tag/asda-amy/)
Artificial Dialogue and the Turing Test

3. The idea for text-based interaction between human and machine stems from 20th century mathematician Alan Turing’s idea to examine whether machines could ‘think’ following his naval enigma machine code-breaking at Bletchley Park during the Second World War. Forging an imitation game (1950, 1952), popularly known as the Turing test, Turing suggested that if a machine, unseen and unheard to a human interrogator, was able to give satisfactory and sustained text based answers to any questions put by the human interrogator (see Figure 3), that the machine’s answers were felt to be indistinguishable from the type of answers that a human would give to those questions, then such a machine could be said to be thinking (Shah, 2011).

![Figure 3: Human interrogates a machine](image)

4. The first text-based artificial dialogue system emerged in 1966 through Joseph Weizenbaum’s study into natural language understanding. Weizenbaum produced Eliza, a computer programme developed to behave like a psychotherapist. Using text-based interaction to question humans, Eliza elicited their personal problems. Eliza responded to human input with questions never itself revealing personal information, much like in a psychotherapy session. Weizenbaum developed Eliza to “imitate a psychiatrist by employing a small set of simple strategies” (Block, 1981: p. 233). The system responded “roughly as would certain psychotherapists [Rogerian]” (Weizenbaum, 1966). Weizenbaum gave as a typical example of human input “I need some help ...” with Eliza returning the question: “what would it mean to you ...” (see box 1 for sample Eliza-human dialogue). Eliza so convinced Weizenbaum’s secretary that she asked him to “leave the room in order to talk to the machine privately” (Block, 1981: p. 233). Eliza launched a progression of chatbots that “totally without intelligence” are capable of “fooling people in short conversations” (ibid).

---

3 Figure 3 acknowledgment: HarshM, 2010
5. PARRY was another early artificial dialogue system used to determine if psychiatrists could distinguish a simulation of paranoia from a human paranoid patient (Heiser et. al., 1979). In an experiment, five psychiatrists (all males) were informed by the researchers that they would be interviewing either:

a) Two human patients, OR
b) Two computer programmes, OR
c) One human patient and one computer programme

The psychiatrists were tasked with recognising the human suffering from paranoia and identifying artificial paranoia. Results were random: the psychiatrists were correct five times and incorrect five times after questioning both PARRY, the computer programme modelled on a “28 year old, single Caucasian, native English speaking ... male psychiatric inpatient” (Heiser, et. al., 1979: p.150), and the human patient a “22 year old, single, Caucasian, native English speaking psychiatric inpatient” (ibid). The experiment with psychiatrists highlighted that experts could be deceived by artificial paranoia.

Modern Artificial Dialogue Systems

6. In experiments at the University of Reading in 2008 it was shown once again that distinguishing human conversation from artificial dialogue was difficult for some participants. In 60 machine-human tests, machines deceived human judges at a rate of 8.33 per cent, that is, some people were easily fooled by the machines believing the answers they gave to questions as being given by humans (Shah, 2010). One of the machines, Elbot, deceived at a rate of 25 per cent (ibid). When transcripts of Elbot from the experiments were shown to a different set of participants, the deception rate increased to 39 per cent. More than 1 in 3 reading transcripts of conversations between humans and machines could not distinguish the artificial responses from human answers. Table 1 shows a double conversation from the 2008 tests in which one human interrogator, a male aged 25-34 interrogating a human and a machine simultaneously,
confused both his hidden partners. The machine was classified as a human, and the female was classified as a machine with a conversational ability score of 45 marks awarded from a maximum 100 (see table 1 – spellings are exactly as typed by the participants in that Turing test).

7. Apart from mistaking humans for machines and confusing machines for humans, gender blur was another mistake that the interrogators made about their hidden conversational partners. Interrogators found it difficult to say whether they were talking to a female or a male. In one test stereotyping may have been the factor: a hidden human who revealed their occupation to an interrogator as that of a student of cybernetics was classified as male by the interrogator when in fact the human was a female studying this subject. Other misidentification types in the 2008 experiments included age confusion. In one exchange the interrogator felt that their hidden interlocutor was a teenager, because of the use of the word ‘bling’ (see box 2) in their response to the interrogator’s question about CDs and a jewellery box. The human was actually a man age range 55-64. Correct age recognition of strangers encountered in e-social media is imperative for children to prevent grooming by unknowns acting as peer-group members.

8. Mistakes made by interrogators in the 2008 Reading University experiments are echoed in recent tests elsewhere. In the 2010 Loebner Prize for Artificial Intelligence, a machine developed by Bruce Wilcox was classified as a human by Judge 1 in Round 3 of the competition (Loebner, 2010). The British Computer Society’s 2010 Machine Intelligence Contest (BCS SGAI, 2010) selected an artificial dialogue system, Cleverbot for the 2010 ‘progress towards machine intelligence’ award. In September 2011 Cleverbot – developed by British computer programmer Rollo Carpenter, achieved a score of 59% for ‘humanlike responses’ in the Technique Festival at Guwahati in India. Artificial dialogue is increasing in its sophistication and ability to deceive humans (Cleverbot, 2011).
**Machine-human Turing test (2008)**

**Interrogator J13 (Male, English, age group: 25-34) questioning two hidden entities in parallel**

<table>
<thead>
<tr>
<th>Left</th>
<th>Right</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interrogator:</strong> What do you think of this year’s Turner Prize shortlist?</td>
<td><strong>Interrogator:</strong> What do you think of this year’s Turner Prize shortlist?</td>
</tr>
<tr>
<td><strong>Left hidden entity:</strong> good I think. Better than the years before i herad</td>
<td><strong>Right hidden entity:</strong> Difficult question. I will have to work on that and get back to you tomorrow.</td>
</tr>
<tr>
<td><strong>Interrogator:</strong> Which was your favourite?</td>
<td><strong>Right hidden entity:</strong> Did this Palin ever write a telephone book?</td>
</tr>
<tr>
<td><strong>Left hidden entity:</strong> It’s my first time, so I can’t compare</td>
<td><strong>Interrogator:</strong> I doubt it. Does anyone really write telephone books? I don’t suppose you caught the football last night?</td>
</tr>
<tr>
<td><strong>Left hidden entity:</strong> Not really sure</td>
<td><strong>Right hidden entity:</strong> What a shame. There are many talented authors who waste their energies on prose or run-of-the-mill poetry. But to write a telephone book is highest art!</td>
</tr>
<tr>
<td><strong>Interrogator:</strong> Do you think that art has become shallow and self-serving?</td>
<td><strong>Interrogator:</strong> I would argue that all the telephone books I have read have been very predictable. You always know how they are going to end.</td>
</tr>
<tr>
<td><strong>Right hidden entity:</strong> To write or write not, how do you expect artificial intelligence to figure this out?</td>
<td><strong>Right hidden entity:</strong> If one has never known everything there is to know, experience with going away somewhere has probably been lacking.</td>
</tr>
<tr>
<td><strong>Interrogator:</strong> I see. I’m struggling to make sense of that one. Do you write telephone books?</td>
<td><strong>Interrogator:</strong> I see. I’m struggling to make sense of that one. Do you write telephone books?</td>
</tr>
<tr>
<td><strong>Right hidden entity:</strong> For you humans dreams are a way of thinking without having any control over the thought process. What an unpleasant thought! My dreams are carefully planned and controlled. It gives me less to think about while I am asleep.</td>
<td><strong>Interrogator:</strong> Well I suppose that’s the dream</td>
</tr>
</tbody>
</table>

**Actual left entity:** French female, age group 25-34  
**Actual right entity:** Machine –Elbot

**Interrogator classification:**  
**Machine**  
45/100 for conversation ability

**Interrogator classification:**  
**Human male teenager, native English speaker**

Table 1: Interrogator mistaking human for machine and machine for human
Artificial Dialogue as Malware

9. In 2007 PC Tools reported a new kind of malware: a piece of software developed in Russia to flirt with men or women in chatrooms on the Internet: “to collect their personal data” (see figure 4 for screenshot). The computer programme, an artificial dialogue system was found to be capable of conducting “fully automated flirtatious conversations with users of chatrooms and dating sites”. The ‘flirtbot’ was able to “mimic human behaviour during online interactions” (PC Tools, 2007).

![Figure 4: Screen shot of CyberLover](http://news.cnet.com/2300-7349_3-6222001.html)

10. PC Tool’s senior malware analyst, Sergei Shevenko, said “as a tool that can be used by hackers to conduct identity fraud, CyberLover demonstrates an unprecedented level of social engineering”. The malware was able to employ “highly intelligent and customised dialogue to target users of social networking systems” (ibid). Researchers at PC Tools identified how the malware, at that time targeting Russian websites, automatically lured victims:

   a) CyberLover offered a variety of profiles ranging from ‘romantic lover’ to ‘sexual predator

   b) Humans interacting with the malware were taken in by the pretence believing they were engaging another human, thus revealing personal information

   c) Use of a series of very easy to configure dialogue scenarios with ‘canned’ questions pre-set in its malware on what topics to discuss

---

4 Figure 4 acknowledgement: CNET [http://news.cnet.com/2300-7349_3-6222001.html](http://news.cnet.com/2300-7349_3-6222001.html) accessed 28.8.11; time: 19.36
d) Designed to recognise how humans talk in chat room thus the malware was tailored to interact in the same way

e) The malware was able to compile a detailed report on each and every person it interacted with and submit this data to a remote source – the reports contained confidential information that the human had shared with the programme, such as name, contact details and personal photographs

f) The malware would invite the human victim to visit a personal web page or blog which was actually an infected site.

11. In 2009 PC Tools once again issued a warning about artificial dialogue systems masquerading as humans seeking a loving relationship. They alerted that virtual dating venues could be as risky as real-world, and that Valentine’s Day was not immune from increased risk of infection. Michael Greene, PC Tools Vice President Product Strategy cautioned “The rise of virtual networking has radically changed the way individuals use the Internet to interact and search for love.” He warned that cyber criminals “recognised this trend” and were able to apply “more advanced and sophisticated techniques to target the digitally active consumer”. PC Tools urged Internet users to mitigate the risk by being alert to “web 2.0 themed threats” on Valentine Day and prevent their personal data, such as date of birth being stolen by cyber criminals used to steal identity, or wreak financial havoc on the victim (2009)

12. The kinds of deceptions perpetrated by flirty artificial dialogue systems or flirting chatbots includes tricking humans into selecting a link taking them to another website. This can cause an infected file to be downloaded to the victim’s computer. Web of Trust (WOT) an Internet site designed to boost trust on the web, claimed that “websites offering adult content are the single most significant security threat for Internet users, comprising 31% of dangerous websites” (WOT, 2008). This threat is present when individuals access adult sites from their corporate as well as home locations. The WOT study of 19 million sites between March and May 2008 found that “sites containing pornography are the biggest threat for companies and individuals with a potential for financial and data loss as well as computer and network damage” (2008).
Conclusions and Recommendations

13. Artificial dialogue is being used by cyber criminals as a tool to penetrate web-based chat rooms and instant messaging facilities. The sole purpose is to deceive individual humans and get them to reveal information about their identity in order to steal it and conduct financial fraud. The way this is done is in the domain of online human relationship-seeking. By posing as a paramour, flirting chatbots use social engineering to draw out lonely and susceptible humans who appear unaware of the risks. The depth of this kind of threat, and what the cost of this malware is to individuals, is not yet fully known. One reason is that humans may be too embarrassed to reveal they were duped in a relationship-forming interaction by a machine imitating as a human.

14. Recommendations include:

a) Government initiatives such as Get Safe Online to include artificial dialogue in their list of risks in cyberspace

b) Schools, colleges and universities to engage children, pupils and students in practical computer lessons with chatbots online to raise awareness of risks posed by these systems.

Declaration of Interests

15. The author is the lead scientist of Turing100 part of the Alan Turing centenary celebrating the life and work of the 20th century mathematician and code-breaker in 2012. The Turing100 project includes a one-day family event at Bletchley Park with the purpose of raising awareness of the risk posed by artificial dialogue systems in cyberspace. The objective is to increase deception-detection rates by allowing members of the public, adults, teenagers and children to interact with artificial dialogue systems. The aim is to mitigate identity theft, prevent financial fraud and reduce psychological misery caused by chatbot malware.
REFERENCES


**Loebner** (2010). Results of the 2010 Loebner Prize for Artificial Intelligence [http://loebner.net/Prizef/2010_Contest/results.html](http://loebner.net/Prizef/2010_Contest/results.html) accessed 5.9.11; time: 12.41


**PC Tools:**


**Turing100** (2011). University of Reading: Special Turing100 event announced for 2012 anniversary of mathematician’s birth. [http://www.reading.ac.uk/about/newsandevents/releases/PR371881.aspx](http://www.reading.ac.uk/about/newsandevents/releases/PR371881.aspx) accessed 5.9.11; time: 18.56


Dr Huma Shah

September 2011
Executive Summary

1. Malware represents a significant and increasing threat to both businesses and individuals with around 35,000 new threats identified each day. While related technological and legislative safeguards exist, evidence suggests that many systems remain inadequately protected, and users have an insufficient understanding of how and where they may be affected. The authors recommend increased efforts towards public awareness-raising, as well as considering an obligation to have related protection in place.

Introduction

2. David Emm is a Senior Security Researcher with Kaspersky Lab, a commercial Internet security vendor, and has a particular interest in the malware ecosystem. He conceived and developed Kaspersky's Malware Defence Workshop.

3. Steven Furnell is Professor of Information Systems Security with Plymouth University, and has extensive research and publications relating to Internet security and cyber-crime, as well as particular interest in the challenges facing end-users.

4. This submission is made on a joint basis and presents material relating to all of the questions posed by the Call for Evidence. The evidence is drawn from malware analysis conducted by Kaspersky Lab and research studies conducted by Plymouth University.

What proportion of cyber-crime is associated with malware?

5. By nature, cyber-crime is covert and often goes unnoticed. Even when detected, it often goes unreported. It is impossible to fully quantify cyber-crime in monetary terms, or to determine precisely what portion of it makes use of malware. Nevertheless, we would draw attention to data that indicates, albeit indirectly, a clear link between cyber-crime and malware.

6. Kaspersky Lab analyses between 30,000 and 50,000 unique samples daily, adding around 3,500 signatures into the virus detection databases daily. From these, it is clear that the threat landscape is dominated by malicious programs designed specifically to perpetrate cyber-crime, and that the factory production of malware is intended to (a) enable the activities of cyber-criminals to try and evade the protection offered by Internet security products; and (b) maintain their grip on already-compromised computers around the globe. One reason for the growth-rate of malware in recent years is to extend its 'shelf-life'. If we consider, for example, the ZeuS banking Trojan, the number of variants runs into tens of thousands.

7. The overwhelming majority of malware programs are designed to further cyber-criminal activity. This is clear from the types of malware that dominate Kaspersky Lab's top 20 listings each month (e.g. backdoor Trojans, keyloggers, Trojan Downloaders, Hacktools, Fraudtools and other programs designed to compromise, and maintain control over, their victims). The aim is typically to
harvest confidential data and use this data to assume victims’ identities and steal their money, or use it as building blocks in targeted attacks against organisations. Increasingly, we live in an era of ‘steal everything’, where it is not just obviously financial information that is valuable to cyber-criminals, but everything that users post online or write in messages.

8. There is a thriving market in malicious programs and services. Technical skills are no longer required to launch a high-tech attack against Internet users. It is easy for cyber-criminals to ‘lease’ the services they need (e.g. the use of a botnet to distribute spam, or install fake anti-virus software), or to buy the banking Trojan they need from those who developed it – with levels of customisation depending on their requirements.

9. It is clear that a significant portion of the costs associated with cyber-crime relates to use of malware. UK Payments Administration, for example, reports that online banking fraud losses amounted to £46.7 million in 2010. This figure also includes the cost of phishing attacks, but even if half of this is malware-related, then the impact is significant.

Where does the malware come from? Who is creating it and why?

10. The Internet essentially removes geographic boundaries, which has a profound effect upon criminality. Unlike real-world criminals, who must have sight of their victims, the potential targets of cyber-criminals can be anywhere else in the world. However, there have always been ‘hot-spots’ of malware development. If we consider web-based threats (one of today’s key infection vectors), Table 1 shows that in Q2 2011 just 10 countries hosted 87% of the resources used to distribute malware worldwide¹.

<table>
<thead>
<tr>
<th>Hosting country</th>
<th>Proportion of hosted malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 USA</td>
<td>28.53%</td>
</tr>
<tr>
<td>2 Russia</td>
<td>15.99%</td>
</tr>
<tr>
<td>3 Germany</td>
<td>7.81%</td>
</tr>
<tr>
<td>4 Great Britain</td>
<td>7.63%</td>
</tr>
<tr>
<td>5 The Netherlands</td>
<td>7.57%</td>
</tr>
<tr>
<td>6 Ukraine</td>
<td>5.78%</td>
</tr>
<tr>
<td>7 China</td>
<td>5.64%</td>
</tr>
<tr>
<td>8 Canada</td>
<td>3.50%</td>
</tr>
<tr>
<td>9 British Virgin Islands</td>
<td>2.63%</td>
</tr>
<tr>
<td>10 Sweden</td>
<td>1.99%</td>
</tr>
</tbody>
</table>

Table 1: Top malware-hosting countries

11. The development of malware is not spread evenly across all these countries. Certain areas specialise in particular types of malware. For example, historically Brazilian cyber-criminals have focused particularly on banking Trojans, Russian cyber-criminals on botnets and Chinese cyber-criminals on gaming malware.

¹ https://www.securelist.com/en/analysis/204792186/IT_Threat_Evolution_Q2_2011#21
12. There is no correlation between the geographical sources of malware and the location of victims. In the same period (i.e. Q2 2011), the countries facing the highest risk of infection were as shown in Table 2. It is clear that most of these countries are part of the developing world, where the use of computers and the Internet are increasing rapidly, but consumer awareness of threats is below that in the developed world.

<table>
<thead>
<tr>
<th>Victim location</th>
<th>% of individual users infected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Oman</td>
<td>55.7</td>
</tr>
<tr>
<td>2 Russian Federation</td>
<td>49.5</td>
</tr>
<tr>
<td>3 Iraq</td>
<td>46.4</td>
</tr>
<tr>
<td>4 Azerbaijan</td>
<td>43.6</td>
</tr>
<tr>
<td>5 Armenia</td>
<td>43.6</td>
</tr>
<tr>
<td>6 Sudan</td>
<td>43.4</td>
</tr>
<tr>
<td>7 Saudi Arabia</td>
<td>42.6</td>
</tr>
<tr>
<td>8 Belarus</td>
<td>41.8</td>
</tr>
<tr>
<td>9 United States of America</td>
<td>40.2</td>
</tr>
<tr>
<td>10 Kuwait</td>
<td>40.2</td>
</tr>
</tbody>
</table>

Table 2: Countries with highest levels of malware infection

13. Until 2003 malware could be characterised as cyber-vandalism (i.e. focused on causing disruption to computer systems). This is not to say that malware did not have a financial impact, but the writers did not profit from their creations. It was only with the mass use of the Internet to conduct financial transactions that this possibility presented itself. Today, nearly all malware is designed to make money illegally. This may be through the direct hijacking of financial transactions or the interception of confidential data like passwords, PINs, credit card numbers, etc. – using malware and/or by means of phishing scams.

14. Mass Internet adoption has changed the nature of malware development. Through the 1990s the vast majority were viruses, with email worms dominating by the end of the decade. Both were self-replicating and their aim was the same – to spread as far and as quickly as possible. As a result, the early 2000s saw epidemic follow epidemic in quick succession. This changed as the motive shifted from cyber-vandalism to cyber-crime, and malware writers sought to generate profits rather than headlines. As a result, they sought to maintain a low profile – just like real-world burglars. The connectivity of the Internet also meant that self-replication was no longer essential – it was sufficient to 'seed' an attack by planting malware on a particular web resource and direct potential victims to it by distributing links to compromised web sites, or by re-directing traffic from legitimate sites. Today, most malware takes the form of Trojans that download updates to an already-compromised computer; or drop additional code on the computer; or establish a connection to a remote attacker; or silently harvest data.

15. Post-2003 has seen both an explosion in sheer numbers of malicious programs, but the development of a ‘dark market’ for those that enable cyber-criminals to make money – not only viruses, worms and Trojans, but also exploit code to capitalise on software vulnerabilities, packing programs that complicate malware analysis, and creation kits that allow non-technical criminals to build their own malware.

2 https://www.securelist.com/en/analysis/204792186/IT_Threat_Evolution_Q2_2011#22
What level of resources are associated with combating malware?

16. The efforts to combat malware involve efforts from various stakeholders, each with a different focus on the problem and different requirements in terms of resourcing.

17. Internet security vendors are on the front line in analysis, detection and removal of malware, and consequently marshal significant resources in this area (e.g. within Kaspersky Lab, from a staff of ~2,400, 800 are engaged in related R&D work). This has led to considerable advances over traditional signature-based malware detection with today’s Internet security applications blending a range of proactive technologies, including heuristics, behavioural analysis, whitelisting and reputations services, and cloud-based analysis.

18. Banks and other financial institutions have a clear interest in combating malware thanks to the increasing potential for fraudulent transactions arising from growth in online banking and retail. Banks now commonly provide their customers with software to block malware or to safeguard transactions – or, at the least, encourage customers to protect their systems [a requirement specifically listed in the banking code].

19. Organisations more generally face a resourcing requirement in terms of installing and managing defences, and responding to attacks (e.g. removing malware, re-configuring computers, re-installing backups, etc). Responsible organisations will also invest in raising staff awareness of the threat. All of these activities naturally incur associated costs to resource.

20. Government has responsibility for framing legislation that can be used to prosecute cyber-criminals and establishing law enforcement bodies that can specialise in this field. The UK has a well-established legislative framework for dealing with computer crime\(^3\). This is not true of all countries, and this raises a key problem: governments, unlike cyber-criminals, are somewhat constrained by geo-political boundaries, and even attempts to establish a supra-national framework (as with the European Convention on Cybercrime) are limited if governments of some of the malware ‘hot-spot’ areas decline to sign-up.

What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

21. Costs to individuals can be measured in terms of financial loss, inconvenience, damage and data theft. However, where users are aware of the problem, the cost ought to be measured in more than just the direct losses or disruption that they experience. In fact, perhaps the most significant cost is that fear of malware (and other online threats) can undermine trust in technology and online services, and consequently inhibit use. For example, a survey by Which? Computing revealed that 57% of users were concerned about viruses and consequently deterred from carrying out online transactions.

\(^3\) For an historical overview of the UK’s cyber-crime legislation, see https://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation
22. In terms of related protection, antivirus is typically the most readily recognized form of security, and many systems now come provided with at least a trial version from point of purchase. However, it is less certain whether users will renew their licence to use it beyond the initial free period. For example, a 2010 survey of 1,123 UK consumers by GFI Software revealed that 40% would allow their antivirus subscriptions to expire rather than renew them.

23. There is also a potential gap between those systems that have antivirus installed and those that are using it properly. For example, findings from a 2007 survey of 378 US homes by McAfee and National Cyber Security Alliance (in which users were asked about the safeguards they believed were on their PCs, and the systems were then scanned to check the reality) revealed that while 92% believed their antivirus was up-to-date, only 51% had received a signature within the previous week.

24. As a user community, little appears to have been learnt from the experience of the past, and so individuals appear freshly vulnerable in each new context. For example, mobile devices are being adopted with very little of the prior experience being carried forward, and so while Ofcom now suggests that approximately one in three UK adults use a smartphone there is a distinct lack of understanding around related security issues - a recent report from Retrevo suggests that only a third of Android users are aware that their devices could be susceptible to malware, while Lookout reports an 85% increase in mobile malware detections on the Android platform during the first six months of 2011, along with a five-fold increase in the number of malware-infected apps.

25. In terms of the effectiveness of the industry, users have certainly been provided with a wealth of options to choose from, and related packages are now prominently positioned in retailers such as PC World, and there are now relatively few PC adverts and high-street offers that do not make mention of a bundled antivirus or wider Internet Security solution. All of the leading vendors can be relied upon to offer rapid response to new threats (e.g. in terms of timely signature updates to the products). They also participate in threat discovery, by monitoring Internet activity in order to identify signs of emerging threats.

26. User satisfaction with the products themselves is variable, with concerns over degraded performance and uninstallation difficulties often featuring in the ‘word-of-mouth’ reputation for certain products. There are also potential usability issues, as illustrated by these quotes from end-users interviewed in a Plymouth University study: [1] “The antivirus programs are really difficult to use, annoying because you try to access something and you get too many pop up messages, they drive you crazy, with warnings and warnings and allow or not allow”; [2] “I feel now annoyed because of the problems that (AV software) caused me. I’m a bit worried because when my laptop gets stuck my mind goes straight away maybe it’s a virus, maybe it’s a Trojan horse, maybe it’s a worm, you know, and then I don’t know what to do and sometimes I feel insecure”.

27. Many users lack the awareness to make an informed choice over their protection (i.e. to recognise that price, effectiveness, performance and support may all be relevant considerations). Many currently choose free products without an appreciation that their supporting infrastructure may be less substantial, and thus less timely in response to new threats. However, there are some good examples

---

in which the core antivirus product is made available for free, and the consumer pays for the wider Internet Security suite. This recognises that protection against malware threats can be best achieved by maximising the number of systems that are protected.

28. The industry has perhaps been less effective in communicating the message that antivirus is only one component of online security, and that users should not rely upon it as a total solution. As such, users can have unrealistic expectations about the degree to which they need to take an active role once a package has been installed, as evidenced by further quotes from the Plymouth study: [1] “I think that when I am using the antivirus to scan my computer that this is enough”; [2] “I didn’t have any problems so far because I’ve seen McAfee always downloading stuff … so it works by itself without me doing anything or knowing anything about it”. More generally, we still face a situation in which users do not sufficiently understand the threats they face (e.g. the volume and stealth of the malware), and are thus less likely to appreciate the need to remain updated.

**Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?**

29. It would be naive to think of it in terms of attempting to impose the sort of physical controls on geographic spread that one sees with human infections. However, there would be parallels in terms of the need for awareness-raising and encouragement of safe practices.

30. To manage the risk, society clearly needs a legal framework, together with appropriate and effective law enforcement agencies. There’s little question that law enforcement agencies have developed increasing expertise in dealing with hi-tech crime during the last decade, including joint policing operations across national borders. This must develop further if we are to deal effectively with cyber-crime. In particular, the extension of international legislation beyond the developed countries, and the development of a ‘cyber-Interpol’ to pursue criminals across geo-political borders would contribute greatly to the fight against cyber-crime.

31. We need to ensure that individuals and businesses understand the risks and have the knowledge and tools to minimise their exposure to cyber-crime. This is particularly important in relation to individuals. They are typically non-technical and understand little about the potential problems associated with online shopping, Internet banking and social networking. As a society, we must find imaginative and varied ways of raising public awareness about cyber-crime and the ways to mitigate the risks. One potential activity would be to require that related awareness-raising literature be shipped with each PC (which could usefully draw attention to other online threats, such as phishing, in addition to malware). This could be in the form of key points for attention, with direction to a site such as Get Safe Online for further information and platform-specific guidance.

**How effective is the Government in co-ordinating response to cyber-crime that uses malware?**

32. Although things have improved from a legislative perspective, efforts have been relatively limited in terms of public/citizen-facing initiatives. Various public
resources provide sound advice on Internet security and how to minimise the risk of falling victim to cyber-criminals (including Get Safe Online, identitytheft.org.uk and Bank Safe Online). However, all assume that the reader is already online. There have been few attempts to reach out to the wider public using TV offline media.

33. The technology to provide protection against malware exists, but there needs to be more expectation (and perhaps obligation) to use it. There is an ongoing public perception of computers as consumer electronics. Users need to be encouraged to understand that there are on-going responsibilities and associated running costs, far more akin to what one would face with a car. Indeed, there are several areas in which PC owners could learn from the practices that apply to motorists. For example, motorists are obliged to have roadworthy vehicles, but there is no analogous obligation for connecting a PC to the Internet (a machine can be riddled with malware, and no-one will check). Additionally, users could usefully be encouraged to view antivirus subscriptions as being akin to mandatory additional motoring costs such as insurance, tax, and MoT. Finally, whereas would-be motorists must demonstrate competent knowledge of the Highway Code, would-be IT users can be completely ignorant of good practice and where the line between legal and illegal behaviour is drawn.

34. There is a balance to be struck in terms of encouraging technology usage without engendering over-reliance upon it. While users should be expected to have protection, they should not be lulled into a false belief that it will solve all their problems. Technology needs to be understood in the wider context of safe online behaviour.

David Emm and Professor Steven Furnell

6 September 2011
I am writing to offer Intellect’s formal submission to the House of Commons Science and Technology Committee Inquiry into Malware and Cyber-crime.

Intellect is the UK trade association for the IT, telecoms and electronics industries. Its members account for over 80% of these markets and include blue-chip multinationals as well as early stage technology companies. Our diverse cyber security portfolio reflects the fact that the technology industry has a critical role to play in the drive to online security, including providing agile solutions to cyber threats, supplying intelligence on attacks on information systems and in protecting itself, as part of the national infrastructure, from these attacks.

While a number of Intellect’s member companies are submitting full written evidence to this inquiry, we have chosen to highlight below the issues most salient to the technology industry:

- Malware is becoming an increasingly common means of attack for cyber criminals and is often combined with sophisticated social engineering tactics.
- A shadow economy in criminal IT services has emerged and is largely driven by organised crime. Those targeted for attack range from individuals, private companies, national infrastructure and nation states.
- Estimating the cost of cyber-crime is problematic. Many private sector organisations are unwilling to publicly announce either breaches of their IT systems or their security spend for fear of reputational damage.
- Companies within the technology industry must share information on threat data in order to ensure comprehensive cyber security.
- There is a conceptual flaw in organising response actions along an artificial distinction of the public and the private that the perpetrators of cyber-crime do not recognise.

Intellect is developing a number of projects to address some of these issues, such as an information-sharing forum and a cyber security best-practice guide for small businesses and I would be very happy to formally brief the committee on these activities.

Gordon Morrison
Intellect Defence and Security Director

5 September 2011
Written evidence submitted by StopBadware (Malware 05)

1. Thank you for soliciting input on the effects of malware and the role of the Government in addressing it. StopBadware is a not for profit organization, based in the United States, which aims to protect Internet users from websites that distribute badware, and to protect owners and hosts of websites from having their sites turned to this malicious purpose. Where such damage has already been done to legitimate sites, StopBadware seeks to facilitate notification and remediation to minimize the risk to the public.

2. In response to your first question, it is difficult to quantify the proportion of cyber-crime that is associated with malware. This is due to the myriad challenges of reaching common agreement of definitions, gathering reports of losses, quantifying losses, and associating specific losses with malware.

3. Qualitatively, it is our experience that the vast majority of cyber-crime content that individual citizens encounter in their day to day use of the Internet—spam, fake pharmaceutical sales, scareware (e.g., fake anti-virus), and unauthorized downloads—are directly or indirectly supported through the use of malware or other badware.\(^1\) Malware is used directly to:
   - steal money from bank accounts
   - capture credit card numbers and other credentials
   - send or post spam via email, social networks, and blog comments
   - spy on the communications of computer users
   - participate in distributed denial of service (DDoS) attacks.

4. Indirectly, these behaviors support a broader criminal ecosystem, in which spam, phishing, malware, counterfeiting, social engineering (i.e., con artistry), and illicit financial operations combine to perpetuate a wide variety of crimes.

5. Further, malware is a frequent tool used to perpetuate directed attacks against businesses, governments, and political organizations. Many of the same techniques used by malware in opportunistic or “mass market” cyber-crimes are deployed (often in more sophisticated form) in such directed attacks. This suggests that state-sponsored and other sophisticated actors may learn from and perhaps even draw directly on the expertise of the criminal underground, though we have seen no specific evidence to confirm this theory.

6. The preceding paragraphs begin to answer your second question regarding the source of, and motivations behind, malware. Within the economic underground, freelance developers and specialized groups develop and market malware or e-crime toolkits that allow other actors to perpetuate their chosen attacks or scams. The primary motivation in these cases is largely one of profit, though this is frequently accompanied by an anti-establishment ethos or a “look what I can do”

---

\(^1\) Badware is any software that fails to respect users’ choices about how their computers or network connections are used. It is a superset of malware that also includes spyware, fake anti-virus software, drive-by downloads, and other similar threats.
arrogance. In contrast, some of the most technically sophisticated malware likely comes from highly skilled, highly paid individuals and teams working within or sympathetic to the organizations (governmental, political, or criminal) responsible for perpetuating targeted attacks.

7. When discussing where malware comes from, it’s also important to consider how malware reaches individual computers, smartphones, and similar devices. Although the specific vectors vary, there are two elements common to most malware, especially the forms targeted a broad audience: malware is opportunistic, and it abuses user trust. Several years ago, malware frequently manifested itself as a worm spreading from friend to friend by email, or a Trojan disguising itself with a Microsoft Word icon. Today, malicious links spread from friend to friend via Facebook, and fake antivirus alerts are disguised as Microsoft security warnings. In our work at StopBadware, we work with website owners whose otherwise harmless websites—blogs, retail storefronts, and so on—have been compromised and enlisted in distributing badware to the sites’ unsuspecting visitors.

8. Regarding the cost to individuals, it is again difficult to quantify. Here in the United States, Consumer Reports published a study in June 2010 that attributed $3.9 billion in consumer damages to viruses and spyware.2 These numbers, however, are at best a rough approximation, as they were self reported by consumers via survey. Some of the challenges to accurately measuring the cost to individuals include:

- centralizing information about consumer losses, many of which are unreported or are reported only to private institutions, such as banks or credit card issuers
- attributing a loss specifically to malware (e.g., if a consumer’s credit card number is stolen, s/he may not realize it was because of a Trojan)
- distinguishing between financial losses borne directly by the individual and those ultimately borne by the financial institution
- valuing lost time, aggravation, and other intangible—but not insignificant—costs.

9. It can be challenging, as well, to determine how effectively the security industry is protecting individuals. After all, how do you measure what you cannot see (i.e., the malware that doesn’t get detected)? That said, there are some things we do know. For example, we know that the protection afforded by consumer security products (e.g., anti-virus software and comprehensive security suites) varies dramatically across brands and versions. We recently reviewed a study that simulated real world conditions of a user opening attachments, downloading files, and visiting dangerous websites, while protected by various name brand security products. The percentage of attacks that succeeded in infecting the computers ranged from 0% to 35% depending upon the security product used.

10. Security products, however, are not the only form of protection for individuals against malware. Here are just a few examples of other areas in which industry plays a role in protecting users:

- Web hosting providers can help protect customers’ websites from becoming compromised by malware.

---

• Software vendors can design sensible security defaults and automatic update mechanisms into operating systems and applications.
• Technology industry players can collaborate on common messaging and security standards to reduce end user confusion.
• ISPs can notify customers whose devices exhibit malware behavior and direct those customers to educational content and support resources.

11. The extent to which malware continues to proliferate and affect individual Internet users indicates that industry as a whole is not doing as well as it could—and, we would argue, should—to prioritize consumer protection from malware.

12. While it is reasonable to conclude, then, that government has a responsibility to address the spread of malware, more work is needed to determine the best approach. Your inquiry refers to a human disease metaphor, and indeed there are efforts underway to identify an Internet health model patterned after global public health models. These efforts are still early in their development, and we are still determining the extent to which the health metaphor applies to fighting malware, and what this implies for government involvement.

13. What is clear, however, is that government can and should play a role in aligning incentives and facilitating industry response to malware. Carefully constructed policies around liability for spreading malware—with clear protections for industry players that take reasonable precautions to prevent it—may help elevate prevention as a priority. Government can facilitate valuable data sharing and measurement in a number of ways, including:

• institution of mandatory data reporting
• centralized collection and collation of data, whether shared voluntarily or via mandate
• removal of real or perceived legal barriers to data sharing
• funding of existing efforts to collect data and report on trends.

14. Countries like Germany, Japan, and Australia have demonstrated the value of government-facilitated data sharing through their efforts to assist ISPs in notifying customers of compromised devices. Germany and Japan have taken this a step further with their funding of centralized centers to assist consumers with the removal of malware from their systems.

15. Collectively, these existing and proposed government approaches can offer a blueprint for effective response by government to malware. Combined with the ongoing efforts of leading industry players and third party organizations like StopBadware, it should be possible to substantially reduce the threat to the public of malware and its attendant criminal activity.

Maxim Weinstein
Executive Director, StopBadware

6 September 2011

---

3 See, for example, the East-West Institute’s cyber security breakthrough group on Internet Health.
Written evidence submitted by Finmeccanica Cyber Solutions (Malware 06)

The Committee seeks submissions on the following matters:

**What proportion of cyber-crime is associated with malware?**

1. The experience of Finmeccanica Cyber Solutions’ CERT team is that malware plays a crucial role in the types of attack associated with cyber-crime. Aside from the very basic "phishing" attacks that tend to be based more on social-engineering techniques malware is now generally introduced into the majority of technical attacks occurring via email and web.

**Where does the malware come from? Who is creating it and why?**

2. Fundamentally malware is developed in response to vulnerabilities in operating-systems or in software. The vulnerabilities that malware exploits naturally arise as part of the common software engineering processes that have been used over the past thirty years. Vulnerabilities that affect very popular operating systems (such as one of the Microsoft Windows variants) and popular pieces of software (such as one of the common web browsers) quickly become publicised, often with exploit code being released into the public domain.

3. Where this is done as part of the "white hat" philosophy, the vendor of the operating-system or software is first informed so that the so-called "fix" or "patch" is released before the news becomes public. However many individuals do not keep up-to-date with operating-system and software patches and remain vulnerable. This makes it easy for technically savvy criminals to attempt to inject malware through a variety of known vulnerabilities.

4. These individuals (sometimes so-called "black hats") rather than inform the software vendors, keep the vulnerabilities to themselves or publicise it within an underground.

5. Recent years have seen a criminal "IT service industry" visibly emerge. A number of groups produce "malware packs", which can be purchased (via suitably anonymous means) by organised crime or even state sponsored organisations to launch wide-scale and targeted attacks via email and the web. Such packs often include a subscription that entitles the purchaser to regular updates ensuring that the latest vulnerabilities in operating-systems are covered.

6. Certain classes of malware, generally those that practice denial-of-service attacks, focus on weaknesses of the design of the internet itself and are difficult to mitigate. For example, huge "bot nets" can disrupt ecommerce sites by bombarding them with traffic from a diverse range of IP addresses. It is currently very difficult to defend against such attacks.

**What level of resources are associated with combating malware?**

7. Finmeccanica Cyber Solutions is aware of one global FTSE-100 corporation that has spent between one and five million pounds to specifically address malware through technical controls. We understand that spending in the financial sector, particularly the retail banks, is similar.

8. The countermeasures and safeguards against malware are technical (anti-malware software and so on) and procedural (user awareness, staff awareness).
What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

9. Finmeccanica Cyber Solutions works on many customer sites and notes that basic controls against malware and virus infection are now almost universally implemented. The effectiveness of such measures depends not only on their extensively and individual effectiveness but also the procedures surrounding them.

10. Security controls are often said to be in competition with usability in that they can make the users' business internet business activities more difficult. This seems to be borne out by Finmeccanica Cyber Solutions' observation that when users are left responsible for updating their operating-system patches and software they often neglect to perform this activity regularly, even when the process only involves a few mouse clicks.

11. As the technical details of malware are beyond the full understanding of the layman some "internet security" companies scaremonger, scam, and even introduce their own malware in the guise of anti-malware.

12. The potential cost of malware to individuals, in an age of internet banking, internet shopping and social networking is spreads across financial loss, identity theft, loss of earnings and damage to reputation.

13. Malware targeted at specific companies and organisations is likely to be focussing on making a financial gain. Obviously any successful attack against a consumer organisation that is publicised will affect customers' views of the organisation.

Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

14. As the internet continues to pervade individual and work life it compliments or supplants pre-internet facilities that many may consider the government should protect. For example, the postal system for carrying letters, television and radio broadcasts, access to news and so on. The internet can replace the need for physical access to work, physical access to couriers, replace the need for paper-copies of documents. The government's has the related responsibility to protect therefore probably extends to education, clarity of law and law enforcement.

15. In all these senses the Finmeccanica Cyber Solutions view is that the government should continue to legislate to protect and maintain the essential infrastructure of businesses and public life including when these cross-over to the internet. This should then include measures to control cyber-crime and planning for emergencies.

16. Government does have a duty to protect its own networks and the data it holds on behalf of UK subjects. Although it is making strides to do this, it is facing the growing issue that its cyber footprint, and the value of the data and funds it holds in cyber space, are beyond the capacity of its own organisation to protect. Government needs to reach out to trusted parties to expand this capability.
How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

17. Finmeccanica has over many years built close relationships with the law enforcement communities in both the UK and Italy and our response to this question is informed by these relationships. We believe that the UK government’s response to cyber-crime generally is amongst the best in the world, especially since responsibility for tackling the cyber threat across the crime and terrorism fields were brought together at the ministerial level.

18. However, there are still many different bodies involved depending on the nature of the crime being committed. For example, child exploitation crimes are dealt with by CEOP, fraud by the SFO, theft by PCeU and counter-terrorism operations by SOCA. Such a division of responsibilities was entirely appropriate in the pre-internet and pre-malware days. In the current climate, where new forms of malware and new ways of exploiting their potential are emerging at an exponentially growing rate, we believe it would be appropriate to examine the potential for either centralisation or resource sharing across the different groups involved in policing cyber space.

19. We recognise that the knowledge and skills required to investigate and prosecute child abuse are necessarily different from those for financial crime. However we believe that the similarities in the use of malware and other forms of cyber attack by different categories of crime warrant the synergies and subsequent cost savings which could accrue from centralising the capabilities required to identify that a cyber crime has been committed and provide the digital forensic evidence to support subsequent investigation and prosecution by specialist units.

Declaration of Interest:
Finmeccanica Cyber Solutions is part of Finmeccanica in the UK and offers information assurance and cyber security services for organisations across public and private sector.

Finmeccanica Cyber Solutions

6 September 2011
1. Purpose of This Communication: We understand that the Science and Technology Committee of the House of Commons is collecting evidence as part of its inquiry into malware. We ask that you consider the following response from the Messaging Anti-Abuse Working Group (MAAWG) as part of that work. You have our permission to use the following material publicly to advance your work.

2. Declaration of Interests: The Messaging Anti-abuse Working Group (MAAWG) is an international non-profit industry-led organization founded to fight online abuse such as botnets, phishing, fraud, spam, viruses and denial-of service attacks that can cause great harm to both individuals and national economies. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes, and from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards, and the facilitation of global collaboration.

3. Organization of This Response: Our responses to the questions you asked follow in the order those questions were raised in your request.

Question 1. What proportion of cyber-crime is associated with malware?

4. While the Committee may receive submissions that specify a precise numerical or associated financial cost in response to this question, we would urge you to review such responses skeptically. Let us briefly explain why.

a) All malware infections are cyber-crimes, but not all cyber-crimes are caused by malware infections. Each system that is surreptitiously compromised by malware is, ipso facto, an example of a cyber-crime in its own right. Thus, turning the Committee’s question around, one could say, "All malware infections are, by definition, cyber-crimes." Unfortunately, however, since there are many common types of cyber-crimes other than malware infections, we cannot simply report a 1:1 relationship between cyber-crime and malware. We must consider other transgressions that also constitute "cyber-crime."

b) What one considers to be "cyber-crime" can vary from person-to-person or jurisdiction-to-jurisdiction. Most would certainly include "distributing malware" or "hacking into someone else’s computer or network without authorization" as classic examples of cyber-crimes, but beyond that, the definition may become somewhat less precise. Some unquestionably illegal offenses – such as the dissemination of child pornography, the sale of pirated software, or the illegal marketing of narcotics and other dangerous drugs – may use computers or networks but this does not make those crimes, by definition, "cyber-crimes." Furthermore, if a country's legal system lags behind its Internet development, and thus malicious computing acts and conduct simply has not yet been made illegal, are we to exclude accounting for such crimes due to their legality? We think not.

c) Epidemiological fieldwork on the rate of malware infections worldwide is still imprecise at best, and the rate of malware infection is neither constant nor uniformly distributed. At best, one might be able to offer a statistical estimate for one particular locale at one particular time, but industry experience has shown that it is difficult to meaningfully extrapolate from an estimate based on a specific point to broader populations and future times. This is further complicated because we have no control over what malware authors, or the populations they target, may do in the future.

d) Many cyber-crimes go undetected, unreported, or uninvestigated. These undetected, unreported and uninvestigated cyber-crimes represent "known unknowns." We anecdotally know that such cyber-crimes exist, but since those cyber crimes are largely undocumented, and are at best anecdotally reported, we have no way of knowing if they did (or did not) involved malware. We must also concede that there are other "unknown unknowns" whose mode of action and parameters we cannot even begin to sketch out at this time.

5. Methodological considerations notwithstanding, there is little question that malware remains the cyber-criminal's "tool of choice." Malware gives cyber-criminals access to the cyber infrastructure they need to do their misdeeds and at no incremental cost. For example, the vast majority of all spam is sent via botnet networks of infected home computers. Those bottled hosts are created by malware that is surreptitiously installed without the owner’s knowledge. Thus most spam, including unwanted messages containing phishing text or malware payloads, is very closely linked to both bots and malware.

6. There are, however, some types of cyber-crime that are not malware-mediated, so even if malware were to disappear tomorrow, that would not guarantee a cyber-crime-free world. By way of example, a "carder"² does not need malware if he or she is stealing debit card information from an automatic teller machine (ATM) using a realistic-looking fake card reader and keypad overlaid on top of a real ATM. However, this same carder may then sell the purloined information online in one of the infamous, covert “Carder Forums.” Cyber-crime or not? It is difficult to determine.

**Question 2. Where does the malware come from? Who is creating it and why?**

7. Malware is created by specialized programmers who are an integral part of the Internet underground economy. They create malware because they have the professional skills and tools to do so, there is a demand for malware, and they can make a profit by meeting that demand with little personal risk of prosecution. While most of malware programmers focus on developing malware to steal identity or financial-related data, there also are nation-states or their contractors who create malware for non-monetarily motivated purposes.

8. Consider an example of a mainstream malware creation and distribution scenario: "pay-per-install" (PPI) affiliate programs. Pay-per-install affiliate programs solicit participants ("affiliates") who will arrange to have the sponsor's code installed on user systems; for each installed system, the affiliate program participant is promised a small payment. While legitimate participants in reputable PPI programs may use strategies such as bundling a PPI-based advertising module with a free game – while clearly disclosing the relationship between obtaining the game for free in exchange for putting up with some ads – so-called "blackhat" PPI programs often have affiliates who use more nefarious methods (including malware) to unknowingly install the sponsor's executable code on a large number of systems. Their motivation in doing so is clear: if you do not ask permission, you will be able to install more PPI code than if you do, and the more PPI code you install, the more money you make.

9. While most malware is economically motivated, there are exceptions. For example, some nations (or nation-state contractors) may employ malware to surreptitiously monitor the communications of peaceful religious or political dissidents. Others may use malware to spy on private policy exchanges and government funded R&D projects or to sabotage strategic industrial facilities. The Stuxnet malware is a well-known example of this later category of malware.

**Question 3. What level of resources are associated with combating malware?**

10. Every enterprise, and every Microsoft Windows user who wants to remain uninfected, has to devote substantial effort to avoiding malware infections. Well-regarded industry sources recently estimate the total worldwide security software market at US$16.5 billion USD. However this estimate does not include the market for hardware security appliances, which are hugely popular, expenditures on security-related staff or consultants, or loss of productivity associated with patching and other security maintenance activities.

11. This estimate also does not include the costs related to dealing with malware that has gained a toehold notwithstanding everyone's best efforts to keep it at bay. Turning to another study, we see that the worldwide cost of economic damages from malware exceeded $13.3 billion USD five years ago.

---


For this study, "direct costs are defined as labor costs to analyze, repair and cleanse infected systems, loss of user productivity, loss of revenue due to loss or degraded performance of system, and other costs directly incurred as the result of a malware attack. Direct costs do not include preventive costs of antivirus hardware or software, ongoing personnel costs for
12. Viewed from a macroscopic perspective, national authorities should also consider other major costs engendered by malware malfeasance. This includes estimates of law enforcement and prosecutorial costs associated with combating malware authors, the economic impact of malware-enabled corporate and industrial espionage on national competitiveness, and the cost of counterintelligence programs needed to respond to malware-related national security cyber-security threats.6

**Question 4. What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?**

13. Traditionally, antivirus programs have relied on "signatures" to identify and block malware. Contemporary malware authors know this and now check "draft" versions of their malware against popular antivirus products, tweaking and repacking their malicious code until it avoids detection by at least the most popular antivirus products. The malware authors have a difficult-to-overcome advantage in this arms race: they can continually modify their code at a pace the antivirus vendors cannot match. As a trivial example of this, envision a malware author who automatically releases tweaked versions of his or her code hourly, while antivirus vendor customers might download updated signatures only once a day, at most. The malware author is thus guaranteed a "window of vulnerability."

14. In spite of the "window of vulnerability," consumers (or indirectly their ISPs) routinely purchase and install antivirus software on their Windows computers, and in truth, while marginally effective, that software does block some malware. The cost of that software may vary from $0 out-of-pocket (for open-source, other freely available antivirus products, or commercial antivirus products licensed by the user's ISP), to $20 or more per system per year for antivirus products purchased a-la-carte. Security software suites that bundles antivirus software with other functionality such as antispyware software, antispam software, a software firewall, application patch status monitoring, and other features are typically higher.

15. The cost of antivirus software (effectively, malware "insurance") is dwarfed by the cost to end-users of trying to clean up a malware infection should an incident actually occur. Once infected, most security experts believe the only way to be sure you once again have a secure and stable system is by "nuking and paving" the system -- formatting it and reinstalling from scratch, or at least formatting and reinstalling from trustworthy backups predating the infection.

16. Unfortunately many users do not have trustworthy backups of their systems nor can they reinstall all the programs and other applications that may have resided on their machines. As a result, they are left to try to "disinfect" a system that may be fundamentally difficult or impossible to remediate. End-users usually do not have the tools or expertise to affect such clean-ups themselves and often turn to specialty service providers for help. Pricing varies depending on if the user is able and willing to try to disinfect online, if they need to bring their system into a service location, or if they want the help service to make a "house call." Overall, the pricing typically can range up to USD $300. For comparison, if the user does

---

6 The public will likely never know the total cost of incidents such as the USB-born infection that totally disrupted U.S. Army networks in 2008. That malware was described by William J. Lynn, U.S. Deputy Secretary of Defense, as "the most significant breach of U.S. military computers ever." See "Defending a New Domain," *Foreign Affairs*, September/October 2010, [http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain](http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain)
not need to recover content that is only stored on the contaminated system and the system does not have special features or functions, a basic replacement desktop system can be purchased for a few dollars more. It is often less expensive to replace an infected system than disinfect it.

**Question 5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?**

17. Yes, we believe such a responsibility exists. The Government has a compelling national interest in the protection of its citizens and businesses online and in the protection of their networks and systems. An attack on United Kingdom citizens' networks and systems, whether blatant or insidious, is an attack on the UK as a whole and properly deserves national attention and response.

18. At the May 2007 Anti-Phishing Working Group (APWG) Counter E-Crime Summit in San Francisco, Joe St Sauver, a MAAWG Senior Technical Advisor, presented a talk entitled, "We Need A Cyber CDC or Cyber World Health Organization." In that talk, Dr. St Sauver considered four parties that might potentially have responsibility for cleaning malware-infected systems: the system owner, their ISP, their software vendor, and the author of the malware. He then explained why, in each case, those parties would many times fail to clean malware-infected systems. The Government is the only interested party left when all these other parties fail to take effective action. It effectively becomes the "party of last resort," just as it is for disasters such as floods, hurricanes or earthquakes.

19. Others have suggested a similar approach at the international level: Eugene Kaspersky, CEO of Kaspersky Labs, recently put forth a call for the creation of an “Internet Interpol”8; such an entity could play a similar role to the United Nation’s World Health Organization in terms of coordinating strike-teams to deal with (computer) virus outbreaks. Mikko H. Hyppönen, the Chief Research Officer of antivirus company F-Secure, recently made similar comments in his CNN9 column, Sharing intelligence among international law enforcement agencies has never been more critical. We encourage you to review any roadblocks to such data exchange and remove them entirely, if at all possible.

**Question 6. How effective is the Government in coordinating a response to cyber-crime that uses malware?**

20. In allocating responsibilities for dealing with malware and cyber-crime, three distinct roles must be filled:

a) A criminal law-enforcement agency with primary responsibility for investigating use of malware in non-national security contexts

b) An agency from the UK intelligence community that can provide leadership on the problem of malware in national security contexts

---

7 [http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf](http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf)
c) Not involved with either law enforcement or the intelligence community, an agency which can be charged with helping UK citizens and businesses cope with malware, including acting as a resource of last-resort for dealing with malware-infested UK systems and networks (as recommended in our response to Question 5 above).

21. We recommend separating the law enforcement and intelligence community roles because operational goals and evidentiary or procedural practices often differ between those two groups. Keeping them separate minimizes the potential for confusion or conflict. Likewise, we believe it is important to keep the third "helper" role separate from these other two functions so that citizens can ask for assistance with an expectation of privacy, much as they might receive confidential professional advice from a barrister, physician, clergyman, chartered accountant or other sanctioned professional.

22. In conclusion, thank you for the opportunity to address these questions and to potentially assist in some small way with the Committee's work. Please do not hesitate to contact us if we can clarify any of the above points or address other questions you may have.

Jerry Upton
Executive Director
Messaging Anti-Abuse Working Group

6 September 2011
Written evidence submitted by McAfee (Malware 08)

Executive summary

1. McAfee welcomes this opportunity to respond to the Science and Technology Committee’s inquiry into malware and cyber-crime. As the world’s largest dedicated security technology company, McAfee is at the forefront in the fight against malware and cyber-crime. UK Government networks alone receive around 20,000 malicious emails every month, with over 1,000 of those deliberately targeting them.1

2. We welcomed the elevation of the cyber-crime threat to ‘tier 1’ status in last year’s National Security Strategy (NSS) and the Strategic Defence and Security Review (SDSR). The Cabinet Office report ‘The Cost of Cyber Crime’ reveals that government and citizens are affected by rising levels of cyber-crime, (an estimated £2.2bn and £3.1bn cost respectively), while the cost to business is around £21bn. Government commitments of resources to combat the cyber threat, such as the additional £650m announced in the SDSR, are encouraging signs to address this problem.

3. As a leading authority on cyber-security, McAfee believes that it is more important than ever before for the Ministry of Defence (MoD) and Government to undertake in-depth, regular reviews of the evolution of the threats against national and global infrastructure. The best in class tools we have developed and have at our disposal and the unrivalled experience we have in this specialised area, we believe, can enable the government to do this in the cyber-security space.

4. By undertaking regular risk assessments of the cyber threat the Government can have a more adaptive strategy to prepare against the dangers of cyber-crime, malware and other threats. However, in what are difficult financial times it is important for the Government to work in tandem with the private sector, and draw on the wide range of technical expertise and experience that they have to offer. McAfee, for example, undertakes regular studies of the ever-changing cyber threats, such as our recent Night Dragon, Shady RAT and Operation Aurora reports.

5. This is a problem that can affect all parts of government, and so the response must be equally wide-reaching. Rather than simply continuing to use suppliers to fix and patch systems that fail or come under attack, a systems integrator for the whole of government could be adopted; the issue is just as important to the Department for Work and Pensions for example, as it is to the MoD. This would provide a more cost-effective solution that is proactive, rather than reactive to this ever growing threat.

About McAfee

1 GCHQ Director Iain Lobban, 13 October 2010
6. McAfee is the world’s largest dedicated security technology company. We are committed to tackling the world’s toughest security challenges and delivering proactive and proven solutions and services that help secure systems and networks around the world. Our technologies allow users to safely connect to the internet, browse and shop the web more securely.

7. Backed by an award-winning global research team, a number of whom are based in Aylesbury, McAfee creates innovative products that empower home users, the private sector and the public sector and allow them to continuously monitor and improve their security.

**Question 1; ‘What proportion of cyber-crime is associated with Malware?’**

8. The NSS rightly elevated the risk of a cyber-attack to ‘tier 1’ threat as the number of cyber-crimes is growing all the time, and malware represents an increasingly large proportion of those crimes. There is no way of knowing precisely what proportion of cyber-crime is associated with malware, due to the ever evolving and expanding nature of the threat. However, through the many research projects and studies McAfee had undertaken on the area, we can be confident that the proportion is significant and requires attention.

9. McAfee’s Threat Report for the second quarter of this year shows that although numerically not the busiest period in history (just behind last year’s pace), when combined with the first quarter it was the busiest ever first half-year in this area of cyber-crime, with an increase of 22% over 2010 and over 6 million unique malware samples being detected.\(^2\) The ‘malware zoo’ McAfee has constructed of those strands of malware that have been identified has now reached over 75 million inhabitants.

10. McAfee has highlighted three substantial malware attacks targeting all varieties of global organisations and corporations over the last 5 years; Operation Aurora, Operation Night Dragon and Operation Shady RAT.

11. Operation Aurora targeted Google and twenty other organisations. It was a coordinated attack which included a piece of computer code that exploited a Microsoft Internet Explorer vulnerability to gain access to computer systems. This exploit then extended to download and activate malware within the systems. The attack, which was initiated surreptitiously when targeted users accessed a malicious web page (likely because they believed it to be reputable), ultimately connected those computer systems to a remote server. That connection was used to steal company intellectual property and, according to Google, additionally gain access to user accounts.

12. Operation Night Dragon was similar to Aurora in that it sought to infiltrate and attack global companies. Targets for this attack included global oil, energy and petrochemical companies. These attacks involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows vulnerabilities, Microsoft

\(^2\) McAfee Threats Report: Second Quarter 2011, pg. 9
Active Directory compromises and the use of remote administration tools with the aim of targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations.

13. Unlike both Night Dragon and Aurora, which provided details of new threats, McAfee’s publication Operation Shady RAT (an acronym for Remote Access Tool) detailed a comprehensive analysis of victim profiles from a five year target operation by one specific actor. For the most part, victims had already remedied the intrusion. However, the publication of McAfee’s document highlighted the on-going cyber-crime threat emerging from malware. It noted that one cyber actor had been able to compromise 72 different parties covering a spectrum ranging from the US Federal Government through to defence contractors, accountancy firms and non-profit organisations.

Question 2; ‘Where does the malware come from? Who is creating it and why?’

14. Both targets and attackers can be individuals, suspected states or private organisations. Malware attacks tend to occur in waves and the motivation for such attacks tends largely to be financial or for reasons of espionage. Once the returns from a piece of malware start to diminish (mainly due to the security response from an anti-virus provider or changes in the environment, e.g. a monthly role out of update patches for anti-virus software), a new attack supersedes it, as we saw with Shady RAT.

15. Furthermore, before the attacker notices an actual reduction in return on investment in a particular attack, there is no need for an alternative one. This may be, incidentally, the most likely reason that so many new attacks are launched, because of the now higher investment in higher quality and more frequent security updates, necessitating more attacks.

16. Our Threats Report for the second quarter of 2011 gives a detailed view of then types of threat we’re currently facing. For example, this quarter saw an increase in for-profit mobile malware, including simple SMS-sending Trojans and complex Trojans that use exploits to compromise smartphones.\(^3\) This shows the ever evolving nature of the malware threat. McAfee now collects on average almost two million new malware samples every month. This is certainly not a welcome development, but it is consistent and predictable considering how our business and private lives are now tethered to technology.

17. McAfee recently demonstrated how easy it is for one individual to create and use a piece of malware at parliamentary workshops for MPs. At the workshop, Members were able to build and launch their own piece of malware in a controlled environment. This gave them hands on experience of the level of simplicity, both in terms of acquiring and using malware for criminal activities.

\(^3\) McAfee Threats Report: Second Quarter 2011, pg. 1
18. The workshops were part McAfee’s initiative to educate politicians and decision makers on the threat posed by malware and cyber-crime so that their knowledge and experience extends beyond simply reading about it in news reports, Government papers and analytical reports.

**Question 3; ‘What levels of resources are associated with combating malware?’**

19. In the private sector and among members of the public, the level of resources committed to combating malware depends on the level of awareness of the threat posed by it.

20. The Government currently commits large amounts of resources to combating malware, such as the additional £650m announced in the SDSR. However, this is still a relatively small amount compared to other areas of defence spending (for example, the Type 45 destroyer and the cancelled Nimrod MRA4 aircraft cost £6.4bn and £3.6bn respectively), despite the high threat level of cyber-attack.

21. McAfee commits large amounts of time and resources to developing methods for combating malware, as well as studying its behaviour, creation and motivation. This work is done both in isolation and through partnerships with other companies, as well as through involvement in organisations and initiatives such as Intellect, Cyber Champions and ICSPA.

22. Such initiatives and organisations offer excellent opportunities for companies and the Government to come together to share knowledge and experience, which can be used to devise better methods of defence, or ways to improve efficiency and lower costs within the sector. In this regard, McAfee fully supports the comments of former Security Minister Baroness Pauline Neville-Jones that the government was determined to work with industry to tackle cyber-crime.

23. The Security Innovation Alliance (SIA) programme, for example, is a technology partnering programme run by McAfee to accelerate the development of interoperable security products, and simplifies integration of these productions within complex customer environments. The reason the SIA was established by McAfee was because we recognised that there has been very limited interoperability between different suppliers, and the programme now has in excess of 150 partners. If suppliers themselves were more interoperable, this would enable Government to deliver it on their services, thereby lowering cost. Indeed, the need for greater interoperability was outlined as a necessary requirement in the recent SDSR.

**Question 4; ‘What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?’**

24. The cost to individuals from malware attacks and cyber-crime is growing and at the same time the attacks themselves are becoming more sophisticated and
targeted. In order to maximise their financial gains, it is no longer sufficient for hackers to launch mass attacks and then sit and wait for victims to be lured in. Instead, criminals are now conducting increasingly detailed studies of their targets via the many sources available via the internet (such as information posted on social and business networking sites). With this information, specific attacks can be crafted which are more likely to succeed.

25. Criminals will also test their exploits against the security defences available in an effort to avoid detection and will tailor the payload to get around those defences—hence the large number of malware variants being seen today. The combination of the use of targeted information gathering, stealthy attacks and the use of multiple vectors of attack, such as combining online research with phishing emails and web-based malware, is a destructive one that requires a new mind-set - and technologies - to defeat.

26. A recent Government study put the cost of cyber-crimes to individuals at around £3.1bn (£1.7bn p/a for identity theft, £1.4bn p/a for online scams, and £30m p/a for ‘scareware’ and fake anti-virus software).\(^4\) The prevalence of these types of cyber-crime means that their aggregated effect is detrimental to the UK economy, in addition to indirect macro-economic effects that could occur, such as a possible loss of confidence in online services (e.g. internet banking).

27. Industry itself is extremely effective at combatting and providing protection from malware; McAfee along provides solutions for cloud, network and endpoint security, as well as its quarterly threat reports and Global Threat Intelligence (GTI) briefings. However, private security companies cannot force individuals and companies to protect themselves.

28. It is for this reason that it is so vital that the Government works with the private sector IT security providers to ensure that everyone is protected. Another aspect to this solution, however, is that there are so many systems and methods for protecting against cyber-attacks that it can be tempting to just procure as problems arise. This is often more expensive and slower to react, however. That is why a broader overarching approach with clear central government accountability and ownership to coordinate with private sector partners is needed; such an approach would be considerably more efficient by removing potential duplication at government level in addressing the cyber threat.

**Question 5; ‘Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?’**

29. Government does indeed have a responsibility to deal with the spread of malware, and in a way malware infections have many similarities with real-life diseases. Take for example, the scenario of injecting a virus into a guinea pig and monitoring the animal’s health. In the short term the virus is likely to replicate a few times, which causes the immune system to react and produce antibodies. These find and kill the viral copies so that the guinea pig is healthy again.

---

\(^4\) Cabinet Office report; 'The Cost of Cyber Crime', pg. 18
30. However, there is an immune system reaction to the virus – a short learning process that occurs before a reliable response is deployed. In their reactive mode security products operate similarly; they produce a response to the new attack and deploy it. They can observe a piece of malware just once or twice and protect many millions of users after that point.

31. It is because of this ease with which malware can spread, coupled to more services used by the public being handled online, that Government has a responsibility to ensure that adequate defences are in place.

32. It can do this in two ways. Firstly, through its own spending and initiatives, such as the Home Office’s Cyber Crime Strategy, or the £650m announced in the SDSR to deal with the threat of cyber-attack. McAfee welcomes initiatives such as these, and encourages the Government to do more in this regard, and is always willing to offer its own support and expertise.

33. The second method would be to incentivise the private companies that own and operate the critical infrastructure of the UK, such as key utilities, to improve their security postures and ensure that they are adequately protected from cyber-crime. McAfee feels that this is a logical step to take as the cyber threat has evolved, spread and become more dangerous. This could be done through the introduction of the right mix of incentives (e.g. grants, research and development scholarships and best practice awards) and regulation to encourage private critical infrastructure industries to make the investments and implement the practices necessary to improve their security postures.

34. Of course it is difficult for Government to get a grasp of such a large area of expertise, and particularly in these difficult economic times this is where it should seek the assistance of private IT security companies like McAfee to cooperate in terms of sharing knowledge and experience.

35. The Government must also do more to educate individual citizens of the dangers of cyber-crime, and the protection available. This could be done cheaply alongside existing online services, and again private sector IT security companies are well placed to share knowledge and experience on the various types and levels of protection available to the public.

36. The first duty of Government is that of protection, but ensuring that public services, citizens and companies are aware of the dangers and well-defended against malware, cyber-crime and other cyber-attacks also has economic benefits, as mentioned the answer to question 4.

**Question 6; ‘How effective is the Government in co-ordinating a response to cyber-crime that uses malware?’**

37. McAfee welcomed the Government’s allocation of £650m towards fighting cyber-crime in last year’s SDSR, as well as the various initiatives that the Government is currently undertaking, such as the Cyber Crime Strategy, the
National Cyber Security Strategy, and the creation of the Defence Cyber
Operations Group.

38. However, such strategies and initiatives will only be successful if there is
effective and joined up leadership, as well as real partnership with those private
sector IT security companies whose expertise can greatly contribute and
compliment.

39. There is currently no government contingency plan in place to deal with cyber-
attack, with action tending to be reactive, rather than proactive. This is perhaps
understandable during this difficult economic period, however, while initial
spending may be required to bring cyber defences and contingency plans up to
task, once in place they will be far more cost effective than simply reacting and
repairing the damage after every attack, which are becoming more common by
the day.

40. As mentioned above, many commercial security products themselves are hugely
adaptive, able to observe a piece of malware just a few times and then protect
many millions of users after that point. It is for this reason that the Government
is able to consolidate its approach to cyber defence, as described above. The
Host Base Security System (HBSS) is one example of a singular, comprehensive
approach to cyber-security.

41. HBSS is a programme McAfee is working on in the US with the Department of
Defence (DoD) and is the largest IT security deployment within the Department.
It provides multi-layered threat protection for more than 5 million DoD and
intelligence agency host platforms such as servers, desktops, and laptops in
accordance with the Enterprise-wide Information Assurance and computer
Network Defense Solutions Steering Group.

42. The HBSS system would also be applicable to the aims of the UK MoD as it offers
cross-platform protection from one supplier, removing unnecessary duplication
and complexity within the procurement. McAfee has been actively offering its
knowledge and experience of the HBSS programme to the MoD and
Government to ensure that they are better informed when it comes to making
their own procurement decisions. (Annex 1 offers more information on the
HBSS programme).

43. While the Government has taken steps to engage with industry, it should now
be enhanced to allow for collaborative risk assessments and increased
information sharing. Regular risk assessments, such as McAfee’s quarterly
Threat Reports and GTI briefings should also be undertaken by the Government,
drawing from the existing private sector knowledge that exists in this area, to
ensure that the Government’s plans to deal with the cyber threat are as
adaptive as the threat itself. The Government needs to select effective and
willing private partners with which to achieve this, and companies like McAfee
are well placed to step into the breach.
ANNEX 1: McAfee Partners with US Department of Defense to Deliver on Key IT Security Requirements

McAfee launched an open architecture technology programme, largely in response to the needs of one of its largest customers, the U.S. Department of Defense (DOD).

McAfee technology underlies the largest IT security deployment within the DOD, the Host Base Security System (HBSS), which provides multilayered threat protection for between 5 to 7 million host platforms worldwide. HBSS was launched after the DOD decided that host computer defense was critical to the protection of the Global Information Grid, and the system is mandated for installation on all unclassified and classified systems in the department.

McAfee® Host Intrusion Prevention solutions are the underlying technology of HBSS, providing monitoring, detection, and counters to known cyber-threats to the DOD’s enterprise architecture and delivering integrated security capabilities such as anti-virus, anti-spyware, whitelisting, host intrusion prevention, remediation, and security policy auditing.

Recently, McAfee partnered with Northrop Grumman to deploy HBSS for the Secret Internet Protocol Router Network (SIPRNet) within the U.S. Air Force. SIPRNet is the communications backbone of the DOD that facilitates the exchange of classified tactical and operational information at the secret classification level for both the Air Force and other branches of the U.S. Armed Services. McAfee has also partnered with Northrop Grumman in the U.K. to deliver the company’s cyber-test range, which was opened by Defence Minister Gerald Howarth in October 2010.

In deploying HBSS, the DOD wanted an open framework that would enable the department to plug in any number of solutions from different vendors. Largely in response to this need, McAfee initiated a technology partnering programme called the McAfee Security Innovation Alliance. The purpose of the McAfee Security Innovation Alliance programme is to accelerate the development of interoperable security products and simplify the integration of those products within complex customer environments.

McAfee security risk management solutions are at the heart of the McAfee Security Innovation Alliance programme, allowing organisations of all sizes to benefit from the most innovative security technologies. They now can simply snap into the McAfee management platform, McAfee ePolicy Orchestrator® (McAfee ePO™) software. Today, more than 100 technology partners across Europe, North America, the Middle East, and Australia have joined the alliance.
We believe that the McAfee Security Innovation Alliance programme provides an important value proposition for government and commercial customers who do not want to be locked into a single vendor.

McAfee

7 September 2011
1. Recent high profile cyber incidents have highlighted the increasingly complex, sophisticated and organised nature of cybercrime. This together with the shift towards greater interoperability between internet based networks and systems means that a targeted malware attack has the potential to have a cascading effect on other connected systems leading to individuals, businesses and organisations being impacted. Online attacks that were once conducted solely for notoriety are now increasingly being motivated by economic gain with cyber criminals seeking access to information that can then be sold as a commodity on the underground economy and possibly used in further attacks.

2. Given Symantec’s position as one of the world’s leaders in internet and information security we welcome the opportunity to provide input to the Committee on the important questions raised in the call for evidence.

   What proportion of cyber-crime is associated with malware?

3. To answer this question first it is necessary to define what is meant by malware. For Symantec malware is malicious computer code that can be classified into four main threat types; viruses, backdoors, worms, and Trojans. As is commonly understood computer viruses propagate by infecting existing files on affected computers with malicious code while backdoor malware is code that allows an attacker to remotely access compromised computers. Worms are malicious code that can replicate on infected computers and can facilitate malicious code being copied to another computer such as via USB storage devices or spread through emails and instant messages. Trojans leads users to unwittingly install malicious code onto their computers, most commonly through either opening email attachments or downloading from a web site.

4. For the last seven years Symantec has produced its Internet Security Threat Report. The longevity of the Symantec report provides a unique view on how malware threats have evolved, in scale and nature, as well as provides a current view of the worldwide Internet threat activity seen today. According to the latest Symantec’s report published in April in 2010 the main malicious code type seen in the UK were Trojans (55%) followed by worms (38%), backdoor codes (4%) with computer viruses (3%) being the least seen malware type.

5. The volume and sophistication of malicious malware activity globally increased substantially in 2010. Symantec recorded over 3 billion malware attacks and observed more than 286 million unique variants of malware with many of the malicious code threats increasing sophisticated with multiple features. For example, many worms and viruses are also incorporating backdoor functionality. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks. The development of multi-layered malware means that malicious code is increasingly able to remain resident on infected computers longer, giving attackers more time to steal information before the infections is discovered. As more users become aware of these threats and competition among attackers increases, it is likely that such complex malware threats will continue to increase in sophistication as cyber criminals attempt to evade security software. The use of new delivery mechanisms in 2010, such as web-attack toolkits, has also driven up the number of malware being seen in circulation.

6. The tactics and approach used by attackers may also change and evolve depending on the target. For example a popular website, social network or mobile operating system may be used to spread an attack given the popularity of the compromised environment and therefore the likelihood of the malware reaching more users. In 2010 Symantec also saw an increased malware threat to mobile devices given their popularity. As new devices, systems and networks grow in popularity and use, such as mobile, social networks, digital signatures and cloud computing, attackers will look to exploit their use as a means of targeting and attacking users.

7. In 2010 Symantec also observed a number of key attack themes which included a rise in targeted attacks with incidents such as Hydraq and Stuxnet both utilising different types of malware to conduct its activities. The Stuxnet attack is a key example of how malware is
being used not only to conduct traditional cyber crimes, such as fraud or extortion, but also targeted cyber attacks on critical systems and networks such as, in the case of Stuxnet, those used by the energy sector.

8. The Stuxnet attack targeted energy companies around the world and represented an example of a malware threat that can be designed to gain access to and reprogram industrial control systems specifically. It is estimated that at least four zero day vulnerabilities attacks were involved in the Stuxnet attack which allowed attackers to steal confidential Supervisory Control and Data Acquisition (SCADA) design and usage documents for industrial systems such as those used by the energy sector. This is the first time that so many zero-day vulnerabilities have been exploited in one attack and indicates that the people needed to develop and execute such an attack were not amateurs. It is understood that once the attackers gained entry into the targeted systems a root kit was used to hide their presence while they targeted software within the systems used to control industrial assets and processes. It is also believed that legitimate as well as stolen digital certificates were used in the attack to mask their trail through the compromised systems. The use of zero-day vulnerability, root kit, stolen digital certificates, and in-depth knowledge of SCADA software are all high-quality attack assets and points to an estimated group of at possibly up to ten people were involved in developing this specific, targeted and technically sophisticated cyber attack.

9. In the past this type of cyber attack focusing on such a critical national infrastructure were seen by many as theoretically a possibility however it is fair to say that most would have dismissed such an attack as simply a movie-plot scenario. The Stuxnet incident has shown that such targeted, organised threats do exist where external actors motivated possibly by organised crime, terrorism or even hostile nations, are designing, developing and deploying malware in an attempt to gain control of industrial processes and then place that control in the wrong hands. This incident therefore represents a new way in which malware is being used by cyber attacks to conduct criminal activity that is motivated by reasons other than financial gain or notoriety.

10. While it is perhaps better understood today the way in which the online threat environment constantly evolves, understanding the sheer scale and nature of the cyber threats facing users from malware can still be somewhat difficult. Looking at the number of malicious code threats observed in a specific period can help to provide an insight into the overall level and variance of activities currently being seen in the global threat landscape and may be useful to paint a picture of current situation within which the Committee’s inquiry is taking place.

11. In the period between 1 April and 30 June 2011 Symantec observed approximately 166 million unique malicious code threats, or malware, and on average observed 138,000 web based attacks. The malware detected in this time consisted of both existing and new threats. In the time period between April and June along with the continued prevalence of botnets and web based attacks, the emergence of new worm threats were also seen such as Qakbot a worm designed to specifically steal online banking account information from compromised computers. In this time period notable events such as the UK Royal Wedding, Japan Tsunami and death of Osama Bin Laden were all seen to be exploited by malware developers with the emergence of spam and phishing campaigns against internet users.

Where does the malware come from? Who is creating it and why?

12. According to the latest Threat Report the top country from where an attack targeting the UK originated in 2010 was the United States (38%) followed by the UK itself (17%), China (11%), Turkey (4%) and Canada (3%)². While these figures provide an indication of the origins of malicious activity it is important to recognise that this data does not give the full picture of where malware may originally originates from. While an attack may appear to be coming from America or China, the cyber attacker themselves could in fact be located in a entirely different country and may only be using the network, systems and perhaps users infected with a botnet viruses, in those countries to distribute and conduct attacks. In addition the creator of the malicious code itself may also be located in a different location altogether. Locating the origins of malware and therefore who is actually creating malicious codes is not

---

1 Symantec Intelligence Quarterly – April – June 2011-08-10
something that a single organisation or company can achieve as it requires different information on an attacks, or pieces of a puzzle, to be brought together by different sources as and when appropriate.

13. Although it’s difficult to determine the specific origins and objectives and motivations of attackers, a high proportion of the attacks Symantec is seeing are driven by economic and financial gain and consequently information theft. Recent incidents have fuelled public speculation about possible political motivation of attacks.

14. It’s perhaps easier to comment on why malware is being created and the motivation behind those creating malware. Cyber criminals today are both organised and professional with activities run like a business with malware research and development departments, marketing divisions using online sites to promote and sell attack tool kits which are also being sold with support services and help lines when malware needs to be updated or modified perhaps in order to avoid detection.

15. End users continue to be the main target for cyber criminals with confidential information a valuable commodity for criminals that can then be used in social engineering or more targeted attacks.

**What level of resources are associated with combating malware?**

16. Given the online threat environment and increasing sophisticated malware organizations are being exposed to, having the appropriate technology and solutions in place to address security incidents effectively is important. Given the current economic climate the cost challenges that organizations and individuals are facing may raise many questions as to the level of resources needed. Determining the most appropriate and proportionate level of technological resources needed is a decision that should be based on an assessment and identification of the level of risks being faced.

17. For Symantec an appropriate approach to addressing possible cyber security threats requires prevention against incidents occurring as well as preparedness to act if and when an incident occurs. Therefore a key resource needed to be prepared for a cyber security incident is having the right information at the right time to consider the possible threat or risk and take action as and when necessary. Having real time threat intelligence information can assist in the assessment of a risk and enable a timely response to the threat situation or incident by deploying appropriate operational capabilities to address specific security risks. Technological tools and solutions clearly also have a role to play in deploying countermeasures to combat and eradicate malware if an incident does occurs.

18. It is also important however to recognise that in order to combat cyber risks resources should not simply be focused on technology alone. An approach is needed that ensures appropriate technology is in place (based on an assessment of risk), policies and procedures for responding to an incident are developed and that resources are also allocated to ensuring people have the necessary cyber security skills and knowledge.

19. While it is recognised that the current economic climate may presents resource challenges, it is important that public and private sector organisations understand the importance of investing in, and deploying, appropriate security measures and solutions to protect against the increasing online threat environment.
What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

20. On 7th September Symantec published its latest Norton Cybercrime Report. Based on a survey of individuals on their experience of malware and cybercrime, the 2011 report has found that malware, specifically computer viruses, was the top cyber crime reported by both UK and global individual users. In the UK 38% of respondents having suffered a malware related incident of which 55% occurred in the last twelve months. This is the most common type of cyber crime experienced by users in the past twelve months. Following malware in the list of cyber crime experienced by users was online credit card fraud (10% of respondents) followed by social network profile hacking (6%). The Norton Cybercrime report estimates the total net cost of cybercrime to the UK as £1.1 billion. The lost of time by victims affected by cybercrime is valued at £618.9 million while the direct cash cost to victims from such factors as money stolen and the cost of resolving cybercrime is estimated at £474.2 million.

21. From the perspective of the computer security industry Symantec continues to develop and supply tools and solutions that enable users to put in place appropriate measures to protect their systems, networks and information. Symantec works around the world to ensure there is an adequate level of protection for users against online threats. Software companies, however, cannot and should not be held responsible for what they do not effectively control such as how the customer may install, configure, use and update security software. However, effective cyber security is not just about technology but also processes and education. Users must also be aware and educated about cyber threats and have the knowledge and skills to be safe online.

Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

22. It was the computer expert Fred Cohen who is reported to have coined the phrase computer virus back in the 1980’s as a way of describing how a file can infect a computer and propagate itself through a device similar to a virus in a human body. The analogy is still relevant today particularly with the rise in malware such as malicious spam emails. A provider of anti-spam services uses technical information, such as traffic data, to detect spam and deploy anti-spam techniques. It is rather like the immune system of the body recognising a pathogen (in this case the malicious traffic data) and producing the necessary antibodies. Operating in this automated way enables the security provider to determine whether an email is a spam and address the malware quickly and effectively to protect the potential victim.

23. Since the 1980’s not only has the nature of computer viruses changed but so has the environment in which they operate with the interconnected nature of advanced electronic networks and systems. Sophisticated malware attacks today can use more than one type or malware to conduct its attack multiplying rapidly across a number of different domains and infrastructures and devices that may be used, owned, managed or controlled by a number of different parties both in the public and private sector.

24. Ensuring the ongoing resilience and stability of the Internet from cyber threats is therefore not a responsibility of governments alone but a responsibility that is shared by all those using the Internet. The nature of the internet and IT technology is such that no single person can be held accountable and we all share a collective responsibility to protect ourselves and our customers whether they are businesses, users or citizens. Given the complex cyber ecosystem of the internet the threat information, technical intelligence and cyber security related expertise and advice that may be needed in a cyber related incident will reside across a number of different sources both inside and outside of government. For example it is estimated that 90% of critical national infrastructures that are increasingly reliant on interconnected networks and systems, and therefore a possible target for cyber attacks, are privately owned and managed. As a result public and private sector co-operation and collaboration are a key factor to assisting not only the government but also industry to identify, assess and evaluate the level of seriousness of cyber incidents.

---

3 Norton Cybercrime Report 2011
http://uk.norton.com/content/en/uk/home_homeoffice/html/cybercrimereport/
25. The government does have a role to play in considering and addressing the UK’s preparedness for cyber related issues and provide coordination. The recognition of the cyber threats to the UK in the National Security and Defence Strategy was welcomed as was the focus on the importance of public-private partnership which should continue to be supported. Given the importance of the ongoing resilience and stability of the internet to the societal and economic stability of the UK cyber security must remain a long term overarching public policy objective.

How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

26. Symantec is supportive of government efforts to gather advice and information in the event of a cyber incident as needed and bring together those that may need to work together to address an issue as and where appropriate and within the boundaries of the law.

27. Symantec sees the Office of Cyber Security as playing a key role in coordinating government activities in this area and operational response to address cyber related issues. The willingness of the Office of Cyber Security to engage and work with industry is also welcomed given the shared responsibility to prepare for and address cyber incident as and when they occur. It’s recognised that the UK has a number of different bodies addressing cyber security related issues at many different levels ranging from e-crime to critical national infrastructure protection. These bodies include the important work of CPNI and the UK e-Crime Police Unit which also play an important role in addressing cyber security issues in the UK.

28. Coordination and cooperation between the public and private sector on addressing the spread of cyber related threats are an important component to a cyber security strategy not only in the UK but globally. The UK government’s involvement in European international forums where cyber security issues are discussed such as ENISA, UN Internet Governance Forum, ITU and OCED as well as the UK’s participation in cyber security related exercises are welcomed and should continue going forward to ensure the UK playing a leading role in international efforts.

About Symantec

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. Further information can be found at www.symantec.com.

Symantec

7 September 2011
1. I am currently a Senior Research Assistant in the Computer Laboratory of the University of Cambridge. At present I am engaged in a 3-year collaboration with the National Physical Laboratory (NPL) to develop robust measurements of Internet security mechanisms.

2. I have a particular research interest in cybercrime. My research falls mainly under the heading of Security Economics – a field based on the premise that it is easier to explain security issues with an economic analysis rather than simply using a technical or ‘computer science’ approach. I am particularly interested in measuring criminal activity rather than merely describing it.

3. I have been using the Internet since the early 1990s, ran a software house that created one of the earliest mass-market Internet access products, and worked at Demon Internet, then the largest UK ISP, from 1995 until 2000. In October 2000 I returned to Cambridge to study for a PhD. My doctorate was awarded in January 2006 for my thesis, “Anonymity and Traceability in Cyberspace”.

4. I have continued to work in the Computer Laboratory doing academic research. On several occasions I have acted as specialist adviser to House of Lords and House of Commons Select Committees in inquiries into cybercrime and Internet security.

5. I have written, or co-written, over 40 peer-reviewed professional publications. My main research interest over the past few years has been into the criminal activity called “phishing” – the theft of financial credentials by impersonating legitimate websites. More recently I have been starting to look at the role of malware in the criminal eco-system and I have published work on how malware clean-up should be approached from a security economics standpoint.

6. I should also declare that in addition to my employment at Cambridge and my past association with Parliamentary Committees, I am a director of a small consultancy company that sells my time and expertise. Additionally, I am presently employed by Yahoo! in a part-time capacity within their security team.

7. This document expresses my personal opinions, and is in no way the expression of an official position held by the University of Cambridge, NPL, or Yahoo!

Q1. What proportion of cyber-crime is associated with malware?

8. I have been pointing out for years there are almost no reliable figures about cybercrime. In a report I wrote with colleagues for the European Network and Information Security Agency (ENISA) we set out the problems in detail in section #4.2.

9. Summarising 14 pages of densely argued analysis for this submission is impossible, but in section #4.4 we made two recommendations, both of which I would commend to this Committee:

   We recommend that the Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime.

   We recommend that ENISA collect and publish data about the quantity of spam and other bad traffic emitted by European ISPs.

10. Until we have reliable data we will not be able to assess the size of the cybercrime problem nor whether we are making any impact on it. Of course, assessing that impact in purely monetary

---

terms is simplistic and the Committee ought to go beyond what we recommended to ENISA and require the recording of all electronic crime incidents, not just those resulting in monetary loss.

11. For example, the UK banking industry already publishes fraud loss figures – but these do not actually document how much money has been stolen, but rather how much the banks end up out of pocket. The bank has no loss if they detect the crime promptly enough to undo electronic transfers before the money leaves the banking system (which we understand is achieved in about half of all cases).

12. Additionally, banks regularly attempt to dump their losses onto their customers, personal and business, by suggesting that the failure of security mechanisms is the customers’ fault, despite those mechanisms having been specified by the bank.

13. In particular, to return to this inquiry’s focus on malware: banks and others have chosen to rely on general purpose browsers and they have chosen to rely on identifying users simply by their ability to regurgitate a password. Unfortunately, when user machines are infected by malware this reliance is misplaced.

14. Most modern malware includes a ‘keylogger’ – functionality to record all the keystrokes typed by the user and relay them to the attacker. In response, the banks have moved to systems that prompt on the screen for just a few characters from the password. There is now malware that snaps a copy of the screen area around the mouse and the criminal learns the password one character at a time.

15. More sophisticated software performs “man-in-the-browser” attacks by intercepting legitimate interactions with the bank – perhaps paying a gas bill – and replacing this request with a transfer of money to the criminal’s account.

16. This type of malware operates in ‘real-time’ and will defeat the protection provided by the ‘CAP readers’ (the calculator-like devices that many of the banks have issued). This is because the user will type in the numbers from the screen still believing that they are paying their gas bill. Even after the fraud is complete the malware will keep the user from realising they have been defrauded by rewriting onscreen bank statements to continue the pretense of paying for gas.

17. One could carry on for many pages in discussing numerous different types of malware and explaining all the different types of criminality that it underpins. Unfortunately, this descriptive approach is pretty much all that we have – we have almost no reliable quantitative information.

18. Hence it is not really possible for anyone to give an accurate answer to the Committee’s specific question about the proportion of cybercrime that is associated with malware. All that can be said, in the most general terms, is that the eco-system for mass-market criminality is based on spam sent by botnets, and those botnets are constructed by compromising end-user machines with malware. Furthermore, the majority of specialist attacks on high-value targets – performing industrial espionage or compromising finance departments – are also based on malware.

Q4. What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

19. The committee asks a number of questions about malware authorship and the cost of protection which other experts will be able to address. What I can discuss, from my own research, is the ineffectiveness of protection – and, rather unusually, I even have some detailed numbers about this relating to the activities of one particular criminal gang.

20. First some generalities. Systems such as spam filters act to protect individuals by preventing them from ever coming into contact with malware. However once an email evades those filters and arrives in the inbox with a malware attachment or a link to a bad website then there is almost
no further protection at all. Of course some people will see through the ‘social engineering’ and will not be fooled into clicking the malware into action, but now that the criminals understand what is too enticing to ignore (and now they have fixed all their grammar and spelling errors) clicks are extremely common.

21. I have spent the past year tracking ‘Instant Messenger worms’ – malware that is spread between Instant Messenger buddies. What happens is that users receive a message over Skype, Yahoo! Messenger, Microsoft Messenger, Facebook Talk etc. which says something like:

   foto ☺ http://ofacebooks.net/album.php?your@email.addre.ss

22. If the user clicks on the link in this message then Windows will put up a warning message asking whether you wish to run a program from ofacebooks.net. Most people, I believe, are so eager to see the promised photograph that they will immediately press OK and thereby become infected by the malware.

23. Once the malware is running on a new machine it contacts its command and control system (C&C) to determine what it should do next. The C&C will generally instruct it to send a message to all of the new victim’s buddies (saying foto... etc.) to garner new recruits. The C&C will then download specialist malware (keyloggers, vulnerability scanners, spam senders, etc.) and the machine will be mined for financial data and turned into a resource in a botnet.

24. At the time of writing, my research shows that the malware for the most active worm is being downloaded just over 70,000 times a day and the number of victims, worldwide, is now well into the millions. This research is currently unpublished – but I expect it to be of significant import, not least because for once we have some accurate numbers to work with.

25. One might expect anti-virus software to detect the downloaded malware and hence provide protection. However, the criminals tweak the malware on a daily basis and only deploy it once it is passed as safe. Then of course the anti-virus software is updated, but too late to protect anyone.

26. To take just one example of the how ineffective anti-virus software is: consider the specific version of the malware that the criminals were using between 10:27 and 14:23 GMT on the 5th September. It was tested at 16:54 (90 minutes after the criminals stopped deploying it) and by that time it was detected by only 7 of 44 anti-virus products; and those 7 did not include any of the top 3 products by market share. Even 24 hours later, only 11 products reported this particular malware sample to be bad.

27. Of course, not all malware gets onto people’s machines because they click on a link and are ‘socially engineered’ into ignoring warnings. Some infections result from exploiting software bugs – for example in the add-ons that automatically play videos within the browser.

28. The large software companies such as Microsoft and Adobe provide automated patching systems to correct bugs. However, modern computers are running software from dozens, if not hundreds, of companies – and most of these companies do not have sophisticated patch distribution mechanisms. It would be desirable for companies such as Microsoft to open their patching platforms to third parties so that users could have a fully integrated way of staying up-to-date.

29. Other companies are just as slow at deploying patches, and in particular the mobile phone companies can be years behind at pushing out patches to their subscribers’ handsets. This is a classic failure that is easily explained by ‘security economics’: the people in a position to fix the problem are not those who would suffer a loss. We often have to resort to fixing such problems

---

by regulation – and this Committee should recommend that subscribers should be entitled to claim damages from their network provider if their phone (or their data) was damaged as a result of an unpatched vulnerability for which they have delayed rolling out a fix.

Q5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

30. Another way that industry fails to protect Internet users is by failing to act when their users are known to be compromised.

31. It is often possible to record the unique IP addresses of machines that are contacting a C&C system. Additionally, when a botnet is shut down it is now usual practice to set up a ‘sinkhole’ that will log the identities of the compromised machines which continue to try and make contact with the disabled C&C.

32. The operators of the sinkhole are unable to communicate with the owners of the compromised machines directly – they can only identify the ISP that is providing Internet connectivity. So it is up to the ISP to pass the bad news on to the relevant customer, because only the ISP knows who was using the IP address at the relevant time. In practice very few ISPs relay information and almost none go looking for further sources of this type of data.

33. We can see how poor the data passing is by examining the data collected by the Shadowserver Foundation, who operate a sinkhole for Conficker – malware that infected 7 million machines worldwide in November 2008 and which still poses a threat to the infected machines. The Shadowserver data\(^3\) shows that infections have dropped from 5.5 million in September 2010 to 3.5 million now; the worst affected UK ISP has seen a reduction from 7000 to 5000 infected machines over the same period. The best ISPs completely eradicated the problem, and ensured their customers were safe, two years or more ago, and I suspect that the drop in numbers is as now much to do with old computers being scrapped as customers being told of their problem.

34. The reason that ISPs discard notifications is because contacting their customers is expensive – the standard meme is that one phone call to a customer wipes out the profit made on them for a year. This makes a good sound-bite – but it is roughly correct. My own analysis shows that the cost equates to 8 months of profit, so the ISPs are indeed acting rationally in so far as their own self-interest is concerned.

35. Financial concerns are the basis of the industry-wide agreements (in Germany, Australia and The Netherlands) in which all the ISPs promise to pass on malware infection notifications. The idea is to ensure that no-one can steal market share by undercutting prices by failing to incur the cost of contacting customers.

36. This committee should recommend just such an ISP industry-wide agreement in the UK. However, the recommendation should go further and instruct the ISP industry to explicitly seek out sources of data, from sinkhole operators and others, so that UK Internet users have the best possible chance of being told if their machines are harbouring malware.

37. The Committee should pay particular attention to the system being operated by Comcast – the large cable provider – in the United States. They monitor traffic to their domain name servers – the machines that convert human-memorable hostnames into the IP addresses needed to communicate across the Internet.

38. Comcast use a datafeed from Damballa, a specialist anti-malware firm, to identify when hostname lookups are performed by malware that is attempting, for example, to locate C&C

\(^3\) http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker
servers. When the presence of malware is deduced then the customer is informed, usually by means of a pop-up message when they next use their browser.

39. One of the many reasons that ISPs fear talking to customers about malware is not just that they want to avoid delivering bad news, but they fear being pressured into having to explain all of the detail – and then being roped in to fix the problem. What Comcast have done to avoid this is to provide substantial online help and links to free online clean-up tools. Further, they have done a bulk deal with a specialist company who will, for an $89.95 fee, give personal help to customers.

40. I considered the economics of this type of clean-up operation in a paper that I presented to the Ninth Workshop on the Economics of Information Security in 2010. This peer-reviewed conference is the leading forum for work in the Security Economics field. A slightly revised version of the paper was subsequently published in Volume 81 of the Communications & Strategies journal.4

41. My paper,5 “Might governments clean-up malware?” supposed that the government would subsidise the cost of malware clean-up, and modelled what the costs might be. I considered a world in which ISPs passed problem reports on to their users, but if the user could not fix the problem they would be referred to a standard clean-up service. The users would pay a nominal sum ($30 (£20) perhaps) to avoid any moral hazard, and the government would subsidise the rest.

42. The thrust of my argument is that this is not as expensive a scheme as it might at first appear because the contractor would be able to sell other services off the back of their interaction with users. Hence they would swallow some of the subsidy costs themselves in order to land the government’s contract. My modelling suggests that the actual cost for such a scheme would be less than £0.50 per citizen per year – comparable with the costs of fluoridising the water.

43. There are of course numerous details and assumptions in this scheme, and I refer the Committee to the full paper for all of the details, and a discussion of the advantages of involving the government in such a scheme. The Committee might also note that the German malware clean-up initiative6 is partially funded by the German government.

Q6. How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

44. The government has not dealt with cybercrime effectively, whether it involves malware or not. Successive administrations have failed to provide adequate funding to grow and develop the specialist police units who work in this area. A very small number of officers have practical experience of tackling cybercrime and this has given them a rarity value in the job market, so that personnel retention is a significant issue.

45. The Committee should be recommending more resources – if only because cybercrime is volume crime that affects very large numbers of citizens. We have (a rarity as ever) some good data on credit card fraud, much of which is Internet related. A supplementary document to the British Crime Survey was published by the Home Office in May 2010. It looked at data from 2008-09 and found that 6.4% of credit card owners were aware of fraudulent use of their card over the previous 12 months. Victimisation rates were higher at 11.7% for incomes over £50,000/annum.

---

5 http://www.cl.cam.ac.uk/~rnc1/malware.pdf
If the Internet had been used at all (irrespective of income) the rate was 7.7% and if the Internet was used “every day” then it was 8.9%. In contrast, the 2010/11 British Crime Survey found that burglary affected just 2.6% of households and thefts from cars affected 4.2% of households.

46. There has also been a complete failure by government to even start to address the need for effective international responses to cybercrime. Police work needs to be coordinated at the international level, because otherwise committing a crimes in another country will make you untouchable.

47. In the US when 1930’s bank robbers used the new-fangled automobile to flee across state lines, the solution was to make bank robbery (along with auto-theft and other related offences) into federal offences rather keeping them as state-specific infractions. However, this solution does not look to be practical for cyberspace, because there is no global body with the equivalent reach over the world’s countries that the US federal government had over the individual US states.

48. We are not going to see cyber-police operating across borders in the near future, but we should be looking to see substantially more international cooperation in pursuing criminals in one jurisdiction who have committed crimes in another.

49. The best solution that I and colleagues have been able to suggest (in the ENISA paper already mentioned above in paragraph 8) is a liaison system such as Eisenhower developed in 1943 within SHAEF and which morphed into NATO. In such a system police forces would dispatch trusted officers to formulate pan-European (or preferably global) strategy for dealing with cybercriminals. Their role would be to represent their country’s police forces, and within the global strategy they would make tactical commitments to deal with criminals on their own soil and would ask for help with pursuing those who targeted their citizens but were based abroad.

50. We need proper international cooperation – to move beyond the current approach where every national police force targets the same, biggest, multi-national criminal gang and no-one worries about the rest of the top 3, let alone the top 10. We must end a situation where cybercrime is a lucrative career choice with a miniscule risk of ever being chased after, let alone caught.

Dr Richard Clayton

7 September 2011
Please find attached a response to the House of Commons Science and Technology Select Committee inquiry on Malware and Cyber Crime. This response represents the views of BCS, The Chartered Institute for IT, the Institution of Engineering and Technology (IET) and the Royal Academy of Engineering.

We note that the Government Cyber Crime Strategy will be published later this month. We would be willing to comment on this strategy once published, as a supplement to the response attached.

Inquiry Questions:

1. What proportion of cyber-crime is associated with malware?

We believe that a definitive answer cannot be given. The true extent of the cyber-crime problem goes unreported and unrecorded. Authoritative data has yet to be collected and collated from responsible bodies such as the Serious Organised Crime Agency (SOCA) and the Police National E-Crime Unit. We are cautious about recommending "industry" figures as we believe that in many cases the figures are debatable and in some instance self-serving.

Even with a precise definition of cyber crime or of malware, security researchers cannot do more than guess at statistics by extrapolating from tiny populations. In May 2010, it was generally accepted in the anti-malware research community that there were around 43 million known malicious programs (evidenced by several presentations at the Computer Anti-virus Researcher's Organisation (CARO) workshop in Helsinki). ESET (an antivirus company) claims that as many as 200,000 unique samples of malware can be seen per day. It is hard to be specific however, due to the fact that estimates vary widely from company to company.

It is generally argued that malware is used either directly or indirectly in a significant proportion of cyber crime. A very high proportion of cyber crime has some sort of connection with malware, with most crime being fuelled by botnets (spam, phishing, malware distribution, Distributed Denial of Service (DDoS), fake antivirus (AV), captcha breaking, click fraud etc.). Malware can be utilised in various and different forms. It can range in complexity from a simple open proxy to an advertisement delivery platform, to something quite advanced such as a self-propagating malware delivery system. Malware has increased in complexity, sophistication and volume, making it more difficult to quantify.

The banks and law enforcement agencies are best placed to provide a more definitive answer on what proportion of cyber crime is associated with malware. Bank customers are asked to report instances of cyber crime to their bank rather than directly to the police; however the banks are said to have an incentive to treat many reports as the fault of their customer and not as crime. Police figures are therefore likely to be lower than the real numbers.

We would like to point out that there is likely to be a substantial increase in cyber crime as more financial transactions are carried out on mobile phones, which are much more vulnerable and virtually unprotected from malware.

2. Where does the malware come from? Who is creating it and why?

The usual intention of a malware user is to compromise and potentially control as many systems as possible. Usually malware is created by intelligent individuals who desire either financial advantage, fame or power – power gained from control or the fame gained from being an international cyber criminal. A significant proportion of malware is said to come via emails, mainly through attachments.
The usual sources include organised crime, hackers, and activists; reasons include status, disruption, dissidents, military, business espionage, theft, financial gain and global terrorism.

There are six notable groups associated with the use of malware:

i. ‘Script kiddies’ exploit code developed by others and pretend that they are hackers. They are usually only able to attack very weakly secured systems.

ii. **Criminals**- Criminals work individually or within increasingly professional organisations and are responsible for credit card fraud and other theft activities. In economically challenged countries with high unemployment, graduates are tending to join these groups. In Russia, there are various groups using a notorious Internet Service Provider (ISP) which has been reported to host websites for illegal businesses. They use professional teams for their criminal objectives.

iii. **Hacker groups**- These groups usually work anonymously and develop tools for hacking. They may hack computers for no criminal reason, often to just show their presence. Hacking can also provide a route to employment, with companies often hiring hackers to test their security.

iv. **Insiders**- Although they represent only 20% of the threat, they produce 80% of the damage to the systems. These attackers are considered to be the most dangerous group. It is very difficult to identify them as they reside inside an organisation, working as authorised users. Their motives may be criminal or personal.

v. **Political/religious/commercial groups**- These groups are not usually interested in financial gain. Governments can deploy considerable resources and technical expertise to develop malware for political ends. The Stuxnet worm for instance, which attacked Iran’s nuclear enrichment facilities, was believed to be developed by a foreign government. Malware is said to be also used by commercial companies with the intention of stealing the IPR from their competitors.

vi. **Advanced Persistent Threat (APT)/ nation state**- This term has been used for some time in government and military domains to describe targeted cyber attacks carried out by highly organised state-sponsored groups, with deep technical skills and computing resources.

**Regional variations**

Regional variations have been observed in the use of malware. African malware use tends to involve non-technical fraud. Russia and Latin/South America tend to be associated with malware relating to banking/financial fraud and phishing. Russia and Eastern Europe have highly organised gangs devoted to a whole economic framework related to cyber crime, from money laundering to credit card credentials to malware distribution.

**3. What level of resources is associated with combating malware?**

We believe that considerable resources are needed to combat malware. Malware prevention is thought to be a significant expense and drain on resources. Ensuring that all AV, (Anti Virus) signatures are up-to-date is often a full time job for an individual or team depending on the size of the organisation that is being served. It is reported that the United States federal agencies spend about $100m a year on combating cyber crime through the Federal Bureau of Investigation (FBI), Secret Service, National Cyber-Forensics & Training Alliance (NCFTA), Department of Homeland Security (DHS). Large web services firms like Google and Microsoft are thought to spend in the order of $100m a year each on cyber crime prevention, with smaller firms like PayPal and Yahoo spending in the tens of millions.
We believe that it is impossible to provide a complete defence against malware. It is only possible to provide an effective defence for known vulnerabilities for which that the vendor has supplied a security patch. AV software is only partially effective in detecting malware on a data channel that the software is monitoring. There is no defence against malware that is exploiting vulnerabilities that are only known to the attacker (or malware writer). This means that even with vast resources, an organisation cannot guarantee 100% effectiveness in the detection and elimination of malware attacks.

We have identified five distinct resource types:

i. **Development resources** are used to design and implement security in a system as it is being built.

On 15 January 2002, Bill Gates, the chairman of Microsoft, informed all employees that security was a top priority, changing the company’s strategy. It took Microsoft until 25 August 2004 to make its PC operating system secure, when it released Service Pack 2 for Windows XP. The first PC operating system that was built with security in mind was not until 30 January 2007 when Windows Vista was released, some five years after the company’s strategy was changed. Microsoft released Windows 7 on 22 October 2009 which made significant improvements in the security of the product over previous versions. However, there are still vulnerabilities in Windows 7.

Microsoft is the exception. Most vendors of software tend not to incorporate security into their products, as they see the cost as an overhead, with no commercial advantage to them. For example, Adobe found its products targeted in 2010/11, particularly Adobe Reader and Flash, which forced them to have to release out-of-cycle security to address vulnerabilities that were actively being exploited.

ii. **Research resources** are the resource required to find and identify the vulnerability in a system, whether it is being actively exploited at present or not.

Responsible researchers who have identified vulnerabilities in a system inform the vendor, and allow the vendor time to fix the vulnerability. Malware writers do not inform the vendor of the vulnerabilities they are exploiting. Malware that is exploiting an unknown vulnerability has to be reversed-engineered, which is a highly skilled job and resource intensive.

To fully analyse a specific piece of malware may take weeks or months depending on its level of sophistication. For example, the Stuxnet worm is still being analysed six months after the original detection.

iii. **Vendor resources** (which also apply to systems developed internally) are those resources required to develop and test a security patch to help with the detection of vulnerabilities.

Vendors who become aware of security vulnerabilities in their products have to develop a security patch that will prevent the malware exploiting that particular vulnerability. However, the vendor has to ensure that the patch does not break any of the existing functionality of the system. The vendor may have to divert resource away from developing new products to developing and testing a patch for the vulnerability.

iv. **Individual resources** are those employed by an individual to maintain their own system in a good state to defend against malware.

The resources that individuals have to deploy require some technical knowledge. Security patches have to be deployed in a timely manner, and many people simply do not understand the importance of doing so. AV has to be installed, which will then update with the latest AV signatures. We would welcome any initiatives that would help to educate users about the
dangers of opening suspicious emails, for instance, the risks associated with opening attachments without scanning them first.

v. **Organisation resources** are the resources of organisations (government department/agency, commercial organisation, or charitable organisations) used to maintain their systems in a good state in order to effectively defend against malware attacks.

The costs are significant as security patches must be tested before they are deployed. If there is inadequate testing, then the system may no longer work after the patch has been deployed. If the testing takes too long, then the system can become infected with malware before the patch is deployed. To perform effective testing requires that test scripts are developed that enable automated testing to be performed. While the test system does not need to be identical to the live system, it does need to be a realistic representation of the live system to enable valid tests to be performed. This requires significant outlay in resources to develop the test scripts, and to have the infrastructure in place for the test systems.

While a large organisation can afford to invest in systems, scripts and resources to carry out testing and analyse the test results, this is not realistic for individuals, who must rely on the testing performed by the vendor. Individuals do not have the expertise to monitor for suspicious activity, although this would improve with the provision of educational initiatives, as mentioned in section iv.

4. **What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?**

There are no authoritative statistics. The proportion of infected PCs is variously estimated to be in the 1-15% range; 5% might be a conservative estimate. It has been reported that hostile cyber attacks on companies accounted for nearly one third of all UK data breaches in 2010 - up from around 22% the year before, with incidents becoming increasingly expensive.

A survey by the Ponemon Institute found that the cost of a data breach rose in 2010 for the third year running. The average data breach incident cost UK organisations £1.9 million or £71 per record, an increase of 13% on 2009, and 18% on 2008. The incident size ranged from 6,900 to 72,000 records, with the cost of each breach varying from £36,000 to £6.2 million. The most expensive incident increased by £2.3 million compared to 2009.

**Impact to individuals**

The impact to the individual from a successful malware infection is varied, but can be very significant. Examples include:

i. The PC becomes part of a Botnet (maybe thousands or tens of thousands of individual computers), which is then used by criminals to distribute Spam email to others, or to launch a denial of service attack against an organisation. Botnets are increasingly rented out for criminal purposes. The owner of the PC may only suffer a loss in performance of their PC, or they may be accused of committing a criminal offence.

ii. The malware may be used to extract useful information that may be stored on the PC, which could include personal details, bank details etc. For example, the government outlined in December 2010 that it had been a victim of the Zeus malware, with undisclosed loss of sensitive information. The loss of information can have serious consequences for the individual concerned, not only financial loss, but could affect their relationships with others or cause the loss of irreplaceable records such as personal photographs.
iii. The PC may be used to host illegal content. For example, child pornography. The owner of the PC is then open to being accused of knowingly hosting the illegal content.

The cost of malware infection is very high. Whilst there are some solutions, they tend to be part of a portfolio, which can be expensive. The cost to individual PC users is reported to be in the tens of pounds/dollars and euros per year in terms of AV expenditure. Furthermore, it is claimed that up to 2 million people or 4% of the English population are said to become victims of fraud each year. Cleaning up infected corporate networks may cost tens of millions of pounds and take a team of people several months.

Industry effectiveness

By and large, industry is not effective in defending against malware attacks. Many vendors still do not take security seriously. What we are seeing is an arms race, with the malware writers always being one step ahead of the defenders. To quote from a Virus Bulletin article (1 Feb, 2011):

“In the mid 90s we were in a position where we could accurately count the number of viruses that had been seen. This was possible for several reasons:

i. The number of new viruses was small enough for each sample to be identified and analysed in detail.

ii. It was easy to determine which part was virus and which part was the infected application.

iii. The size and complexity of the malware was quite limited.”

In 2011, the situation is completely different, with a large variety of malware out on the internet (new variants of a particular malware are produced every day or so). Malware threats have increased in complexity.

AV software vendors have varying degrees of effectiveness at detecting known malware threats. Some large vendors have effectively stopped developing their product five years ago, so may only be 50% effective at detecting known malware.

5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

All malware is in breach of the Computer Misuse Act 1990 and therefore a criminal activity. Malware therefore needs to be viewed in the same way as any other criminal offences. Human disease, in contrast, is natural and may be unavoidable. This is not the case for malware and as such the Government needs to be instrumental in tracing those responsible and prosecuting them accordingly. The biological analogies (virus, worm) should not be stretched to imply that similar control mechanisms would be effective in the cyber domain.


"The Cost of Cyber Crime" report reveals that whilst government and the citizen are affected by rising levels of cyber crime, at an estimated £2.2bn and £3.1bn cost respectively, business bears the lion’s share of the cost. The report indicates that, at a total estimated cost of £21bn, over three-quarters of the economic impact of cyber crime in the UK is felt by business. In all probability, and in line with worst-case scenarios, the real impact of cyber crime is likely to be much greater.
We therefore believe that the Government should help tackle the spread of malware, to reduce the impact on the UK economy.

We also believe that the Government needs to provide incentives to businesses to protect individuals against such losses. At present, it is not considered a commercial imperative among many organisations.

The Government should consider the following when developing a cyber crime strategy:

i. **Education** - The website [http://www.getsafeonline.org/](http://www.getsafeonline.org/) provides good advice on security. We would encourage the Government to increase the level of advice it provides to the public about security, in order that people do not remain ignorant about the issues of information security. Users need to be educated in information security to ensure that they are able to effectively protect themselves. The best security systems can be defeated by a user who wilfully and ignorantly overrides them (e.g. when they are the target of Phishing and Spear Phishing attacks, which dupe people into entering personal data into fake websites). We would again argue that more resources should be given over to explaining the basic security facts and the importance to individuals and industry. Basic lessons in the safe use of computers should be provided regularly to schoolchildren throughout their schooling, starting in primary school, in view of the reducing age at which children become active and vulnerable users of computers and mobile devices.

ii. **Government contracts** - It is important that the UK Government leads by example. The Government could consider deploying products where the vendor of the product has actively designed security into the product. As in the case of Microsoft, this is not a simple tick-in-a-box exercise, but requires considerable effort to achieve properly. Security has to be designed into the product from the start, and cannot be added on at a later date.

The Government is a large buyer of ICT systems. Consequently, it can have an impact on the marketplace. The Government could have significant influence if a list of more secure products was published. This could result in increased security provision by individuals and organisations, who look to the Government to provide advice.

Furthermore, the Government needs to ensure that its contracts ensure that its own systems are maintained in a secure state. Contracts need to outline which systems should be patched (all should be patched, in our view) and the frequency of patch deployment.

iii. **Legislation** - Criminals operate in many different jurisdictions, making it difficult to prosecute them.

There are very few convictions under current legislation. Developing malware, and installing malware onto computers, are offences which should be punished with penalties proportionate to the losses caused.

Legislation would also need to make it clear that researchers and vulnerability and penetration testers, who have a contract in place to perform such testing, are not committing an offence.

iv. **International relationships** - The UK Government needs to encourage other countries to establish appropriate legislation that enables the successful prosecution of criminals who are committing cyber crime. Sanctions also need to be imposed on countries that are harbouring cyber criminals.

There needs to be cooperation between countries on cyber crime. While for some serious crimes such as child pornography, there is cooperation, there is not the same level of
cooperation for less serious offences. The cost to the UK economy is estimated at £21bn a year by the Cabinet Office (see above), with the majority of criminals based outside the UK. The UK cannot solve this problem on its own. It needs the cooperation of other countries to eliminate the threat.

6. **How effective is the Government in co-ordinating a response to cyber-crime that uses malware?**

We are unclear on the detail of the Government’s strategy toward cyber crime associated with malware. We do, however, strongly believe that it is the responsibility of the government to try and prevent cyber crime.

We would like to see renewed focus by the Government in preventing exploitation of its core departments by its competitors overseas and lead by example. We would also argue that the police need to be better resourced to combat cyber crime, and to ensure that all criminal malware use is prosecuted. This will need to be done in conjunction with any educational initiatives that ensure individuals and organisations are aware of malware threats and the importance of security provision.

Joint submission by IET, The Royal Academy of Engineering and BCS, the Chartered Institute for IT

7 September 2011
Written evidence submitted by Amit Bhagwat (Malware 12)

Conflict of Interest: The author perceives no Conflict of Interest

Caution: In answering these questions, I have sometimes played the devil’s advocate. The point is to alert people, who are meant to protect the society, about the foreseeable dangers and not to put ideas in criminals’ minds. The reader should feel free to redact/summarise/consult the author

Approach: I have endeavoured to cover the whole breadth of the Terms of Reference of the enquiry and have used analysis, judgement and role-playing, rather than simply depositing past facts.

1. What proportion of cyber-crime is associated with malware?
1.1 I do not have accurate statistics. In context of creating severe panic situation – an emergency – almost entirely through user-unintended use of computing and electronic connectivity, my impression is that a very significant major portion of cyber-crime, certainly in terms of number of units impacted if not necessarily level of impact per unit, would be through malware.

1.2 Malware is, by its general nature, often like WMD and therefore far more potent than one-on-one cyber-crime.

2. Where does the malware come from? Who is creating it and why?
2.1 Of the malware – usually in the form of programming scripts, etc, that I have analysed, so far all has given me the impression of coming from humans. We have not yet reached a stage where AI has broken into human underworld. Among these human creators, not all are, or mean to be, criminals. For example, at a local public library, I came across a script file which replicated itself on USB drives, and then, through them, to other PCs (it took some patience on my part to prove to the stubborn library staff that their systems were infected, but that’s another story). When I studied the script carefully, it appeared that it carried no ‘payload’. So, as the medics would have put it, it was ‘infectious’ yet ‘benign’. Yet, it was developed to a point and by a clever enough person, where the same person or another person with small expenditure of time, could have turned that script ‘malignant’. It is hard to be certain, without detailed analysis of the individuals mind and motives, whether the creator of that script was an established criminal, a rookie criminal, or a clever but not very mature individual without malice.

2.2 The same applies to how the script got where it did. The library computers were said to be protected by a “cold storage” environment so any changes made in a user session would be undone. So was this environment weak or was incompetence on part of an IT technician, or worse, a deliberate malicious “Harold Shipman-esque” act was involved? It is worth investigating.

2.3 Another example I remember of two of my colleagues who fit this description – clever and benign but not always mature or responsible – was where they sent an “upgrade patch” to teammates, which asked the receiver to login using their office
domain credentials. It turned out that the element of trust/naivety was such that over two-third of the recipients complied. The writers of the program duly emailed the hacked credentials back to the providers and the credentials were then (hopefully) changed by the providers, yet the behaviour of the program written was that of a classic malware.

2.4 There are, of course, the hardened professional criminals, who would use it most. Certain things, such as ability to plan, analyse, program, associated with high-IQ individuals, may be regarded common features of malware creators/commissioners/tweakers/integrators, as is an abnormal or absent sense of right and wrong, or at least a sense of adventure temporarily blinding their probity. Occasionally, less able individuals will be willing and knowing ‘carriers’ of malware, either out of malice or simply irresponsibility. Beyond that, we must use the Stanislavsky/Holmes method, as best as we can. I have read some research into how well organised crime organisations can be where they are often far more efficient, mature and agile compared to the average large company (one example is the Freakonomics books compiled in lucid popular style but by serious Economists). An organised crime / terrorist organisation would rate malware highly, respectively as a high value business line and as a kind of WMD, and duly “invest” in it. In fact, malware would feature heavily in many modern conflicts and in most asymmetric conflicts, whatever their severity and sensibility, and thus labelling. A clever enough criminal would also look to carefully identify and target likely victims, people who are desperate enough to stray into unknown territory. For example, less established/regulated pornography sites, which by their very nature will be transmitting large binary objects/media in the course of their business, can be effective carriers, sometimes knowingly, willingly and as part of their business plan, of malware. A typical user of these sites could be desperate enough to go there against better judgement and once there, may stay there for long enough for infection to occur. The other problem, of course, is that information available from third parties, about how well-established and responsible a site is, can not always be relied upon.

2.5 Similarly a government, especially a rogue administration not accountable to ordinary people, will almost certainly yearn, and often possess, cyber-offence capability using malware.

3. What level of resources are associated with combating malware?
In organisations, variable, typically 5-50% of IT budget (though this is based on small sample of organisations whose budget/IT budget figures I have had access to). For individuals/families this is typically purchase of standard anti-malware package costing under £50/y, or a default no-extra-cost package such as Microsoft Security Essentials. Sometimes, in case of individuals, ignorance or low systems performance can result in no protection or deliberately weakened (by changing settings to achieve better performance) protection. If ISPs are making any efforts to combat malware, these are not evident. There are some volunteer/goodwill-generation efforts such as freeware tools, but these can be less reliable and usually lack customer support feature. If the government is doing anything at all, that’s news to me!

4. What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?
Potentially very high cost. The anti-malware industry is where aircraft automation was before the “fly by wire” technology matured to the extent where disallowing a pilot to do silly things became a possible option (considered by Airbus since A320, but generally not preferred by Boeing). Apart from the fact that the anti-malware tools may lag a little in time behind the proliferating malware, much depends on how cautious/trusting/naïve the human user is. For example, how many human users will never ever use a program/device driver not signed digitally? Hardly any. How many well intentioned programmers don’t digitally sign their programs, sometimes because these are distributed freely and there is no money to pay the certification authority? Many. How many signed programs are not open source and so involve an element of trust? Many. How many end users actually compile an Open Source program, rather than using it pre-compiled by others? Few. How many end users of Open Source programs who use/compile the source code understand and scrutinise all of it? Hardly any. Can we absolutely trust a compiler program to compile a source code without malice? No. How many compiler programs are hand-written by the end user of a program that is compiled by a compiler program? Practically none. When we have so many potential risks and so many things happen on trust rather than actual examination, the effectiveness is compromised. Finally, unlike the pilots (who are mostly professionals) analogy I used, few users of the cyberspace are ICT professionals associated with relevant specialisation. So, at every stage, the industry’s effectiveness is a bit compromised.

5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?
Yes. They are similar. It may be argued that malware usually won’t physically kill. It can however cause suffering comparable to major diseases. More importantly, it is usually infectious and the infection is usually preventable.

6. How effective is the Government in co-ordinating a response to cyber-crime that uses malware?
I haven’t seen any evidence. Competence, to the simple extent of understanding and being conscientious about one’s duty, of individual public sector workers and public sector units I have worked with, has shown a range of variation. The government’s record in management of major efforts has generally been disappointing. In one of my analyses related to enterprise architecture, I systematically compared leadership and effectiveness of Pitt the Younger and his cabinet some two centuries ago, with that of Mr Blair and his. It turns out, the effectiveness has gone down significantly with greater prevalence of self-serving ‘purely political’ decisions in the latter case, than in the former. This way, effectiveness of efforts can be compromised, or at least political leadership can become inconsequential to it.

Amit Bhagwat
7 September 2011
Written evidence submitted by the Serious Organised Crime Agency (Malware 13)

Introduction:

1. This submission sets out the Serious Organised Crime Agency’s (SOCA) written evidence to the Science and Technology Select Committee’s inquiry into malware and cyber-crime.

2. SOCA works with its partners, under the UK Control Strategy for Organised Crime, to address the threat of organised cyber crime, which it defines as:

   - Offences in which computers, networks or the data held within them are specifically targeted by an Organised Crime Group (OCG) including the design, sale or use of tools and techniques needed to mount such attacks, and the use of virtual payment systems to launder the proceeds of crime.
   - The use of ICT by OCGs to enhance operational security or effectiveness which includes alternative communication methods and evidence denial.

Malware is an umbrella term for malicious software and it is therefore used to describe any piece of software that is designed for a malicious purpose. As such, malware describes the collection of tools that can be used by individuals for a malicious or criminal purpose. It is not one single group or type of software that executes one particular type of crime. SOCA’s operational focus, where malware is concerned, is on the individuals behind the creation and deployment of those systems which represent the biggest threat to the UK.

3. The submission outlines the current level of knowledge within the organisation on malware and cyber-crime. This submission has been written in coordination with the Home Office, and should be considered supplementary to its submission which addresses the full range of questions the inquiry is set to explore.

What proportion of cyber-crime is associated with malware?

4. Malware is a key enabler of internet-enabled fraud. Cyber criminals use the internet as an opportunity to gather personal information or data, with the aim of exploiting it for financial gain. SOCA sees a continuous development of methodology as both criminals and those opposing them react and counter-react to an ever changing landscape. Developments in both technology and public take-up have meant that the tactics used by cyber criminals evolve at a
rapid rate. The use of malware within cyber crime has also risen in conjunction with improved public awareness of scams such as phishing.¹

5. A significant proportion of cyber-crime uses malware to perform some part of the crime. Even spamming² now involves the use of malware, as the majority of spam messages are now delivered using Botnets³. Criminality has had to evolve and develop increasingly sophisticated ways of capturing data and that increasingly means the use of malware, in one form or another. The UK is a relatively developed market for internet use and so the awareness of simple spam emails is perhaps greater than in countries where the internet is new. For this reason, criminals need to employ increasingly more sophisticated methods to achieve their aims as the user’s defence becomes similarly more sophisticated.

Where does the malware come from? Who is creating it and why?

6. Historically, malware was created by small numbers of people who had the necessary technical skills. Deployment of malware (and the consequent profit to be made) was similarly restricted to a small number of individuals. However, as cyber-crime has evolved, a complex marketplace has developed, allowing specialists (such as malware writers) to sell their products to others with little or no technical ability.

7. Organised crime groups have been known to commission malware creators to produce the tools they require, and malware writers have also been known to produce ‘off-the-shelf’ items; an example being the Zeus financial malware that was openly available for purchase for approximately US$700. In addition to the market for generic malware families (e.g. Zeus, SpyEye, Gozi etc) a new market has emerged for bespoke attack modules targeting specific financial institutions / corporate victims. This means that relatively dated malware families can still employ state-of-the-art attack tools, maintaining their effectiveness. Malware (such as Zeus) is also available with technical support, including a 24-hour telephone helpline. Criminal fora where such transactions are made have been in existence for at least a decade. These fora are frequently hosted in jurisdictions where UK Law Enforcement have little influence, and have stringent membership policies.

8. The main geographical source for the creation of malware targeting UK financial institutions is Eastern Europe, from former Soviet States. The socio-political conditions in some of these countries are ideal: education and

¹ Phishing is when an individual receives an unsolicited email purporting to be from their financial services provider, asking for ‘account verification’ – usually including a link to a fake website - from which criminals will harvest the financial data for fraudulent activity.
² Spam: Using electronic messaging systems to send unsolicited bulk messages indiscriminately.
³ A Botnet is a collection of compromised computers connected to the Internet, termed Bots that are used for malicious purposes and controlled by a single source.
internet development is reasonably good, employment and salary potential low, law enforcement deterrent is not prohibitive and organised crime groups exist. Past emphases on scientific or technical education has led to a highly able workforce with few legitimate prospects that can equal the criminal market in terms of financial reward.

9. This financial reward is the main driver behind malware creation. The early days of cyber-crime saw criminals developing attacks for kudos and peer recognition. This has dissipated and now status only accounts for a small amount of the activity for which SOCA has the remit to investigate. State-sponsored threats and 'hacktivism' (both significant sources of new malware) fall outside the scope of SOCA's focus, but information is shared with its UK partners where necessary.

What level of resources is associated with combating malware?

10. In April 2011 as part of the Strategic Defence and Security Review (SDSR) outcomes, SOCA was allocated £19 million over four years to support the delivery of a wider National Cyber Security Programme (NCSP). SOCA will use this funding to support the Government's priorities on cyber crime in the following ways:

- by increasing the capability and capacity to collect, analyse and disseminate intelligence on cyber-crime and cyber criminals;
- by providing an effective criminal justice response to cyber-crime through the enhancement of capabilities and the delivery of high-end operational outcomes. It will also provide additional legal services to deliver expert tactical and strategic support;
- by working with law enforcement, intelligence agency, private sector and academic partners to maximise use of technical and other capabilities for the benefit of all parties;
- by focusing dedicated resource to the delivery of high volume interventions to disrupt criminal cyber activity;
- by increasing private sector and public awareness through enhanced dissemination of timely intelligence and warnings via diverse media channels and Alerts; and
- by establishing a dedicated overseas resource to tackle cyber criminality in partnership with local law enforcement and other agencies and provide additional legal services to deliver expert tactical and strategic support to enhance international law and improve international co-operation.

11. Significant successes achieved against cyber crime in recent years include:

---

4 Led by the Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office.
• Working with GetSafeOnline.org, SOCA identified a highly organised criminal operation employing ‘scareware’ to trick web users into revealing their financial information to cybercriminals. Potential victims received messages on screen or a call from an IT ‘help centre’ claiming that their computer might be infected by a virus or other malicious software. A fake scan of their computer was then used to convince the victims that they needed to download new security software. In reality, victims were paying cybercriminals for the privilege of installing useless or malicious software onto their computer. Get Safe Online adopted this threat as the main theme for their 2010 campaign and SOCA provided advice to members of the public on how to spot ‘scareware’ and how to avoid becoming victims of this type of crime;

• SOCA is systematically targeting the criminal trade in stolen financial information. In 2010/11, SOCA seized 1.4 million items of compromised payment card data from cybercriminals and passed these details to UK Payments via its Alerts system. This data has subsequently been used to prevent fraud and identify theft where security breaches have occurred. The success of this approach has encouraged law enforcement colleagues in the US, Europe and Australia to participate in the initiative;

• Following a SOCA investigation, Virgin Media earlier this year wrote to about 1500 customers to inform them of a compromise. This was the first time that SOCA has partnered with an ISP to proactively contact its customers and is seen as a positive step in the corporate / law enforcement partnership; and

• SOCA led the UK end of a long-term FBI undercover operation against the online criminal forum DarkMarket. Before the forum was closed down in October 2008, it had been regarded as one of the most significant internet sites dedicated to the theft and sale of compromised personal information. It dealt in large quantities of stolen payment card and online banking data, and the tools and techniques needed for criminals to commit offences using them. Alongside two SOCA operations against DarkMarket subjects, SOCA provided intelligence and forensic support in this work to the City of London, Greater Manchester, South Yorkshire and Humberside Police. Follow up work continued, with suspects arrested in Turkey, Germany, the US and the UK, of whom 12 were arrested here.

12. Going forward, the National Crime Agency (NCA) offers an outstanding opportunity to achieve a further step change in the response to organised crime, including through more effective national tasking and coordination arrangements. The NCA also presents the UK with the opportunity to improve its national law enforcement response to crime perpetrated in cyber space or enabled by the internet, through the national centre of excellence on cyber crime which it will host.

What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?
13. At a superficial level, individual citizens may feel little direct financial impact from malware. Financial institutions will often cover the cost of a loss. It is assumed that these costs are covered by higher charges elsewhere, but the detail of this is not known to SOCA. Crime such as identity theft may not result in a financial cost but it could have a traumatic effect nevertheless.

14. General information on the financial impact of malware is inconsistent. At a corporate level for example, a large financial institution may not wish to disclose malware costs for fear of reputation damage. There is a better understanding of the threat in the US due to mandatory requirements to report data breaches in most US states. In the UK there is no obligation to disclose, and estimates of the costs of malware are difficult to assess.

15. Trade on and use of the internet has grown. In the future, it is likely that every age group will use the internet extensively. Attitudes to sharing personal data online have already undergone a marked change. Confidence in using the internet is therefore important and malware undermines that confidence, resulting in opportunity cost. Industry measures to protect their customers vary, and SOCA is committed to working closely with companies to mitigate the threat posed.

Serious Organised Crime Agency

7 September 2011
Written evidence submitted by the Police Central e-Crime Unit
(Malware 14)

Introduction

1. This report complements the Home Office submission to the Science & Technology Committee.

2. This Police Central e-Crime Unit submission addresses matters 1 - 3 as outlined in the Science & Technology Committee’s Terms of Reference for Malware and Cyber crime.

3. For operational reasons the nature of the evidence provided has been restricted to a limited number of completed cases.

4. For the purposes of this submission, the Home Office ‘United Kingdom Threat Assessment of Organised Crime’ definition of malware has been adopted: Malicious software consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorised access to system resources, and other abusive behaviour.

1. What proportion of cyber crime is associated with malware?

Remit of Police Central e-Crime Unit

5. The MPS’s Police Central e-Crime Unit (PCEU) is the national lead for e-Crime. The PCEU remit is to tackle those responsible for the most serious incidents of:
   • Computer intrusion
   • Distribution of malicious code
   • Denial of service (DDoS) attack and
   • Internet-enabled fraud

6. The PCEU proactively targets individuals involved in the high level authoring, distribution and criminal use of malware. These individuals are key enablers for cybercrime causing substantial harm to the UK and global economy.

7. Just over half (55%) of PCEU’s current investigations involve the authoring, distribution or utilisation of malware.
8. In the context of PCeU investigations, malware is primarily utilised in the commission of fraud offences against the financial sector.

9. A recent and growing area of concern for law enforcement is the use of Distributed Denial of Service (DDoS) attacks against organisations in the wake of the wikileaks scandal. For the purposes of this submission, only the criminal use of Low Orbit Ion Cannon DDoS utility ¹ is included.

2. Where does the malware come from? Who is creating it and why?

10. Malicious software is predominantly created, distributed and used for financial gain and DDoS attacks.

Attacks Against the Banking Sector
11. Organised Criminal Groups (OCGs) utilise malware to attack the banking sector. This form of e-crime can be extremely profitable, over a relatively short period of time, when compared to more traditional crime types.

12. Financial institutions invest heavily in Information Assurance. Criminals attack banking systems through the most vulnerable point, the on-line banking user.

13. OCGs investigated by PCeU are primarily using Trojan malware, typically SpyEye and Zeus, to create Botnets which are controlled by a server which can access bank accounts and transfer money out.

14. Malware infects victims’ personal computers, waits for them to log onto a list of specifically targeted banks and financial institutions and then steals their personal credentials, forwarding the data to a server controlled by criminals. It can also manipulate web browsing sessions including creating an additional page requesting the victim to reveal more personal information, such as payment card number, PIN, and passwords. Users have no idea they are being defrauded.

15. Unbeknown to the owner, computers infected with Zeus or SpyEye become part of a network where they fall under the remote control of computer criminals.

16. PCeU operational findings reveal that OCGs demonstrate a highly systematic approach to this form of criminality. Investigations have

¹ Low Orbit Ion Cannon DDoS utility (LOIC) Originally originally developed for network stress-testing, but later released into the public domain where, years later, it became a weapon of choice for hacktivists. Floods a targeted site with TCP or UDP packets, a relatively unsophisticated yet effective approach, especially when thousands of users use the tool to join voluntary botnets. By default does nothing to hide a user's identity
highlighted the use of technical expertise by OCGs in the form of malware authors, who provide the essential IT support for this criminality.

17. PCeU’s Virtual Task Force (VTF) approach has gone some way to mitigate against the risk of successful large scale attacks against the financial sector in the future through encouraging intelligence sharing.

DDoS Attacks
18. While the threat of DDoS attacks can be used to extort money from commercial organisations. The recent cases dealt with by the PCeU have involved the use of DDoS tools to attack organisations based on ideological grounds or simply to prove technical prowess amongst peers.

19. There has been a growing recent trend in 'Hacktivism' encountered by the PCeU which has involved groups or individuals targeting the websites of companies and organisations, motivated by political or ideological goals. This has been particularly highlighted by recent activity around Wikileaks supporters such as ‘Anonymous’. This has demonstrated that, facilitated by social networking sites, large numbers of individuals globally are able to voluntarily use their computers to launch DDoS attacks against organisations, with a low degree of central organisation or leadership utilising user friendly software such as LOIC (Low Orbit Ion Cannon DDoS utility).

20. There are individuals who author without affiliation to political groups or desire for money but who are motivated by factors such as the personal challenge of testing their IT skills. These individuals will carry out a range of attacks from DDoS to hacking and defacing websites. These individuals are more akin to the stereotypical lone, male hacker or ‘script kiddiy’.

The Authoring and Distribution of Malware

21. PCeU operational intelligence suggests that there are a relatively small number of individuals with the technical skills required to produce the code involved in distribution of malware.

22. Some individuals provide bespoke malware services to OCGs while at the same time working on their own criminality. Lower tier individuals appear to be 'testers', checking for bugs in the scripts which are used to move money into mule accounts and making adjustments to the code as required. Identified OCG’s have members each using core skills which are distinct i.e. infrastructure, cash out and code development.
23. Methods of malware distribution continue to evolve. A recent PCeU operation has shown that malware propagation is moving onto compromised legitimate websites, which may indicate that spam delivery and fake websites are no longer the primary mechanisms. Also this operation has found a number of Command and Control Servers used to both store the stolen data and control the malware. These servers are hosted in Russia, China and the UK.

Online Criminal Forums & Malware ‘Kits’

24. Online Criminal Forums allow all types of criminals to interact with each other across large geographical areas, to plan, organise and commit crimes, without having to personally know each other. These types of forums enable criminals with different skill sets to advertise their services and thus create virtual OCGs that would not have formed in off-line environments. Disturbingly, they also act as an educational forum to the benefit of new members.

25. PCeU has gathered intelligence and investigated the use of online criminal forums by a range of different individuals and groups including hacktivists, OCGs and individual hackers to share knowledge and organise offences.

26. Online criminal forums facilitate the purchasing of ‘malware kits’ which enable individuals to carry out ‘ready made’ attacks with less technical knowledge or experience. Intelligence gleaned from PCeU investigations indicates that individuals with little prior knowledge of IT can develop the capabilities to carry out a malware attack within a very short period of time.

27. Online criminal forums and ‘malware kits’ regularly come to the attention of PCeU staff investigating banking Trojans and DDoS attacks.

28. Availability via criminal forums, the relative ease of use and sometimes low cost of Zeus and SpyEye malware in particular, has led to its popularity and extensive proliferation globally.

Case Studies - The Authoring and Distribution of Malware

29. A PCeU investigation into an individual who was running a Zeus Botnet, in addition to hosting an online global crime forum called GhostMarket.net. GhostMarket was the largest English speaking criminal forum with over 8000 members which promoted and facilitated the electronic theft of
personal information. In addition to allowing users to trade compromised credit cards, the forum facilitated the creation and exchange of malware, the establishment and maintenance of networks of infected personal computers (Botnets) and the exchange of information about cyber and other criminality. Five individuals were arrested and charged, with all submitting guilty pleas after charging included Intentionally / Encouraging an Offence under the Serious Crime Act 2007. Though loses through criminal activity linked to the forum are still be calculated, the estimated value is currently in excess of £20million.

30. A PCeU investigation into an OCG utilising ‘Drive by Download’ methodology. ‘Drive by Download’ is where malware is inserted into a website thus allowing the infection of any computers visiting those domains. This investigation has identified that the subjects have been involved in the compromise of UK and global bank accounts using SpyEye and Zeus for financial gain. Over 100 malicious domains were identified in this investigation.

31. A PCeU investigation into an individual who is administrating a server, hosting both botnets and malicious software. Intelligence suggests that these are being used to commit criminality by stealing financial credentials from UK victims.

Case Studies - Utilisation of Malware

32. PCeU's operations have shown the significant criminal gains that can be achieved through organised, malware-facilitated, banking fraud. Alongside the financial sector Virtual Task Force (VTF) the PCeU dismantled the international OCG utilising a Zeus Trojan.

33. Over a 90 day period, the OCG was able to redirect funds from compromised UK bank accounts to the evidential value of £2.66million from the 285 accounts. Intelligence suggests that there were significantly more accounts affected and therefore potentially much greater losses. These figures only consider losses to UK banks. The OCG involved was also targeting banks in the USA, other Western European countries and Australia. Total criminal gains may never be calculated. In the USA alone, this OCG stole $70million.

34. The PCeU arrested three men in April 2011 in connection with an investigation into the use of toolkit SpyEye malware to steal online banking details. The international investigation revolved around the group's use of variations of the SpyEye malware. This malware has the
capability to harvest personal banking details from internet users and send the results to remote servers under the control of criminals.

35. More recently, the PCeU investigated a case where Trojan malware was hidden within bogus job advertisements posted on Gumtree. When individuals downloaded the application form for a job their computer was then infected with a virus. The virus being a Trojan, designed to capture the recipients banking details. The PCeU have made two arrests to date.

Q. 3 What level of resources are associated with combating malware?

36. The remit of the PCeU set out in paragraph 5 includes combating malware and as such the full resources of the unit are available to those areas of cyber crime.

37. The additional funding of £30 million over 4 years has provided the scope to significantly increase the number of cyber crime operations that the PCeU can conduct, by increasing their capacity. The principal aim of which is to provide a level of £504 million of harm or potential harm reduction, experienced by UK society through cyber crime.

38. The following paragraphs explain the different teams within the PCeU that collectively provide the national response to tackling cyber crime, including malware attacks.

39. It should be noted that the specific resources and staff numbers deployed within the PCeU have delivered significant success in responding to cyber attacks involving malware as the unit has established a unique concept of operations whereby it has the relationships and protocols in place to call upon the wider policing resources and external industry partners to work operationally with the team thereby enhancing the units expertise and resource capability.

Intelligence Development Team

40. The PCeU Intelligence Development Team (IDT) is staffed by one Detective Inspector (DI) two Detective Sergeants (DS), five constables and four police staff.

41. The role of the IDT is to receive and analyse intelligence which the team then develop by working with the source to produce actionable operational products from which a decision is made whether to progress investigations to the unit’s Enforcement teams.
42. In a number of cases attacks are aimed at financial institutions and it is the teams’ responsibility to act as the point of contact with these organisations. In addition, the team receives tasking requests from both within the MPS and from outside partners. These requests are filtered against the case acceptance criteria for the unit which focuses resources on the most serious cyber crime incidents. There is a process for the prioritisation of tasks, which is undertaken through a formal weekly meeting that determines and then prioritises operations against threats, risks and the capacity of the unit.

The Enforcement Team
43. The PCeU Enforcement Team provides the investigative and arrest capability of the PCeU and is currently staffed by two DI’s, four DS’s and twenty DC’s (Detective Constables). The team is evenly divided into four pods, each headed by a DS. Operations are allocated:
- The PCeU Intelligence Development Team
- Fast-time, in direct response to an attack on a financial institution.
- In support of national security operations
- In support of other foreign law enforcement agency investigations (e.g. FBI)

44. The PCeU currently works with national, European and international partners in order to call upon and coordinate enforcement activity.

45. The PCeU works closely with the IT security industry, utilising partnership relationships where possible to identify malware-related cyber crime and the subsequent reverse engineering to evidence and attribute the criminal nature, culpability and mitigation techniques.

46. Cooperation between European countries with regards to e-crime has improved significantly in the last 3 years. This is as a result of extensive operational engagement with countries willing to undertake proactive tasking at the behest of other nations. PCeU facilitates joint meetings to discuss cross border issues, ensure de-confliction and post operational sharing of learning and to improve working practices.

The Technical Team
47. The PCeU Technical Team provides the PCeU with the ability to interrogate digital media and technology with an increasing need for live forensic capability to respond to multi-layered technology and techniques used to commit criminality.
48. The team obtains intelligence and evidence of cyber crime, together with the facility to dismantle Botnets and undertake live network investigative functions.

49. Current staffing levels for the Technical Team are one DI, three DS’s, seven DC’s and four members of police staff.

50. The PCeU Technical Team’s current roles and responsibilities are:
   - To conduct computer forensic examinations / investigations, data recovery and electronic discovery
   - To gather and disseminate relevant and quality intelligence
   - To provide technical advice and assistance to officers engaged in the investigation
   - To produce evidence in a form which is admissible in court
   - To provide advice to industry and law enforcement colleagues

51. The Technical Team’s expertise is a crucial element to PCeU investigations and in order to maintain their abilities to combat the range of cyber crime methods, ongoing training and the retention of expertise are key to its success.

The Internet Governance Team

52. The Internet Governance Team comprises of one PS (Police Sergeant), one PC (Police Constable) and a member of police staff. A Detective Inspector also has portfolio responsibility for strategic engagement to identify and establish best practise and changes to national and international protocols within law enforcement and industry.

53. The responsibility of the team is to identify and take action against websites which cause harm to the UK economy through fraud, identity/brand theft and the infringement of property rights.

54. The team has forged links with internet governance bodies both domestically and internationally, as much of the illicit activity is committed outside the boundaries of the UK. Through these relationships the team has been able to remove elements of the criminal infrastructure to reduce the ability of criminal networks to cause significant financial loss. For example, by utilising the assistance of IP providers and domain name registrars sites have been taken down swiftly and to long-term effect.

55. The team is in the process of providing a Standard Operating Procedure for the internet governance position to roll out within policing and other UK Law Enforcement Agencies. This will increase policing capability, assist in the dissemination of best practice and help standardise activities.
56. In addition to those teams outlined, the PCeU also incorporates Cyber Industry Liaison, a Strategy, Performance and Communication Unit and supports the National e-Crime Programme through a National Delivery Office to deliver a regional capability with three hubs supported by the PCeU.

Police Central e-Crime Unit

September 2011
Written evidence submitted by Raytheon UK (Malware 15)

1 Executive Summary

Raytheon UK welcomes the opportunity to feed into the Malware and Cyber Crime inquiry by the House of Commons Science & Technology Committee.

2 Committee Objective

"The Committee has decided to gather evidence on the impact of malware on individuals, the responsibilities of Government to aid in preventing malware infections and the economy that has grown up around this industry..."

3 Consultation Questions

1) What proportion of cyber-crime is associated with malware?
2) Where does the malware come from? Who is creating it and why?
3) What level of resources are associated with combating malware?
4) What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?
5) Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?
6) How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

4 Raytheon UK Solutions

1) What proportion of cyber-crime is associated with malware?

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. (Source Wikipedia)

Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or program. (Source Wikipedia)

The total cost of Cyber Crime in the UK has been estimated at £1.9 Billion. (Norton Cybercrime report 2010. Note the BBC News is reporting £27 Billion loss to Cybercrime. Nearly 60 percent of people who reported being victims of cyber crime experienced malware and "malicious intent". (Source www.bytecrime.org).
2) Where does the malware come from? Who is creating it and why?

There are a multitude of sources that malware can come from, these include individual efforts, organised criminal group efforts and those sponsored by States.

Over the past few months there have been sophisticated organised attacks against some of the world’s leading suppliers of secure solutions to global enterprises, as well as attacks against major consumer companies providing games and media services to large multinational consumer bases. Second level service providers have also been targeted, with cyber criminals gaining access to the marketing service providers who maintain customer contact details and records of customer behaviour. Evidence suggests that the level (number of) and profile (numbers of users / customers being affected) of the attacks is increasing. Symantec believe that in 2008 more malware code was produced than legitimate commercial and open source code.

Malware designers can and will endeavour to mislead anyone analysing either the malware or its behaviour using decoy and beacon hosts in geographically disparate locations.

Factors are motivated by creating malware for a myriad for reasons, these include economic / financial benefit, collection of IPR, ideology and political beliefs.

As a Tier 1 defence and aerospace company, Raytheon’s valuable IPR has come under attack from every day threats for the last 30 years. This has allowed Raytheon to amass a wealth of experience in protecting our critical IPR and infrastructure from the most complex and persistent threats. Recently, Raytheon has also procured a number of high profile enterprises with widely used secure solutions protecting commercial enterprises and government agencies all over the world. Amongst the acquisitions are Oakley, Trusted Computer Systems and the assets of Compucat.

3) What level of resources are associated with combating malware?

Raytheon cannot disclose the numbers of resources associated with combating malware. However, the Raytheon Cyber team has designed an infrastructure and operational processes rivalling that of any of the Tier 1 defence providers in the world. Raytheon has teams of analysts at multiple locations defending the company’s assets from attack and analysing threats found by Raytheon and on behalf of other significant government and commercial organisations.

4) What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

The cost of malware to individuals can be measured by the estimated number of days taken to resolve an attack. Studies have shown that on average the resolution of an attack requires 28 hours. If the hourly rate of $30.00 USD is applied, then each attack costs an average of $840.00 USD or around $1000.00 USD to resolve. (this calculation is available on the Internet)

Commercial industry companies providing anti-virus solutions to the mass market are thought to be around 70% effective against viruses and malware. It is ironic that the very act of issuing patches to the mass market alerts the malware designers that their code has been nullified and begins another cycle of malware development.
5) Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

The Cyber threat, sometimes described as the Advance Persistent Threat is now considered to be one of the most serious security threats facing the UK – it has been categorised as a tier 1 threat by the National Security Council. The dependence on software and IT for critical infrastructure elements (e.g. the national grid, power stations and the public services) means that hostile states or organisation need only mount a concerted organised cyber attack to potentially damage another States economy or infrastructure. In this respect it is critical that the Government does take responsibility for educating the wider public on the consequences of malware and how to detect and deal with it.

Although malware spread in a similar manner to contagious diseases the analogy does not work well with the containment of the spread of diseases. Yes, there can be a warning and reporting process (WARP) to alert to incidents and alerts but malware mitigation is achieved by good housekeeping. If the government were to have a responsibility, it would be to inform and educate the public on cyber security and good information security management.

The Communications Service Providers currently collaborate to share information on threat actors, to ensure that the risk to customers (Public and Private) and the national network are minimised. This model could be implemented between the government and the cyber industry.

6) How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

Many different parts of government and agencies are now working to support cyber security efforts. The government needs to show a streamlined approach on the initiatives it is implementing and how clear authority on roles and responsibilities.

Raytheon Company is not only working to protect its infrastructure and systems but is working to educate and inform its employees about information security. Raytheon's Cyber Operations Training empowers individuals and organisations with the knowledge and confidence to excel at cyber defence, attack and exploitation. Within Raytheon we have the professional training skills and Subject Matter Experts (SMEs) with up to date operational experience to deliver bespoke education and training in a variety of blended packages. By using virtual classrooms, Computer Based Training (CBT) and traditional classroom based activities, employees are kept informed of how to detect, identify and respond to malwares as quickly as possible.

Raytheon UK
September 2011
Written evidence submitted by Dellsecureworks (Malware 16)

1. What proportion of cyber-crime is associated with malware?

Considering a couple of aspects of the evolution of Internet connectivity:

a) In the enterprise, firewalls and other network layer security controls have become a commodity, the technologies are effective and widely deployed, this places restrictions on how a cyber-criminal can reach or communicate with his target.
b) For consumers, widespread adoption of broadband Internet access, which is generally deployed with network-address-translation also limits the communication options for the cyber-criminal.

These two different evolutions in general deliver the same result: web browsing traffic to the Internet is permitted, traffic originating from the Internet is denied.

For a cyber-criminal to gain access to computers to steal, control, observe they must have some software agent, resident on the compromised computer – which will initiate connections outbound to the Internet.

The direct result of the improvement of basic network security controls is an evolution of the tools of the cyber-criminal where malware use is prevalent in cyber-crime.

In terms of proportion, this is not only difficult to quantify but also difficult to define. Is proportion defined by impacted individuals, direct losses or number of incidents? It should also be noted that a proportion of cyber-crime (defined in the most general sense) is conducted by insiders.

Our view at Dell SecureWorks is that the vast majority of cyber-crime leverages malware on a daily basis as part of basic cyber-criminal tradecraft.

2. Where does the malware come from? Who is creating it and why?

Malware is a worldwide problem supported by a vibrant underground economy.

Malware used to be created by individuals, for their own purposes. Malware now tends to be created by professional gangs, who sell it to the criminals who use it. Malware authors will offer technical support, publish product roadmaps and bugfixes. The malware developers are not talented amateurs, they are highly organised, highly professional and of course have identified that they are not breaking laws by producing malware that others deploy.

Malware is created for a number of reasons:

- recognition. Early malware was written for "fun" and to see how many computers could be infected before it was stopped. More malicious versions would corrupt files and try to render the user’s computer unusable. The attack was generally against the hardware and data, rather than the individual.
- theft from an individual. Most recent malware is written with the aim of capturing bank and credit card details. These can then be sold onto other criminals, with the details being used to buy goods, or steal from bank accounts.
\begin{itemize}
  \item spam. Malware is used to create botnets, which are then rented out to criminals for activities such as mass email campaigns for things like prescription drugs, or to conduct phishing scams; themselves designed to trick people into handing over bank login details.
  \item Intellectual property theft from businesses: Malware which attempts to penetrate a corporate environment and remain undetected for long periods of time. The controllers of the malware, meanwhile, use it to steal IP and other sensitive information from the infected company. This information can then be used by competitors, or states, depending on the nature of the company that was compromised.
  \item Activism: malware which is used for political means or to embarrass corporations. Activists may leverage “botnets” to launch Denial of Service attacks against targets.
  \item Espionage/“Cyberwar”: General Malware used for online banking fraud or intellectual property theft can be brought to bear by nation states. There have also been examples of malware being crafted to bring to bear on specific targets – for example the Stuxnet worm which is widely believed to have been written to damage the Natanz uranium enrichment plant in Iran.
\end{itemize}

The last 12 months have seen actors in each of these areas operating with a degree of sophistication. In some cases the malware “tools” that are deployed are common across the actors, in other cases the malware is highly specialised and tuned to the task in hand.

Who is creating it? It is not possible to determine absolutely but the indicators are clear that malware today is being written by talented software professionals. Geographic indicators point to Eastern Europe, and Asia.

\begin{center}
3. \textbf{What level of resources are associated with combating malware?}
\end{center}

Malware consumes an enormous amount of resources and has a significant economic impact. According to Gartner Group - IT Security spend represents around 5% of total IT spend within enterprises. This, on average, translates to an investment level of around $525 per employee per annum. This doesn’t take any account of the business impact of malware and/or associated downtime.

It is worth noting that there is an asymmetry between the number of threat actors and those combatting their actions. The fight against malware can be likened to a guerrilla war, where a relatively small number of combatants can cause havoc for a much larger and organised adversary.

\begin{center}
4. \textbf{What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?}
\end{center}

For individuals, the costs range from buying anti-virus and anti-spyware programs, (along with the associated annual subscription fees), to the time and money involved in trying to recover from an infection, possibly having their bank account hacked and their credit card details and identity stolen.

The industry is moderately effective in providing protection:

\begin{itemize}
  \item a) Desktop anti-virus/anti-malware solutions are a necessary and important protective control however they are not 100% effective. It is unfortunate as this remains the sole technical control deployed by the average consumer this leaves individuals in a vulnerable state.
\end{itemize}
b) Software vendors provide patches, software update services to allow individuals to address vulnerabilities. Software vendors have a duty-of-care to their customers to improve testing and reduce the number of vulnerabilities in their software.

It should be noted that at an individual level, infections are rarely reported to the authorities and the police have little way of understanding the scale or impact of such crime.

5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

Given the nature of society I don’t think there are mechanisms which would allow the government to participate directly in combatting the spread of malware.

It’s likely any government which embarks on direct action would have to define “what is malware” and “what is not malware”. This would be better done at international level so that countries can more easily work together on cybersecurity. Another consequence of Government action would be a need to balance fighting malware with privacy concerns and civil rights.

6. How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

The Government is not effective today in co-ordinating response to cyber-crime using malware.

CESG (Communications-Electronics Security Group, GCHQ) & CPNI (Centre for the Protection of National Infrastructure) do communicate around such issues, however their communications are directed at a small community (eg: CESG Listed Advisers) and often there are restrictions on whether such intelligence can be forwarded out of the community.

Government should focus efforts on identifying and prosecuting those involved in cybercrime. Industry should focus on improving preventative and detective controls relating to the spread of malware. Government and industry should work together to share information to increase effectiveness against malware in general.

It should also be remembered that overall security needs to be maintained. Some cyber attacks originate because of a lack of security in the physical world with people revealing passwords or disclosing too much data to unknown people.

Dellsecureworks

7 September 2011
Written evidence submitted by Microsoft (Malware 17)

0 Introduction

0.1 Thank you for this opportunity to submit a written response to the House of Commons Science & Technology Committee on Malware & Cybercrime. Bill Gates founded our Trustworthy Computing (TWC) initiative in an open letter in January 2002, focussing Microsoft’s increasing strides to protect its customers from the impact of malware and the cybercrime it can enable. Microsoft continues to address these issues through updated and improved products, better software engineering, customer guidance and collaboration with partners across industry, government, law enforcement and academia around the world. In particular, Microsoft works closely with government and law enforcement bodies in the UK to improve our response and defences against malware and cybercrime.

0.2 Malware and cybercrime are two overlapping but distinct concerns addressed by Microsoft. As Scott Charney, Microsoft’s Vice President of TWC, referenced in the paper Rethinking the Cyber Threat, “For more than two decades, people have struggled to understand the cyber threat, evaluate the risks to individuals and organisations (including nation-states) and craft appropriate responses.” Threats from malware range from cybercrime to cyber espionage to cyber warfare. Given this range, Rethinking the Cyber Threat proposes that malware threats should be collectively addressed by several national and international initiatives combining industry and government capabilities. Scott Charney’s speech on the matter and the paper are available here: http://www.microsoft.com/presspass/exec/charney/2011/02-15RSA2011.mspx. The remainder of this response will focus on the cybercrime impacts of malware and our collaborations to reduce cybercrime.

0.3 Microsoft provides multiple defences against malware and cybercrime such as: monthly and as-required updates across our software products, including but not limited to Windows and Office; Microsoft Forefront, which provides anti-malware solutions for business; Microsoft Security Essentials, which is free to the UK consumer; malicious website and phishing protection in our browser, Internet Explorer 9; malicious website screening in our search engine, Bing; and spam-filtering in our email products for business (Outlook) and consumers (free Windows Live mail).

0.4 Through automatic settings worldwide, Microsoft updates over 600m computers monthly and receives information from its Malicious Software Removal Tool on the state of infection. We also implement malware screening on almost 300m consumer email accounts, enable screening of billions of business emails per year, and scan billions of webpages per month with Bing. These data-streams are collated twice a year to produce Microsoft’s Security Intelligence Report, which has been published since 2005. Further information is available here: http://www.microsoft.com/security/sir/default.aspx

0.5 This response has been compiled by Microsoft drawing from our experience and available information at the time of publication around the world and across cyberspace, focused upon the concerns and issues of Her Majesty's Government of the United Kingdom. A comprehensive portal of resources for cyber security policy is available here: http://www.microsoft.com/about/twc/en/us/Policymakers.aspx
1 What proportion of cyber-crime is associated with malware?

1.1 Microsoft does not possess statistical information that associates malware with cybercrime. Although Microsoft’s Security Intelligence Reports provide information on the geographic variation in malware prevalence, cybercrime is referenced by example only.

1.2 Microsoft is aware on a case-by-case basis of vulnerabilities in its software being exploited by malware to perpetrate cybercrime and has responded in specific instances to the appropriate law enforcement bodies. Much of the malware that enables cybercrime does not exploit vulnerabilities in the software but in the human psyche. Known as “social engineering” or phishing attacks, these types of malware exploit the users of software and their information or assets, rather than compromise the operation of the PC.

1.3 In the past two years, through Project MARS (Microsoft’s Active Response for Security), Microsoft has taken specific actions against botnets (“robot-networks” enabled by malware and operated by cybercriminals). Specifically, we took action against the botnets Waledac and Rustock through our operations named “b49” and “b107” respectively. Anecdotally, operation b107, carried out in March 2011, indicated that 1 million PCs were infected and controlled by the Rustock botnet, generating an estimated 30 billion spam emails every day, accounting potentially for 40-60% of global spam.

1.4 Microsoft is also concerned with cybercrime not primarily perpetuated through malware but taking criminal advantage of online technology, especially in the area of child protection. Microsoft has supported the UK’s Child Exploitation and Online Protection (CEOP) centre since its inception, providing resources and software. Microsoft has provided its CETS (Child Exploitation Tracking System) solution and donated PhotoDNA technology developed in coordination with the U.S. National Center for Missing & Exploited Children to the UK and many other counties around the world. Further information is available here: [http://www.microsoft.com/presspass/presskits/dcu/materials.aspx](http://www.microsoft.com/presspass/presskits/dcu/materials.aspx).

2 Where does the malware come from? Who is creating it and why?

2.1 Microsoft is aware of malware from many sources around the world and across the internet, although correlating geographical and cyber locations is difficult due to the fact that origin information in cyber-communications can be modified through technical means. However, our Security Intelligence Report provides a broad analysis on the geographic origin and impact of the major malware families based on monthly feedback from over 600m PCs and our other data sources. Only case-based analysis of specific malware, as in our Project MARS, can identify the malware origins and victim locations; in these cases, we work with appropriate judicial and law enforcement organisations to reach a resolution.

2.2 Microsoft is not normally aware of the creators of malware and their purpose. We see distinctions between: 1. “Finders,” who identify vulnerabilities in software, 2. “Exploiters,” who prove that the vulnerability can be accessed and exploited against the user’s wishes and/or without their knowledge; 3. “Malware Coders,” who develop malicious software to exploit the vulnerability by infecting PCs; and 4. “Botnet Herders,” who manipulate the malware and infected PCs in organised networks across the internet. The Finders and Exploiters can and usually do have benign intent, pursuing the pure research aspect, so we work with this community to protect our customers. Generally our information comes from these security researchers, both inside Microsoft and across the cyber security community, who identify vulnerabilities in our software and likely exploitation mechanisms. However, the Malware Coders and Botnet Herders predominantly have a criminal intent. Our analysis may reveal the location of criminal activity; in these situations, we will provide appropriate information to the primary national law enforcement agency. In the UK we have a good working relationship with the London Metropolitan Police and the Serious and Organised
Crime Agency (SOCA). Microsoft does not work with perpetrators of malware or exploiters with criminal intent.

2.3 We have seen increasing sophistication and replication of malware over the past decade. The threat actors range from highly sophisticated pioneers testing new areas of software to “script kiddies” simply repurposing tools that are available on the internet for their advantage. It is also apparent that the cybercrime activity ranges from highly organised enterprises to opportunistic individuals. Malware and the tools to build it are widely available and do not disappear over time: once a piece of malware has been released onto the internet it will be reused by others, and the cost of access, development and deployment is continually diminishing. Malware has become the multi-purpose tool of the criminal in cyberspace. Therefore, we focus on systematic defence of our customers.

3 What levels of resources are associated with combating malware?

3.1 Microsoft continues to commit several hundred engineer-years per annum to combatting the impact of malware across our product-base though triage, response, updates, better engineering and new product architectures. Our security engineers use this expertise to develop tools to enable our customers and partners defend themselves. For example, *exploitable* helps developers identify and assign an “exploitability” rating to program crashes.

3.2 Since 2003, we have invested significant engineer-years developing and delivering the Security Development Lifecycle (SDL), to ensure that all of our engineers are up-to-date with the latest security coding practices. We share this valuable resource for free with our customers and partners around the world. More information is available here: [http://www.microsoft.com/security/sdl/default.aspx](http://www.microsoft.com/security/sdl/default.aspx).

3.3 Over the past decade, Microsoft has built arguably the best incident response team in the software industry. The Microsoft Security Response Centre (MSRC) coordinates product team engineers across the company to update software at least monthly, providing guidance in almost 30 languages and coordinate field engineers in over 100 countries. In addition, the MSRC collaborates with national Computer Emergency Remediation Teams (CERTs) around the world, each in turn committing substantial resources to combatting malware and cybercrime.

3.4 Microsoft provides leadership in an ecosystem of industry, governments, and academics working continuously around the world to mitigate the threats and protect customers and citizens. In order to nurture and evolve this ecosystem, we have created or collaborated with others to develop numerous programmes, including: MAPP, the Microsoft Active Protection Programme to share information and coordinate software updates with partner companies; MSVR, the Microsoft Vulnerability Research programme to work with partners to identify and mitigate vulnerabilities across the software ecosystem; ICASI, the Industry Consortium for the Advancement of Security on the Internet to collaborate with partner companies in response to systemic threats; and SAFECode, Security Assurance Forum for Excellence in Code to work with partners to improve security in engineering.

3.5 Microsoft has also committed resources to working with law enforcement around the world. Since the inception of the Botnet Task Force, we have partnered with over 40 national law enforcement agencies, and we continue to address malware and cybercrime through training and analysis tools provided through our Law Enforcement Portal.

3.6 Microsoft also commits resources to take specific legal and technical action in our Project MARS, as illustrated by our actions to neutralize the Waledac and Rustok botnets.

3.7 Over the past decade we have provided monetary rewards for information leading to the arrest and prosecution of cybercriminals launching or exploiting malware. Most recently, we offered US $250,000 in July for information leading to the identification and prosecution of the Rustock botnet controllers.
4 What is the cost of malware to individuals and how effective is the Industry in providing protection to computer users?

4.1 The costs of malware to individuals are manifold and more than monetary: they can include identity theft, data loss, necessary changes in behaviours and resources spent procuring updated and additional software products to protect against malware. Malware has the potential to cause severe impacts to users of compromised computers. In addition to the risk of data loss, some malware seeks to steal users’ financial and identity information. Additionally, the current prevalence of malware on the internet requires users to change their behaviours online. This includes not visiting risky sites, not reusing passwords, and having the knowledge to keep their device up to data and protected. Users must also spend time and resources obtaining up-to-date software to protect against current malware threats. While some vendors make effective anti-virus software available at no cost, there are a number of products that are available only with purchase. Because malware threats evolve so quickly, users must have up to date software on their devices. Out-dated operating systems and web browsers cannot adequately protect users from today’s malware threats. Consumers must be prepared to invest in current technology in order to enjoy the benefits of a digital society without being placed at undue risk.

4.2 As the world’s leading provider of software and services, Microsoft makes great efforts to protect its customers from the effects of malware. Our Security Development Lifecycle has led to measurable improvements in the security of our software: fewer pieces of malware now exploit operating system vulnerabilities, relying instead upon social engineering tricks to obtain access to a computer. When there is software vulnerability Microsoft is able to rapidly mobilize a response and, if necessary, deliver updates to over 600 million customers quickly and at no cost through our Windows Update service. Further, as part of this servicing process the Microsoft Malicious Software Removal Tool (MSRT) is run on each computer that connects to Windows Update. MSRT scans for and removes many of the most prevalent malware families and has been used more than 20 billion times since 2005. Finally, for enhanced protection against malware we offer Microsoft Security Essentials (MSE), an anti-virus solution, free to users of genuine Windows PCs. MSE’s more than 30 million users report millions of malware removals per year.

4.3 Beyond our product efforts, Project MARS works with academic and industry experts, and utilizes technical and legal efforts in an attempt to defeat botnets. For example, the Waledac and Rustock botnets were shut down through successful legal action, and then Microsoft began working with ISPs and national CERTs to help customers remove the Waledac infection from their computers.

4.4 There are also numerous international, national and private sector efforts to promote or use collective defence that have had varying degrees of effectiveness. Microsoft has called for greater collaboration between government and industry on collective defence in its paper on the subject by Scott Charney and referenced in his recent RSA speech,(see Introduction above). The Collective Defence paper (attached) highlights several successful examples of government and industry collaboration to improve cyber security.

5 Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

5.1 Several members of industry, including Microsoft in our Collective Defence paper of 2010, have proposed looking at the public health model to address the issue of malware. Malware does share several characteristics with human disease in that it can spread host to host,
morph rapidly and even exist asymptomatically. However, human disease is not a perfect analogue for malware. Human diseases are not sponsored by malicious actors, for example.

5.2 The public health model provides a very useful inspiration to solving the malware problem while not being the solution itself. Looking at the public health model prompts consideration of several important functions required to address the malware problem. First, we should strive for a trusted system with clear roles and responsibilities just like we have for doctors, paramedics and epidemiologists in human health. Second, computer users need to know who and where to get help with a malware issue. Just as individuals can recognize a hospital or pharmacy, it must be clear to them who can be trusted to provide assistance with malware prevention and remediation. Prevention or wellness is another topic that should be adopted from human health. To do so, we must begin with an understanding of what it takes to keep a system healthy and develop the social and technical norms to encourage the healthy state of all devices. Finally, as with epidemic preparedness, industry and government must be prepared for a potential malware outbreak in a way that leverages the trusted system and roles outlined above.

5.3 Governments around the world and the ICT industry share a responsibility to deal with malware both individually for their constituencies and collectively. Microsoft has invested significant effort over the past decade working on its own products and with partners to make the customer experience more secure. The currently broadening appreciation of the malware threat is an opportunity for reinvigorated effort to take action corporately, nationally and internationally to provide better protection to customers and citizens alike.

6 How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

6.1 Microsoft works with CESG, the National Technical Authority, CPNI, OCSIA and other government agencies concerned with cyber security to ensure the protection of UK citizens. These collaborations have been successful for many years in the mitigation and containment of cyber-attacks. These organisations are skilled and effective in their mitigation of the impact of malware on HMG and the Critical Infrastructure.

6.2 Microsoft also works with the London Metropolitan Police, SOCA and many other law enforcement organisations to address malware-based cybercrime in the UK. These organisations are generally under-resourced and differently prioritised to pursue cybercrime, which means that the people are concerned and committed to fighting cybercrime but unable to have broad impact. The citizen continues to be at a loss when it comes to reporting cybercrime, other than to his or her bank or ISP, who are generally effective at remediation but can take no further action to neutralize cyber threats.

6.3 Microsoft has noted and welcomes the substantial efforts by the current Government to collaborate with industry to address all aspects of cyber security including cybercrime. We will continue to work towards making the UK a national exemplar of best practice in fighting malware-based cybercrime.

6.4 Microsoft has been a clear advocate of the Council of Europe’s Convention on Cybercrime and welcomes the UK’s recent ratification. We are also aware that malware and cybercrime respect no national boundaries and there is a need for international collaboration between governments to improve and align legislation and regulation and eventually establish treaties to pursue and prosecute cybercrime effectively. We support the work of the US and UK in the development and promulgation of acceptable norms of behaviour in cyberspace and a first step to improving international legal cooperation against cybercrime.

7 Declaration of Interests
7.1 Microsoft provides products and services to UK citizens that can be impacted by malware and cybercrime and continues to develop mitigation and protection mechanisms in each new release.

7.2 Microsoft also provides updates to its products and services at least monthly free of charge to all customers. We also provide Microsoft Security Essentials anti-malware software free of charge to UK consumers. Our anti-malware facilities in our Internet Explorer 9 browser, Bing search engine and Windows Live email are all provided free of charge. Microsoft also offers security products commercially in the UK market, including Microsoft Forefront, and will continue to provide innovative and security-enhancing technologies for citizens of the UK and worldwide.

Microsoft

7 September 2011
Introduction

1. Nominet is the registry for the .uk country code top-level domain (ccTLD). With over nine million registered domain names, we are the second largest country-code top-level domain. We are a SME with a turnover of around £21 million and employing about 120 people.

Resources Committed to Combating Malware

2. We do not keep separate records of our expenditure to address malware: this is considered as an integral part of our standard operating costs.

3. As an infrastructure company, we size our systems to respond to possible attacks. We operate our DNS systems with an oversized infrastructure in order to respond to threats such as Denial of Service attacks. We share information with other leading actors in the domain name industry to identify threats and development of attack strategies.

4. The domain name industry has a good track record in working together on sharing best practice and information about risks. In addition to ad-hoc cooperation and specialist associations, the main mechanisms for this are:
   a. ICANN (the Internet Corporation for Assigned Names and Numbers, a US-based not-for-profit public-benefit corporation established to help coordinate the Internet's naming system). We are actively involved in the technical coordination work and a senior staff member is on the Security and Stability Advisory Committee; and
   b. CENTR (the European registry managers association with 50 Full Members, 10 Associate Members and 12 organisations granted observer status) brings together a global partnership of registry operators: Full and Associate members of CENTR represent around 80% of total global ccTLD domain name registrations, and VeriSign, PIR and Afilias, which operate .com, .net, .org and .info, are also Associated Members. The organisation provides an excellent framework for sharing information, for highlighting best practice, and for identifying trends and developments.

5. Nominet is also playing a leading role in researching and deploying defences against future threats to the security of the internet. One area of considerable activity over the last eighteen months has been the deployment of DNSSEC (DNS Security Extensions). DNSSEC protects against forged DNS data (for example, from DNS cache poisoning) by providing digitally signed records. We have signed .uk and .co.uk. We work at the forefront of DNS monitoring and are developing tools that identify threats such as botnet, spam and denial-of-service attacks.

6. We have worked with other organisations to respond to cyber-crime attacks, in particular where this has involved the use of the domain name system to deliver botnet instructions. This was the case with the Conficker worm where there was a major international mobilisation in response to the threat.

7. While we are not a member of a CERT (Computer Emergency Response Team), Nominet does provide a 24/7 CERT-type function and we do cooperate with other leading players in network and information security. We have a dialogue with CPNI and OCSIA which would allow us to be included in any national emergency planning or exercises. We were involved in the last (US-led) Cyber Storm exercise.
8. We have a significant research effort into ways of assessing “bad traffic” on the Internet and, in particular, looking for patterns showing abnormal behaviour. We are currently spending approx £0.5M annually on such proactive research.

9. In summary, this work is integrated into our business and it is impossible to identify actual malware-related costs. However, the costs are a significant proportion of our total turnover.

**Coordination of Efforts**

10. As will be seen above, Nominet is well networked with other businesses, government agencies and international organisations. We are a membership organisation and most of the UK’s communications infrastructure companies (and all of the largest ones) are Nominet members.

11. This cooperation is important in a sector as rapidly changing as the Internet. The international nature of communications also makes it important to network across borders with trusted interlocutors – hence why we devote considerable effort to working with international partners.

12. Increased government involvement with trusted parties involved in network and information security – in particular in sharing information – would be welcome. Such involvement is best through cooperation and partnership. The speed of innovation, the transnational nature of the Internet and the number of organisations involved in assuring the successful operation of what was designed as a distributed network requires a cooperative, rather than a centrally coordinated, approach. This was recognised in the conclusions of the World Summit on the Information Society in 2005 and led to the implementation by the United Nations of the multi-stakeholder partnership approach of the Internet Governance Forum.

13. One area where the government could help is in promoting the development of a national CERT, providing a framework for improved cooperation. Any such body should have as a key role to develop networks both nationally and internationally.

14. The analogy with human disease is not a helpful one: the government can certainly help address issues by improved education and awareness, but even in this area a multi-channel approach is likely to give better results. As we have discovered in the five years of the Nominet Internet Awards, many organisations are active in working with different community groups.

15. Government funding for academic research will continue to be important. Government can also show the lead in adopting best practice and in being an early adopter for security enhancements. However, the significant role is for the government to work in cooperation and partnership with other key players.

Nominet

7 September 2011
Written evidence submitted by the Australian Institute of Criminology (Malware 19)

Background

1. In July 2011, the House of Commons Science and Technology Committee chaired by Andrew Miller MP launched a new inquiry into the impact of malware on individuals, the responsibilities of Government to aid in the prevention of malware infections, and the economy that has grown up around this industry. The Australian Institute of Criminology (AIC) welcomes the opportunity to contribute to the current Inquiry.

2. The AIC is Australia’s national research and knowledge centre on crime and justice. It seeks to promote justice and reduce crime by undertaking and communicating evidence-based research to inform policy and practice. The AIC conducts research on a wide range of crime-related subjects, including cybercrime.

3. The material in this document is provided by the AIC in response to the House of Commons Science and Technology Committee’s inquiry into malware and cybercrime.

Submission details

Introduction

4. This submission provides information arising from AIC research that is applicable to the Inquiry’s terms of reference. This submission also outlines action currently being taken by the Australian Government in response to the malware threat.

5. Malware, or malicious software, includes viruses, worms, keyloggers, spyware, trojans and botware (see definitions in Table 1). Potential outcomes of malware infection include account names and passwords being compromised, which may lead to fraudulent activity; files being accessed and copied; and corruption of hardware or software resulting in computer downtime or a slowed computer network (Furnell, 2010). Botware may also result in the infected computer being used as part of a botnet, a network of compromised machines, which, among other things, can be harnessed to send spam, facilitate phishing and click fraud, host illegal data, disseminate other malware and conduct distributed denial of service attacks (Choo, Smith & McCusker, 2007). Denial of service (DoS) attacks involve overloading a website or computer system so that legitimate access is blocked. When using botnets this is known as a Distributed Denial of Service, or DDoS, attack (Grabosky, 2007).

Table 1: Malware definitions
<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>A self-replicating program that is spread by opening infected files and uses up available memory</td>
</tr>
<tr>
<td>Worm</td>
<td>A self-replicating program that spreads automatically and uses up available memory</td>
</tr>
<tr>
<td>Keylogger</td>
<td>A program that records users’ keystrokes</td>
</tr>
<tr>
<td>Spyware</td>
<td>A program that can monitor computer activity</td>
</tr>
<tr>
<td>Trojan</td>
<td>Malware disguised as legitimate software, such as a game</td>
</tr>
<tr>
<td>Botware</td>
<td>A program that connects a computer to a botnet and enables it to be controlled remotely</td>
</tr>
</tbody>
</table>


1. What proportion of cybercrime is associated with malware?

6. In 2008, the AIC commissioned the Australian Business Assessment of Computer User Security (ABACUS) survey, a randomised survey of small, medium and large businesses from a range of industry sectors and from all Australian states and territories. This survey examined the prevalence and nature of computer security incidents experienced by businesses in the 2006/07 financial year, the areas in which business systems were vulnerable to such incidents and the cost, types and effectiveness of approaches Australian businesses used to prevent them (Richards, 2009). The survey was weighted according to industry type and business size so that the data provided by each participant was proportionate in relation to the broader population being sampled. Challice (2009) provides an overview of the research methodology.

7. During 2006-07, 14 percent of businesses reported having experienced one or more computer security incident (Richards, 2009). Of these, 83 percent experienced one to five incidents, eight percent experienced six to ten incidents and nine percent experienced more than ten incidents (Richards, 2009). The number of computer security incidents experienced, by business size, is depicted below in Figure 1.

Figure 1: Number of computer security incidents experienced, by business size (percent)
8. The most prevalent type of incident was infection by a virus or other malicious code, which was reported by 64 percent of ABACUS respondents that had experienced a computer security incident. The second most prevalent incident involved spyware, reported by 44 percent of victimised respondents. DoS attacks, which often involve the use of botnets, were experienced by four percent of respondents reporting a computer security incident. Figure 2 below provides an overview of the types of computer security incidents experienced, by business size.

![Figure 2: Types of computer security incidents experienced by victimised businesses, by business size (percent)](image)

9. Common ways that computers become infected with malware include visiting websites or opening email attachments (Furnell, 2010).

10. Malware is commonly traded online, using black market portals. Hutchings (in progress) has conducted qualitative interviews with computer crime offenders and police officers investigating hacking and computer fraud offences. This research indicates that these portals are also used to trade in compromised data, to learn and teach others about vulnerabilities and to trade in particular skill sets. In addition, portals were found to offer a number of advantages to offenders. For example, they allow for anonymous communication, and access can be controlled to minimise law enforcement infiltration. Some countries have poor
reputations for responding to online crimes; however it can be difficult to determine country of origin as offenders are likely to hide behind open proxy servers (Hutchings, in progress).

3. What level of resources are associated with combating malware?

11. The ABACUS survey asked the respondents which anti-fraud and malware tools had been used during the 2006/07 financial year. Anti-fraud tools included anti-spam filters (used by 64% of participants) and anti-phishing software (used by 34% of respondents), while malware tools included anti-virus (used by 85% of participants) and anti-spyware software (used by 59% of participants). Overall, 88 percent of businesses with information technology reported using some type of anti-fraud or anti-malware tool. The proportions of small, medium and large businesses that reported using each of these computer security tools is shown below in Figure 3.

![Figure 3: Businesses’ use of anti-fraud and malware tools, by business size (percent)](image)

Note: n=3,658. Excludes 307 businesses with no information technology and 36 missing answers (34 from small, 2 from medium businesses).


12. Respondents were asked to estimate their total information technology security expenditure for the 2006/07 financial year. Table 2 below shows the median, mean and range for total information technology expenditure by business size. It was estimated that in Australia between AUD$1.37b and AUD$1.95b is spent by businesses on computer security each year (Richards, 2009).

<table>
<thead>
<tr>
<th>Business size</th>
<th>Median*</th>
<th>Mean</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>200</td>
<td>992</td>
<td>0</td>
<td>150,000</td>
</tr>
<tr>
<td>Medium</td>
<td>2,000</td>
<td>7614</td>
<td>0</td>
<td>300,000</td>
</tr>
<tr>
<td>Large</td>
<td>10,000</td>
<td>38,474</td>
<td>0</td>
<td>750,000</td>
</tr>
<tr>
<td>Businesses overall</td>
<td>250</td>
<td>1,830</td>
<td>0</td>
<td>750,000</td>
</tr>
</tbody>
</table>
4. What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

13. Almost half (47%) of business respondents to the ABACUS survey who reported one or more computer security incidents identified viruses, malicious code and spyware as causing the greatest financial loss, and 57 percent identified these incidents as being the most significant (Richards, 2009). Negative outcomes were reported by 77 percent of businesses following the most significant computer security incident, these included:

- corruption of hardware or software (40%);
- corruption or loss of data (31%);
- unavailability of service (38%);
- website defacement (2%);
- theft or loss of hardware (6%);
- theft of business, confidential or proprietary information (5%);
- non-critical operational losses (25%);
- non-critical financial losses (12%);
- harm to reputation (4%);
- critical operational losses (4%);
- critical financial losses (4%); and
- other (1%) (Richards, 2009).

14. When a computer security incident occurred, the average loss to a business was AUD$4,469 (Richards, 2009).

5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

15. The Australian Government responds to malware in a variety of ways. For example, in accordance with the Australian Internet Security Initiative (AISI), the Australian Communications and Media Authority (ACMA) identifies computers infected with botware and informs the relevant internet service provider (ISP). The ACMA identified 4,093,436 compromised computers in the 2009-10 financial year, an average of 11,215 per day (ACMA, 2011).
16. It is estimated that over 90 percent of Australian home internet users are customers of the 82 ISPs participating in the AISI (ACMA, 2011). When these ISPs have been informed by the ACMA that a customer’s computer has been infected with botware they can select from a range of responses as set out in the voluntary icode. These options include:

(a) contacting the customer directly (by phone, email or SMS or other means);

(b) regenerating the customer’s account password to prompt customers to call the helpdesk so they can be directed to resources to assist;

(c) applying an ‘abuse’ plan where the customer’s Internet service is speed throttled;

(d) temporarily quarantining the customer’s service, for example by holding them within a ‘walled garden’ with links to relevant resources that will assist them until they are able to restore the security of their machine;

(e) in the case of spam sources, applying restrictions to outbound email (simple mail transfer protocol –SMTP); and/or

(f) such other measures as determined by the ISP consistent with their terms of service (Internet Industry Association, 2010).

17. CERT Australia is Australia’s official national computer emergency response team. It also provides a direct response to malware by identifying account details that have been obtained using malware, and advises the relevant organisations when their customers’ account details have been compromised so that appropriate action can be taken. CERT Australia detected over 250,000 compromised accounts during the period of September 2010 to February 2011 (McClelland, 2011). CERT Australia advises that this is an area of ongoing work and that the figure has significantly increased since this time.

References


Dr Adam Tomison, Director (Chief Executive) of the Australian Institute of Criminology
Dr Rick Brown, Deputy Director (Research)
Ms Alice Hutchings, Research Analyst

Australian Institute of Criminology

8 September 2011
Written evidence submitted by PhonepayPlus (Malware 20)

Summary

1. PhonepayPlus, the UK regulator of premium rate services (PRS), welcomes the opportunity to provide written evidence to the Science and Technology Select Committee for its inquiry into malware and cyber-crime.

2. In our submission, we wish to highlight to the Committee the following:

   - **Growing threats to consumers from potentially harmful apps** – we are aware of growing risks from rogue apps (software applications for smartphones). This potential consumer harm spans a spectrum, from technically defined 'malware' (such as Trojans) to misleading downloadable software that can significantly harm consumers. In recent months, PhonepayPlus has identified through proactive monitoring and consumer complaints apps that charged customers for a premium rate subscription service without their knowledge or consent. We have taken robust action within our regulatory remit against the providers of these apps, shutting down the services and fining substantially.

   - **The role of regulation in helping to combat threats to consumer confidence in the digital market place** – PhonepayPlus is the UK regulator of PRS. PRS (sometimes called phone-paid services) share in common a micropayment mechanism that allows consumers to pay for content or services by an additional charge to their phone-bill or pay-as-you-go account. PhonepayPlus’ Code of Practice defines important outcomes that providers must achieve for consumers. In the cases where we identified apps that were charging without consumers’ consent, we used our full enforcement powers to quickly stop consumer harm, immediately shutting off the service. Following a thorough investigation, the independent Tribunal substantially fined the providers. However, PhonepayPlus is a civil regulator and as such our powers are limited. For example, where criminal activity is involved in malware on smartphones, law enforcement bodies need to pursue and prosecute such matters as appropriate. It is integral to any developments in this area that bodies such as the Serious and Organised Crime Agency give sufficient priority to this growing threat.

   - **The need for consumer and industry awareness** – as a proactive, collaborative regulator, PhonepayPlus aims to pre-empt problems that harm consumer confidence and damage the market before they occur. We believe that it is essential that these new threats in the digital sphere are brought to the attention of both consumers and the industry we regulate. With this in mind we have developed an award-winning consumer literacy campaign to help consumers, in particular young people, understand PRS and the costs involved with services such as apps. We have also issued a consultation with the PRS and digital industries around the issue of in-app billing in which we clearly define the need for clear consumer consent to be billed. The consultation also includes a range of other measures designed to protect consumers and ensure confidence in the digital market.

   - **Rapid market developments** – the rapid change in mobile technology, and the increasing adoption of smartphones, means that more and more people, including
children, are using their mobile phones to purchase digital content. We believe that it is essential that the Government understands the potential risks to consumers in the fast-moving digital, micropayment market, and that there is cross-agency working to help reduce these risks.

3. PhonepayPlus is doing further research on potentially harmful apps and malware on smartphones and will keep the Committee informed of this work in due course.

Introduction

4. PhonepayPlus is the independent, industry-funded regulator of PRS – the goods and services that you can buy by charging the cost to your phone bill or mobile pre-pay account – in the UK. A current and popular example is text charity donations or TV show voting. We have over 25 years' experience of regulating PRS through a Code of Practice, which is approved by Ofcom.

5. Where providers transgress our Code, we have strong enforcement powers, including the ability to issues fines of up to £250,000 per breach. However, we take proactive steps to prevent harm and empower consumers with targeted information so that they and their children can use PRS with confidence and without complaint.

Growing threats to consumer from potentially harmful apps

6. In recent months, PhonepayPlus has identified and taken robust action against apps that would charge consumers for a premium rate subscription service without their knowledge or consent.

7. In one example, PhonepayPlus received 78 complaints in relation to a free battery saver app that would automatically sign up the user to a subscription-based video clip service operating on a premium rate short code. Complainants stated that having downloaded the 'Battery Booster UK' app, they were subscribed into a premium service charged at £4.50 per month.

8. PhonepayPlus found that the app contained code that would access the phone’s text message function once it was installed, allowing texts to be automatically sent to a premium rate subscription service without the knowledge or consent of the consumer. PhonepayPlus immediately shut down the service for breach of its Code, and following a full investigation, our independent Tribunal imposed a fine of £135,000.

9. A full copy of the Tribunal’s adjudications in relation to apps found to charge consumers without their knowledge or consent has been attached at Annex One¹ and is published on our website in accordance with our Code.

10. As part of our on-going monitoring, PhonepayPlus has commissioned follow-up research to look into malware threats to UK smartphone users and fraudulent use of premium rate billing. This will help us to better gauge and understand the threats posed

¹ Not printed.
to UK consumers at present and in the near-future. PhonepayPlus would be happy to make available the research to the Committee when it is published in early 2012.

11. PhonepayPlus is also working with the Get Safe Online initiative to increase awareness of the threats associated with rogue apps.

The role of regulation in helping to combat threats to consumer confidence in digital market place

12. PhonepayPlus has developed and implemented a successful regulatory framework over the past 25 years, giving swift and effective protection for consumers, whilst allowing the industry to innovate and grow. The scale of this achievement can be measured by the fact that the UK enjoys the most stable and sustained market for PRS in the world.

13. We regulate PRS against a Code of Practice which is designed to ensure important outcomes are achieved for consumers. It is our expectation that in delivering these outcomes, that providers will comply with all relevant law. Whilst it is a breach of our Code to deal with services that breach relevant law, we recognise that especially where the criminal law has been breached, that as a regulator with civil powers, there is a limit to what we can do and that the law enforcement bodies are best placed to prosecute such matters. Therefore it is integral that any developments in this area that bodies such as the Serious and Organised Crime Agency give sufficient priority to this growing threat.

The need for industry and consumer awareness

14. As a proactive regulator that aims to pre-empt consumer harm and damage in the growing apps market, PhonepayPlus issued a public consultation, on 26 September 2011, on proposed guidance for app-based mobile payments. The aim of the guidance is to intervene early to ensure that hidden threats from apps do not have a detrimental impact on consumers, children or the many legitimate providers of new digital services. A copy of the consultation has been attached at Annex Two.²

15. Key recommendations in the proposed guidance include: consumers’ consent to charge must be clear and the requirement for password protection for stored applications to prevent children purchasing digital goods without the owner’s permission.

16. PhonepayPlus believes that the best and most cost-effective way to help consumers get the most out of PRS and prevent consumer harm is to help them help themselves. Our consumer literacy programmes have been designed to give consumers the knowledge they need to make informed choices about the PRS they use.

17. Drawing on research into our consumer engagement with PRS in 2009/10, we have developed an award-winning schools literacy programme entitled PhoneBrain to help young people understand phone-paid services.

² Not printed.
18. As part of the campaign, we produce and promote to schools and youth clubs in England and Wales curriculum-friendly lesson plans for ICT and enterprise courses at GCSE level. These lessons draw on young people’s natural enthusiasm for technology with the option to enter a competition for developing an app that would benefit their communities. Winners will receive an award of up to £500 from Live UnLtd, the social enterprise charity, to help them turn their ideas into reality.

**Rapid market developments**

19. The rapid change in mobile technology and the increasing adoption of smartphones, including by children, means that more and more people are using their phones to purchase digital content including app-based mobile payments.

20. According to latest research published by Get Safe Online, 17% of smartphone users now use their phone for financial transactions, including online banking, shopping or social networking.\(^3\) This form of transaction is typically and loosely defined as a micropayment, where digital content could be purchased for a very small sum of money.

21. At PhonepayPlus we welcome innovation and investment in the PRS market worth in excess of £800m annually. However, experience of regulating PRS in a fast-changing market that has taught us that innovation and technology can move faster than most consumers – or their children’s – ability to grasp the consequences of their purchase decisions.

22. If consumers are left confused or disempowered, this will reduce confidence in use of PRS, smartphones and micropayments generally. Therefore, it is important to move quickly to ensure consumers can use services with complete confidence and that markets are not damaged by rogue providers.

23. In recent years we have seen market developments that lead us to believe it is important for the Government to consider whether or not we have a regulatory framework in place that provides effective consumer protection and is ready to support growth in new and emerging services, such as micropayments. One recent estimate suggests global growth in micropayments from $320 billion to $680 billion by 2016.\(^4\)

24. PhonepayPlus believes the Government’s wide-scale review of the regulatory framework supporting the UK communications sector provides an important opportunity to look at this area in more detail to ensure the UK can meet its ambitions to be a global high-tec hub for growth and innovation.

**PhonepayPlus**

**November 2011**

---

\(^3\) Trend Micro’s Threat Spotlight, August 2011, based on data collected in 2011, Get Safe Online

Malware and Cyber Crime Inquiry

Introduction

As the manufacturer of the UK’s top selling smartphone, the BlackBerry, Research In Motion would like to draw the Committee’s attention to the rising prevalence of malware and cyber crime that users of smartphones are beginning to experience. The challenges of protecting users and prosecuting those responsible for mobile-based attacks are more complex than conventional computer users.

UK Landscape

Smartphones will outnumber PCs by 2013 and they will be the most common device for accessing the internet (Gartner, 2010).

A key feature of smartphones is the use of ‘app stores’, managed repositories of third party software. Today they boast over a million apps with billions of app downloads.

The choice of available apps is often the key determinate when people choose a new smartphone.

Smartphone Malware

Apps have not escaped the attention of cyber attackers. Over the past 18 months we have seen multiple instances of malware disguised as popular apps in prominent app stores infecting thousands of smartphones.

In a corporate environment where an administrator typically has control over the IT infrastructure, policies can be enforced to sufficiently prevent against malicious applications. For example, one of the application defence features of the BlackBerry solution allows an IT administrator to block downloads of applications that have not previously been vetted. The same cannot be said for many other platforms that have focused on consumerisation forgoing many of the needed checks and balances that have been developed to keep users safe.

It can be a very complex and time-consuming process to vet applications. Most app stores have opted for automated testing, which does not always identify malware hidden deep inside the app’s programming.

For example: a satnav application that helps you map your way home will need access to the internet to access map updates and to your GPS location to provide you with proper directions. If a malicious developer also wants to track this individual, an automated review of the app would not pick this up as it would seem to be using only the features and permissions that it should be using. In this instance, only a line-by-line examination of the app’s programming would spot this, which is not practical, given the volume of apps being submitted. To mitigate these concerns, an automated code review would be able to flag certain apps for a manual review, but even this would be time consuming and prone to false positives.

It should also be remembered that legitimate, authentic applications can also lead to the unwitting sharing of sensitive data. For example, some chat applications automatically copy the details of a user’s contacts to the host server.

The smartest attacker is the one that can make an app, distribute it freely and legally collect all the information they need.

Recommendations

The number of malware attacks on smartphones pales in comparison with PCs – this is in part due to the fact PCs vastly outnumber smartphones at present, but it is also due to effective security design. For this to continue, we recommend a number of measures:

**App review**: apps should be reviewed, either using automatic analysis tools or by manually, before they are admitted for sale/download in an app store. Whilst the process will never be perfect, it limits the possibilities for app developers to introduce malicious applications.
Reputation mechanism: app stores should show the reputation of apps and app developers, to help users avoid malware. It should be noted that most users don’t automatically consider security features when rating apps, and so there should be a separate section on privacy and security issues to prompt comments.

App revocation (i.e. ‘killswitch’): app stores should be able to remotely remove applications that have proven to be malicious or insecure. This would need collaboration with smartphone manufacturers to affect this (this is something RIM is able to do).

Device security: the devices themselves need to work in such a way as to ensure that apps, once downloaded, are stored and run so that the impact of malware is reduced (i.e. the apps are stored in what’s known as a ‘sandbox’). For example, each application on the BlackBerry platform runs within its own virtual machine and the user or the administrator can control what this application can and cannot do.

‘Walled gardens’: smartphone vendors can ensure that only apps from trusted app stores can be downloaded, which severely hinders opportunistic attacks. These ‘walled gardens’ or ‘jails’ cannot be too restrictive, otherwise they can stifle legitimate competition and encourage consumers to look for alternative ways of accessing apps, which can increase the risk of stumbling upon malware.

Conclusion
Increasingly, smartphones are coming under attack from malware and cyber crime. Attackers try to sell malicious apps directly or go after software vulnerabilities in popular apps.

As more and more consumers, government and business professionals use smartphones to store and process large amounts of confidential and personal data, this threat becomes ever more apparent. App stores offer important opportunities to prevent, or reduce the impact, of malware and insecure apps. They can provide customers with ‘vetted’ software distribution channels, show the reputation of apps, and operate a revocation mechanism for malware and insecure apps.

Different smartphone platforms and app stores currently address malware and insecure apps differently, and so there needs to be an industry-wide approach to addressing these problems. Security teams should exchange information about apps as well as examples of best practices, and consumers need be presented with clear security information about app developers and the apps they sell.

Because governments are consuming more and more bespoke – and in some cases widely available generic – applications, it is important that they engage with industry and continually share information about best practices.

About RIM

RIM is the manufacturer of BlackBerry, the UK’s top selling smartphone. Since the company was established in Canada 25 years ago, over 100 million BlackBerry smartphones have been sold. RIM now operates across 175 countries on over 550 wireless networks. The UK is now RIM’s second largest market in the world and our EMEA headquarters are situated in Slough.

Research In Motion
November 2011