Computer Viruses and Other Malicious Software

A THREAT TO THE INTERNET ECONOMY

OECD

Computer Viruses and Other Malicious Software

A THREAT TO THE INTERNET ECONOMY

OECD

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

Corrigenda to OECD publications may be found on line at: *www.oecd.org/publishing/corrigenda*.

Foreword

Addressed primarily to policy makers, this book was developed over the course of 2007, by the OECD Working Party on Information Security and Privacy (WPISP) in partnership with the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG). The report was declassified by the Committee for Information, Computer and Communications Policy (ICCP) on 6 March 2008.

In drafting the book, Audrey Plonk and Anne Carblanc from the OECD Secretariat have been assisted by Michel van Eeten of Delft University of Technology and Johannes Bauer of Michigan State University, consultants to the OECD, who have written Part II, and by a group of experts who provided feedback on Parts I and III. This group of experts included Mr. Graham Ingram and Ms. Kathryn Kerr (AusCERT); Mr. Colin Whittaker (APACS, UK Trade Association); Mr. Gilles André and Mr. Fabian Pouget (CERTA France); Mr. Kevin Houle and Mr. Jeffrey J. Carpenter (CERT/CC); Mr. Erka Koivunen and Mr. Kauto Huopio (CERT-FI Finland); Dr. Pei-Wen Liu (Chinese Taipei); Mr. HyunCheol Jeong and Mr. Jinhyun Cho (KrCERT/CC Korea); Mr. David Pollington, Mr. Jean-Christophe Le Toquin and Mr. Uwe Manuel Rasmussen (Microsoft); Mr. Christophe Birkeland (NORCERT Norway); Mr. Bill Woodcock (Packet Clearing House); and Mr. Jeremy Ward (Symantec Corporation). The Secretariat also benefited from the contribution of OECD and APEC delegates, including Mr. Keith Besgrove and Ms. Sabeena Oberoi (Australia); Mr. Shamsul Jafni Shafie (Malaysia); Mr. Jean-Jacques Sahel and Mr. Geoff Smith (United Kingdom); and Ms. Jordana Siegel and Mr. Joshua Goldfarb (United States). The Dutch government made a special contribution to enable work on the economics of malware, which is gratefully acknowledged.

A broader volunteer group of OECD and APEC delegates from Australia, Canada, China, China CERT, Chinese Taipei, Finland, France, Japan, JPCERT/CC, Malaysia, Norway, United Kingdom, United States, and the Business and Industry Advisory Committee to the OECD (BIAC), reviewed the report at different stages.

Acknowledgements

A new study such as the one on the economics of malware (Part II) incurs considerable debt along the way. First and foremost, we thank our interviewees, who gave generously of their time. They also provided valuable comments on a draft version of this report and checked and approved the use of their quotes where appropriate. Their input is greatly appreciated. To maintain confidentiality, none of those interviewed is named in the text.

Special thanks go to our colleagues Mark de Bruijne, Wolter Lemstra and John Groenewegen in Delft and Tithi Chattopadhyay, Yuehua Wu in East Lansing. They have provided invaluable contributions in the course of this project and we have greatly benefited from the exchanges of ideas with them.

We also would like to thank Anne Carblanc, Audrey Plonk and Sam Paltridge at the OECD and Ronald van der Luit and Edgar de Lange at the Netherlands Ministry of Economic Affairs for supporting this research and for their engaging questions and comments. Selected findings from this report are included in the OECD's report on *Malicious Software (Malware): A Security Threat to the Internet Economy*, developed in collaboration with the APEC Telecommunications Working Group.

We have given presentations to conferences on our findings, including the 35th Telecommunications Policy Research Conference (Alexandria, VA, September 28-30, 2007), the LAP/CNSA/MAAWG Workshop (Arlington, October 9-11, 2007), the 2007 GOVCERT conference (Noordwijk, October 18-19, 2007). Some of the very best feedback has been from the presentation of our interim findings at the meetings of the OECD WPISP and the workshops with policy makers at the Dutch Ministry of Economic Affairs.

Table of Contents

Figures

Boxes

Executive Summary

Spurred by the prevalence of always-on, high-speed connections, the Internet has become a powerful tool for enhancing innovation and productivity. The increasing dependence on the Internet and other communication networks, however, means the Internet has also become a popular and efficient way to distribute computer viruses and other types of malicious software.

"Viruses", "worms" and "zombies" might sound like science fiction, but they are in fact the reality presented by the spread of malware. The power and threat of malware are that it can infiltrate, manipulate or damage individual computers, as well as entire electronic information networks, without the users' knowing anything is amiss.

All of this has brought the electronic world to an important juncture. The onslaught of malware attacks is increasing, both in frequency and sophistication, thus posing a serious threat to the Internet economy and to national security. At the same time, current efforts to fight malware are not up to the task of addressing this growing global threat; malware response and mitigation efforts are essentially fragmented, local and mainly reactive.

This report is a first step toward addressing the threat of malware in a comprehensive, global manner. As such, the report has three major aims: (1) to inform policy makers about malware – its growth, evolution and countermeasures to combat it; (2) to present new research into the economic incentives driving cyber-security decisions; and (3) to make specific suggestions on how the international community can better work together to address the problem.

The need for a consistent approach to a global problem is not new, but malware presents particular challenges owing to the wide variety of actors working on the problem: governments, businesses, end users and the technical community. These different actors need to improve their understanding of the challenges each of them faces and to co-operate, within their communities and across communities. Furthermore, this co-operation must occur at the global level. It is not enough for one country or one community to effectively self-organise if others do not do so as well.

In light of the need for a holistic and comprehensive approach to malware, a common point of departure is needed from which to build co-operation and collective action. This report calls for the creation of a global "Anti-Malware Partnership" involving governments, the private sector, the technical community and civil society.

The rise of malware

No longer limited to the realm of computer hackers and tech researchers, malware in the 2000s has become a serious business and a multi-million-dollar criminal industry. The major drivers can be summarised as follows:

Malware is widely available. Virtually anyone can buy it online at a nominal cost, as well as from underground markets. And malware is user-friendly, meaning it provides attackers with the capability to launch prolonged, sophisticated attacks beyond their skill level.

Malware can infect all sorts of devices. Since it is nothing more than a piece of software, malware can infect not only personal computers but also the backbone of the Internet – the servers and routers that move data worldwide. While malware often propagates through the Internet, it is important to note it can also be introduced into computer systems not connected to the Internet.

Malware is profitable. Together with other cyber tools and techniques, malware is a low-cost, reusable way to carry out highly lucrative forms of cybercrime. Two prime examples are the capture of credit card and bank account data via "spyware" and the launch of "denial-of-service" attacks used to extort money or concessions.

The costs

Malware can harm critical information infrastructures, cause major financial losses and, perhaps worst of all, undermine trust and confidence in the Internet economy. Therefore, malware is increasingly a shared concern for all Internet market participants: governments, businesses and individuals in both OECD countries and Asia Pacific Economic Co-operation (APEC) economies.

Governments, for one, are increasingly dependent on the Internet for providing services, making them and their citizens vulnerable to malware. In addition to the complex and expensive task of securing their own systems, governments are being called upon to protect the general public from online ID theft and other Internet crimes.

Malware is also taking a toll on the private sector. With few exceptions, many private Internet market participants – from Internet Service Providers to e-commerce companies to software vendors – have had to increase security-related investments in order to expand their online business.

The key Internet market participants interviewed for this book (please see Part II) were devoting an estimated 6% to 10% of their technology budgets to protect against malware. Combined with indirect costs (such as funding watchdog organisations, public education campaigns and law enforcement efforts) the total costs of malware for key Internet market participants may well be above 10% of technology spending.

Problematic trends

As explained in Part I, the deployment of malware is becoming ever-more sophisticated and targeted, presenting a great challenge to those attempting to measure and combat the problem. Key findings include:

- Self-sustaining cyber attacks increasingly depend on "botnets", or groups of malware-infected computers (also called "zombies") that can be used to remotely carry out attacks against other computer systems.
- Many malware attacks are smaller and deliberately limited in scope, in an attempt to stay "below the radar" of the security and law enforcement communities.
- Spam has evolved from a nuisance, to a vehicle for fraud, to a vector for distributing malware.
- The overall malware problem is difficult to quantify: no single entity has a global understanding of the scope, trends, development and consequences of malware.
- Data on malware are not consistent, and terminology for cataloguing and measuring the occurrence of malware is not harmonised.
- The effectiveness of current approaches in combating malware is constantly challenged by both ongoing technological changes and faster exploitation of software vulnerabilities.

The role of economic incentives

To a great extent, cyber security is affected by the behaviour of the key Internet market participants: Internet Service Providers; e-commerce companies; domain name registrars; software vendors; and end users. Part II of this book presents new field research on how these Internet market participants make their information-security decisions.

During 2007, 41 in-depth interviews were conducted with organisations confronted with malware. In each instance, the following questions were asked: how the organisation is confronted with malware; what its responses are; what trade-offs are associated with these responses; and how the organisation is affected by the security actions of other market participants. Some key findings were:

- How key market participants address malware is greatly influenced by the specific incentives they face: greater online traffic vs. higher security costs, for example. Some of these incentives work to enhance online security while others work to reduce it.
- In many instances, market participants make decisions that pass on the costs of malware to others in the network (thus "externalizing" them), such as when end users opt not to protect their computers against viruses.
- Owing to existing feedback loops, which should be strengthened and expanded, the extent of passed-on costs and benefits is probably smaller than had been previously assumed. On the other hand, many of these passed-on costs remain unaddressed.

A global approach

While this work details many of the problems presented by malware, it is only a first step towards a solution. To prevent malware from becoming a serious threat to the Internet economy and to national security, a global partnership against malware is needed.

A wide range of communities and actors – from policy makers to Internet Service Providers to end users – all play a role in combating malware. But there is still limited knowledge, understanding, organisation and delineation of the roles and responsibilities of each of these actors.

Therefore, a global "Anti-Malware Partnership" should involve not only governments, but also the private sector, the technical community and civil society. Such an inclusive, co-ordinated effort would be more likely to produce co-ordinated policy guidance to fight malware on all fronts – from educational to technical to legal and economic.

This type of international co-operation should be supported and enhanced by accurate measurement of the problem and analysis of the underlying economics at play. Also, the limitations of current actions against malware should be addressed, and the question of how to strengthen anti-malware incentives for market participants should be further explored.

Improvements can be made in many areas, and international co-operation would benefit greatly in areas such as: proactive prevention (education, guidelines and standards, research and development); improved legal frameworks; stronger law enforcement; improved tech industry practices; and better alignment of economic incentives with societal benefits.

Background

The Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP) and the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG) have both experience and expertise in the development of policy guidance for the security of information systems and networks.

In 2002, the OECD adopted the *Guidelines for the Security of Information Systems and Networks* ("the *Security Guidelines*") which provide a clear framework of principles at the policy and operational levels to foster consistent domestic approaches to addressing information security risks in a globally interconnected society. More broadly, the *Security Guidelines* reflect a shared ambition to develop a culture of security across society, so that security becomes an integral part of the daily routine of individuals, businesses and governments in their use of Information and Communication Technologies (ICTs) and in conducting online activities.[1] In 2003 and 2005, the OECD monitored efforts by governments to implement national policy frameworks consistent with the *Security Guidelines*, including measures to combat cybercrime, develop Computer Security Incident Response Teams (CSIRTs), raise awareness, and foster education as well as other topics (OECD, 2005a). In 2006 and 2007, the OECD focused on the development of policies to protect critical information infrastructures (OECD, 2007c and 2008).

Likewise, in 2002, APEC issued the APEC Cybersecurity Strategy outlining six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education. To supplement the APEC Cybersecurity Strategy, in 2005 the APEC TEL adopted the Strategy to Ensure a Trusted, Secure, and Sustainable Online Environment to encourage APEC economies to take action for the security of information systems and networks.

Shared OECD and APEC objectives

In 2005, the APEC and OECD co-organised a workshop to share information on evolving information security risks and to explore areas for further co-operation between the organisations to better tackle the international dimension of information security risks. In 2006, both organisations agreed that the need to encourage a safer and more secure online environment was more pressing than ever due to the continued growth of economic and social activities conducted over the Internet and the increased severity and sophistication of online malicious activity. Subsequently, they decided to organise a workshop[2] and develop an analytical report to examine the issues of malicious software, commonly known as "malware", with a view to:

- Informing national policy makers on the impacts of malware.
- Cataloguing trends in malware growth and evolution.
- Examining the economics of malware and the business models behind malicious activity involving malware.
- Evaluating existing technical and non-technical countermeasures to combat malware and identify gaps; and,
- Outlining key areas for action and future work.

Prepared by the OECD Secretariat in close collaboration with volunteer government experts from OECD and APEC as well as the private sector, this report does not discuss every aspect of malware, all types of malware, or all propagation vectors. Rather, it focuses on issues of significant concern and areas which may pose problems in the future. Similarly, the report does not examine all possible strategies associated with preventing, detecting and responding to malware but rather focuses on elements of relevance to OECD member countries, APEC economies, and other governments and organisations more broadly. Finally, the report refers to forms of cybercrime, such as spam and phishing[3] that may not *directly* involve the use of malware but nevertheless demonstrate how malware can also be used *indirectly* to facilitate cybercrime.

Notes

1. The United Nations, the Council of the European Union, the Asia Pacific Economic Co-operation (APEC) and the Asia-Europe Meeting (ASEM) all recognised and used the Guidelines in their work.

2. Information on the joint APEC-OECD Malware Workshop is available at: *www.oecd.org/document/34/0,3343,en_2649_34255_38293474_1_1_1_1,00.html*.

3. Phishing refers to a social engineering attack, where an attacker manipulates a user to disclose their online account access credentials or other personal information (typically) to a website in the control of an attacker. According to this definition phishing may not *directly* involve malware. However, when the term is used to, for example, also refer to certain types of Trojan attacks, malware is implicated.

Part I. The Scope of Malware

Part I of this book defines the various forms of malicious software (malware) and their impact, growth and evolution. Specifically, Chapter 1 presents the major types of malware; Chapter 2 focuses on the types of malware attacks possible and their perpetrators; and Chapter 3 explains the toll that malware takes on the information and communications industry, as well as why malware is a growing and major concern for governments, businesses and citizens of OECD countries and APEC economies.

Chapter 1. An Overview of Malware

What is malware?

Malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners.[1]

Malware can gain remote access to an information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity.

Different types of malware are commonly described as viruses, worms, Trojan horses, backdoors, keystroke loggers, rootkits or spyware. These terms correspond to the functionality and behaviour of the malware (*e.g.* a virus is self propagating, a worm is self replicating).[2] Experts usually group malware into two categories: family and variant. "Family" refers to the distinct or original piece of malware; "variant" refers to a different version of the original malicious code, or family, with minor changes.[3]

Overall characteristics of malware

Although not the only means by which information systems can be compromised, malware provides attackers convenience, ease of use, and automation necessary to conduct attacks on a previously inconceivable scale.

Malware is multi-functional and modular: there are many kinds of malware that can be used together or separately to achieve a malicious actor's goal. New features and additional capabilities are easily added to malware to alter and "improve" its functionality and impact (Danchev, 2006). Malware can insert itself into a system, compromise the system, and then download additional malware from the Internet that provides increased functionality. Malware can be used to control an entire host[4] or network, it can bypass security measures such as firewalls and anti-virus software, and it can use encryption to avoid detection or conceal its means of operation.

Box 1.1 Malware: a brief history

Viruses and worms date back to the early days of computers when most viruses were created for fun and worms were created to perform maintenance on computer systems. Malicious viruses did not surface until the 1980s when the first personal computer (PC) virus, Brain (1986), appeared and propagated when the user "booted up" his/her computer from a floppy disc. Two years later, in 1988, the Morris worm received significant media attention and affected over 6 000 computers. Although other types of malicious software appeared in the mid 80's, the landscape of the late 80s and early 90s predominantly consisted of viruses. Until about 1999, most people related viruses to the example of a teenager hacking into the Pentagon's systems as seen in the 1983 movie Wargames.

In the mid to late 1990s, the landscape began to change with the growth of the Internet and personal computer use, the rise of networking, and the adoption of electronic mail systems. The so-called "big impact worms" began to reach the public in novel ways. The increased use of e mail brought high-profile mass-mailer worms such as Melissa (1999), "I Love You" (2000), Anna Kournikova (2001), SoBig (2003) and Mydoom (2004) that made the headlines and entered the public consciousness. These types of worms doubled their number of victims every one-to-two hours, rapidly reaching peak activity within 12-to-18 hours of being released. This marked the parallel rise in organised, sometimes co-ordinated attacks. The explosive growth of online financial transactions resulted in increased security incidents and in the appearance of new types of malicious software and attacks. Today, mass worms and virus outbreaks are becoming ever scarcer while stealthy malware such as Trojans and backdoors are on the rise. Many attacks are smaller to stay "below the radar" of the security and law enforcement communities. The goals of the attackers tend to be focused on financial gain. These new trends help explain why malware is now a global multi-million dollar criminal industry.

Malware is available and user-friendly: malware is available online at a nominal cost thus making it possible for almost anyone to acquire. There is even a robust underground market for its sale and purchase. Furthermore, malware is user-friendly and provides attackers with a capability to launch sophisticated attacks beyond their skill level.

Malware is persistent and efficient: malware is increasingly difficult to detect and remove and is effective at defeating built-in information security counter-measures. Some forms of malware can defeat strong forms of multi-factor authentication and others have been able to undermine the effectiveness of digital certificates.[5]

Malware can affect a range of devices: because malware is nothing more than a piece of software, it can affect a range of devices, from personal devices such as personal computers (PCs) or Personal Digital Assistants (PDAs) to servers[6] across different types of networks. All these devices, including the routers that allow traffic to move across the Internet to other end points, are potentially vulnerable to malware attacks.

Malware is part of a broader cyber attack system: malware is being used both as a primary form of cyber attack and to support other forms of malicious activity and cybercrime such as spam and phishing. Conversely, spam and phishing can be used to further distribute malware.

Malware is profitable: malware is no longer just a fun game for script kiddies[7] or a field of study for researchers. Today, it is a serious business and source of revenue for malicious actors and criminals all over the world. Malware, together with other cyber tools and techniques, provides a low cost, reusable method of conducting highly lucrative forms of cybercrime.

How does malware work?

Malware is able to compromise information systems due to a combination of factors that include insecure operating system design and related software vulnerabilities. Malware works by running or installing itself on an information system manually or automatically.[8] Software may contain vulnerabilities, or "holes" in its fabric caused by faulty coding. Software may also be improperly configured, have functionality turned off, be used in a manner not compatible with suggested uses or improperly configured with other software. All of these are potential vulnerabilities and vectors for attack. Once these vulnerabilities are discovered, malware can be developed to exploit them for malicious purposes before the security community has developed a “fix”, known as a patch. Malware can also compromise information systems due to non-technological factors such as poor user practices and inadequate security policies and procedures.

Many types of malware such as viruses or Trojans require some level of user interaction to initiate the infection process such as clicking on a web link in an e-mail, opening an executable file attached to an e-mail or visiting a website where malware is hosted. Once security has been breached by the initial infection, some forms of malware automatically install additional functionality such as spyware (*e.g.* keylogger), backdoor, rootkit or any other type of malware, known as the payload.[9]

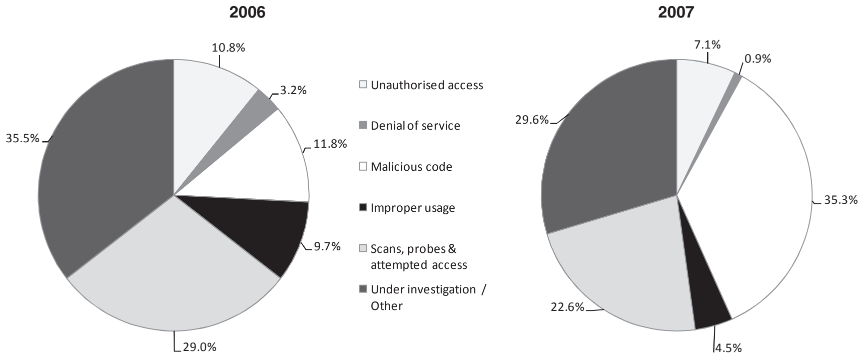
Social engineering[10], in the form of e-mail messages that are intriguing or appear to be from legitimate organisations, is often used to convince users to click on a malicious link or download malware. For example, users may think they have received a notice from their bank, or a virus warning from the system administrator, when they have actually received a mass-mailing worm. Other examples include e-mail messages claiming to be an e-card from an unspecified friend to persuade users to open the attached "card" and download the malware.

Malware can also be downloaded from web pages unintentionally by users. A recent study by Google that examined several billion URLs and included an in-depth analysis of 4.5 million found that, of that sample, 700 000 seemed malicious and that 450 000 were capable of launching malicious downloads (Google, Inc. p.2). Another report found that only about one in five websites analysed were malicious by design. This has led to the conclusion that about 80% of all web-based malware is being hosted on innocent but compromised websites, unbeknownst to their owners (Sophos, 2007, p. 4).

A different report found that 53.9% of all malicious websites observed are hosted in China (Sophos, 2007, p. 6). The United States ranks second in the same study with 27.2% of malicious websites observed located in there. Furthermore, the data provided below demonstrates that by mid-2007 malware on web pages accounted for 58.2% of the incident reports received by the United States Computer Emergency Readiness Team (US-CERT).

Figure 1.1 US-CERT incident reporting trends for January 2006 - August 2007

Overall distribution of cybersecurity incidents and events across the six major categories



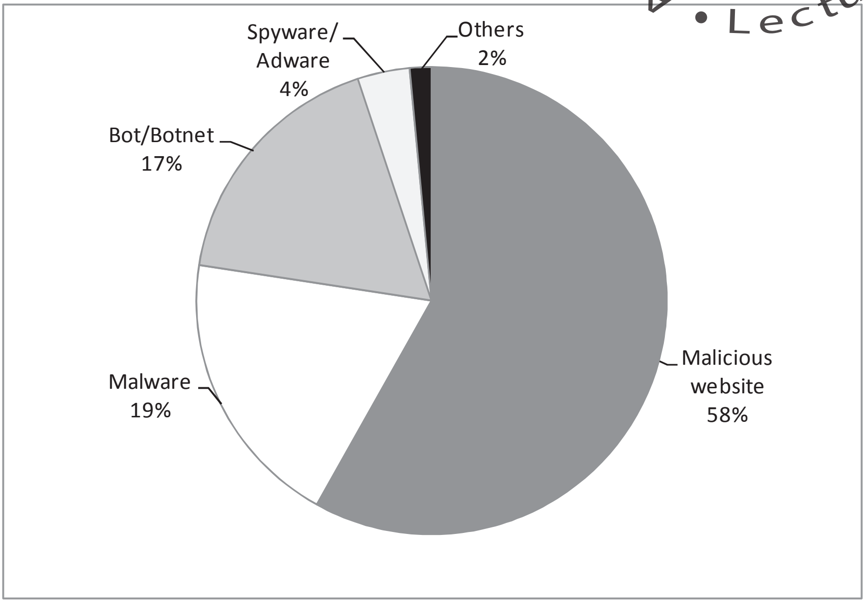
Source: NIST (2008).

Figure 1.1 above displays the overall distribution of cyber security incidents as reported to US-CERT across the six major categories. US-CERT utilises the reporting categories outlined in the National Institute for Standards and Technology (NIST) Special Publication 800-61 (US-CERT).

The number of incidents involving malware (malicious code) has significantly increased from 2006 to 2007.

Figure 1.2 below depicts the top five malware sub-categories being reported to US-CERT. The category labelled as "Malware" includes Trojans, worms and viruses. The graph shows "Malicious websites" as the most commonly reported sub-category.

Figure 1.2 Top five malware (2007)



Source: US-CERT.

What is United States Computer Emergency Readiness Team (US-CERT)?

A partnership between the Department of Homeland Security (DHS) and the public and private sectors. Established in 2003 to protect America's Internet infrastructure, US-CERT co-ordinates defense against and responses to cyber attacks across the nation. The organisation interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response co-ordination and to reduce cyber threats and vulnerabilities.

Malware propagation vectors

Malware propagation vectors refer to the electronic methods by which malware is transmitted to the information systems, platforms or devices it seeks to infect. Email and instant messaging applications are some of the most common vectors used for spreading malware through social engineering techniques. Any medium that enables software to be distributed or shared, however, can be a vector for malware. Examples of malware propagation or distribution vectors include the World Wide Web (WWW), removable media (such as USB storage keys), network-shared file systems, P2P file sharing networks, Internet relay chat (IRC), Bluetooth or wireless local area networks (WLAN).[11]

Bluetooth is one prominent vector for malware propagation on mobile devices. Bluetooth is a wireless personal area network (PAN) that allows devices such as mobile phones, printers, digital cameras, video game consoles, laptops and PCs to connect through unlicensed radio frequency over short distances. Bluetooth can be compromised by techniques such as bluejacking and bluesnarfing[12] and is most vulnerable when a user’s connection is set to "discoverable" which allows it to be found by other nearby bluetooth devices.[13]

Box 1.2 Examples of malware propagation vectors

E-mail: Malware can be “mass mailed” by sending out a large number of e-mail messages, with malware attached or embedded. There are numerous examples of successful malware propagated through mass-mailers largely due to the ability of malicious actors to use social engineering to spread malware rapidly across the globe.

Web: Attackers are increasingly using websites to distribute malware to potential victims. This relies on spam e-mail to direct users to a website where the attacker has installed malware capable of compromising a computer by simply allowing a browser connection to the website. If the website is a legitimate and popular site, users will go there of their own accord allowing their computers to potentially become infected/compromised without the need for spam e-mail to direct them there. There are two methods of infection via the web: compromise existing web site to host malware; or set up a dedicated site to host malware on a domain specially registered for that purpose.

Instant messengers: Malware can propagate via instant messaging services on the Internet by sending copies of itself through the file transfer feature common to most instant messenger programmes. Instant messages could also contain web links that direct the user to another site hosting downloadable malware. Once a user clicks on a link displayed in an instant messenger dialog box, a copy of the malware is automatically downloaded and executed on the affected system.

Removable media: If malware is installed on removable media, such as a USB stick or CD-ROM, it can infect and/or propagate by automatically executing as soon as it is connected to another computer.

Box 1.2 Examples of malware propagation vectors (continued)

Network-shared file systems: A network share is a remotely accessible digital file storage facility on a computer network. A network share can become a security liability for all network users when access to the shared files is gained by malicious actors or malware, and the network file sharing facility included within the operating system of a user's computer has been otherwise compromised.

P2P programmes: Some malware propagates itself by copying itself into folders it assumes to be shared (such as those with share in its folder name), or for which it activates sharing, and uses an inconspicuous or invisible file name (usually posing as a legitimate software, or as an archived image).

Internet Relay Chat (IRC): IRC is a form of Internet chat specifically designed for group communications in many topical "channels," all of which are continuously and anonymously available from any location on the Internet. Many "bot masters" (as the malefactors who operate networks of malware-infected/compromised machines are often called; see the chapter "The Malware Internet: Botnets") use IRC as the central command and control (C&C) communications channel for co-ordinating and directing the actions of the bot infected/compromised information systems in their "botnet."

Bluetooth: Bluetooth is a wireless networking protocol that allows devices like mobile phones, printers, digital cameras, video game consoles, laptops and PCs to connect at very short distances, using unlicensed radio spectrum. Because the security mechanisms implemented in Bluetooth devices tend to be trivially bypassed, such devices are vulnerable to malware through attack techniques which have been called "bluejacking" or "bluesnarfing." A bluetooth device is most vulnerable to this type of attack when a user's connection is set to "discoverable" which allows it to be found by other nearby bluetooth devices.

Wireless local area network (WLAN): Wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers without using wires. WLAN utilises spread-spectrum or OFDM (802.11a) modulation technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

Malware on mobile devices

There is some debate around the current seriousness of threats to mobile devices, such as cell phones, PDAs, and smartphones.[14] For example, some factors seem to indicate that threats to mobile devices are still limited. These factors include the following:

- some of the current forms of mobile attacks can only be launched within the 10 metres personal area of the network (PAN)[15] range – which limits the scope of the danger compared to traditional malware threats which have a global reach;

- mobile devices are restricted by bandwidth because there is a limited amount of spectrum allocated for their use;
- the very small user interface is still an impediment to conducting Internet banking and other value transactions – until mobile devices become a popular means to conduct such transactions there are fewer incentives for attackers to develop malware for the mobile telephone platform[16];
- the cost associated with using general packet radio service (GPRS) to connect to Internet Protocol (IP) data networks may also make the mobile device less popular compared to Internet-connected PC which use technologies such as asymmetric digital subscriber line (ADSL), cable or broadband wireless.

However, there is also recognition that such threats, while emerging, are quite real. Some data show that although still relatively small in comparison to the amount of PC malware, mobile malware, which first appeared in 2004, increased from only a few instances to over 300 in total in a two-year period (Hypponen, 2006).

Further, concerns about security increase as mobile devices become more prevalent and are used to access more critical or ‘valuable’ services.[17] For example, the use of smartphones is on the rise with projections as high as 350 million in use by 2009 (Hypponen, 2006). In 2006, Apple announced that a number of video iPods had been shipped to customers with the RavMonE virus.[18] Many experts are concerned that mobile malware will soon become far more dangerous to the mobile devices themselves, the wireless networks over which those devices communicate and the corporate networks, servers and/or personal computers with which those devices exchange information. Undetected malware on a smartphone could get transferred to a corporate network and used to perform further malicious functions (iGillottResearch Inc, 2006).

The Malware Internet: botnets

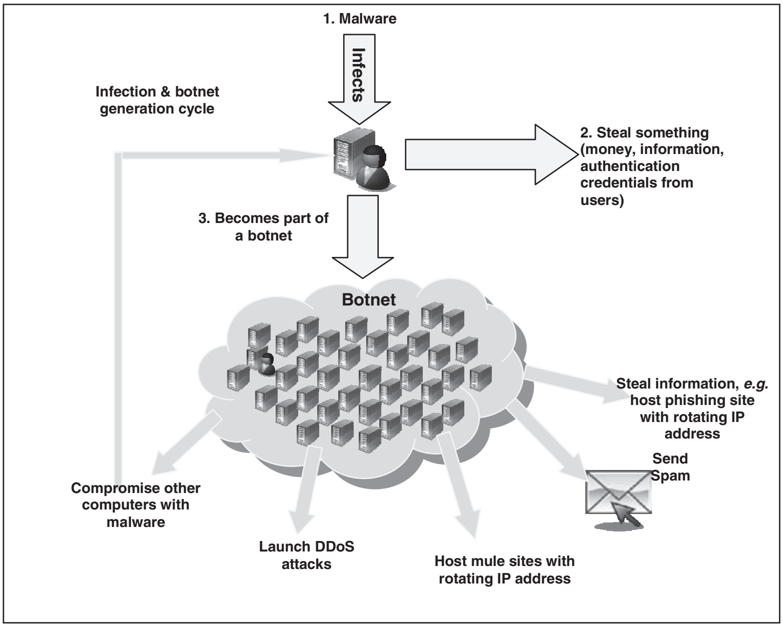
What is a botnet?

A now prevalent form of malware, botnets are key tools attackers use to conduct a variety of malicious activity and cybercrime. A botnet is a group of malware infected computers also called “zombies” or bots that can be used remotely to carry out attacks against other computer systems.[19]

Bots are generally created by finding vulnerabilities in computer systems, exploiting these vulnerabilities with malware, and inserting malware into those systems, *inter alia*. Botnets are maintained by malicious actors commonly referred to as "bot herders" or "bot masters" that can control the botnet remotely. The bots are then programmed and instructed by the bot herder to perform a variety of cyber attacks, including attacks involving the further distribution and installation of malware on other information systems. Malware, when used in conjunction with botnets, allows attackers to create a self-sustaining renewable supply of Internet-connected computing resources to facilitate their crimes (see Figure 3). Some of the malware discussed earlier in this report is distributed using botnets. There is thus a cyclical relationship: malware is used to create botnets, and botnets are used to further distribute spam and malware.

Figure 1.3 demonstrates the relationship between malware and the botnet lifecycle. When malware infects an information system, two things can happen: something can be stolen (*e.g.* information, money, authentication credentials etc.) and the infected information system can become part of a botnet. When an infected information system becomes part of a botnet it is then used to scan for vulnerabilities in other information systems connected to the Internet, thus creating a cycle that rapidly infects vulnerable information systems.

Figure 1.3 The botnet lifecycle


1. Malware
Infects
Infection & botnet generation cycle
2. Steal something (money, information, authentication credentials from users)
3. Becomes part of a botnet
Botnet
Steal information, *e.g.* host phishing site with rotating IP address
Send Spam
Compromise other computers with malware
Launch DDoS attacks
Host mule sites with rotating IP address

What are botnets used for?

Botnets are mostly used for the following purposes:

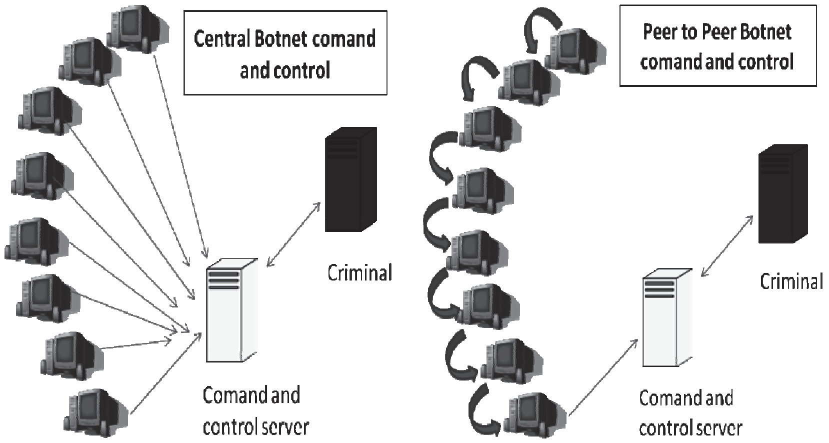
- Locate and infect other information systems with bot programmes (and other malware). This functionality in particular allows attackers to maintain and build their supply of new bots to enable them to undertake the functions below, *inter alia*.
- Conduct distributed denial of service attacks (DDoS).
- As a service that can be bought, sold or rented out.
- Rotate IP addresses under one or more domain names for the purpose of increasing the longevity of fraudulent web sites, in which for example host phishing and/or malware sites.
- Send spam which in turn can distribute more malware.
- Steal sensitive information from each compromised computer that belongs to the botnet.
- Hosting the malicious phishing site itself, often in conjunction with other members of the botnet to provide redundancy.
- Many botnet clients allow the attacker to run any additional code of their choosing, making the botnet client very flexible to adding new attacks.

Botnets Command and Control (C&C) models

Typically, bots communicate with the bot master through an Internet Relay Chat (IRC) command and control (C&C) server which provides the instructions directing the operation of the botnet. The C&C server usually is also itself a compromised computer running various network services. After a computer system is infected and compromised by a bot program, the bot periodically connects back to the C&C server, checking for instructions. Although there are various C&C models, the most popular has traditionally been the centralised model (see Figure 1.4) where all bots report to a single location to wait for commands. The centralised model is popular among bot masters because it offers software tools that make it easy to operate. Furthermore, the centralised model results in few communication delays between the bot master and the bots (Trend Micro, 2005). Increasingly, attackers are also using the HTTP and HTTPS web protocols[20] as the communication method between bots and the C&C server. This means that it is more difficult for network operators to detect and block bot communications to or from their network as it is hidden among the vast volume of normal web traffic.

An alternative innovative C&C model designed to make it more difficult for security practitioners to stop botnet hosted attacks is the increasing use of the peer to peer (P2P) model (see Figure 1.4) (Govcert.nl, 2007). The peer to peer model lacks a central hierarchy of communication which makes the botnet more resilient to dismantling (Trend Micro, 2005). It is therefore extremely difficult to stop attacks launched from botnets that communicate using P2P as there is no single point of failure.

Figure 1.4 Command and control for botnets


Central Botnet comand and control
Criminal
Comand and control server
Peer to Peer Botnet comand and control
Criminal
Comand and control server

In addition to the models above, botnets are increasingly using what is known as "fast flux" networks to evade detection. Fast flux networks are networks of compromised computer systems with public DNS records that change constantly thus making it more difficult to track and shut down malicious activity (The Honeynet Project, 2007). Furthermore, this model abandons the traditional centralised C&C server and uses proxies to hide the servers controlling the fast flux network.

Botnet figures

While botnets vary in size, they typically number tens of thousands of compromised computers. There have been exceptions including a group of attackers in The Netherlands who reportedly controlled 1.5 million bots (Govcert.nl, 2006). Typically, the number of bots being controlled by a single attacker will fluctuate depending on whether the compromised computers are connected to the Internet, whether they have been "cleaned", or whether the attacker is using his botnet to locate and compromise more information systems to add to the botnet. Furthermore, there are incentives for bot herders to use smaller botnets and launch smaller, more targeted, attacks to avoid detection. For example, large botnets sending spam or conducting DDoS attacks generate a high volume of network traffic that is usually detectable by ISPs and network administrators, whereas smaller attacks that use less bandwidth may go undetected.

Botnets have become a contracted commodity. Malicious actors can hire or buy a bot master to carry out an attack. One report averaged the weekly rental rate for a botnet at USD 50-60 per 1 000-2 000 bots, or around 33 cents per compromised computer (MessageLabs, 2006). This is extraordinarily cheap compared to the cost of the computer to the legitimate owner in terms of hardware, software and bandwidth.

Box 1.3 The Dutch botnet case

In October 2005 the Dutch National Police arrested three men – members of a group of cyber criminals – suspected of large scale "hacking". The men controlled several botnets that were thought to have consisted of over 1.5 million infected computers. The botnets played a key role in numerous cyber crimes including: phishing, identity theft, online fraud, and online extortion. In due course, it became clear that botnets played a central role in the activities of the cyber criminals by serving as the basic infrastructure that allowed for the successful attacks.

In June 2005 a report was made to the CERT community in the Netherlands that an important Netherlands-based computer centre had been hacked. The CERT community in turn reported the incident to the High Tech Crime Unit (formerly the Dutch National High Tech Crime Center) of the Dutch National Police.

Based on information combining IP addresses and the name of the suspect with a broadband Internet connection in use at his home address, the prosecutor formally requested the interception of Internet traffic in order to collect more evidence. To determine the size of the botnet and the illegal activities of the suspect, all IRC protocol traffic in the intercepted data was analysed. It was clear that this botnet was very large and used multiple IRC channels on multiple IRC servers. In this specific investigation, the team realised that the criminals controlled at least two large botnets used for their cyber crimes and that even after apprehending the criminals, the possibility existed that the botnets would still be operational. Together with the CERT community and several large ISPs, the team undertook action to dismantle the botnet and prevent it from growing and to disrupt its malicious function. It was agreed that the most suitable timing for the disruptive action was immediately after the arrests.

The prevalence of botnets has been increasing. Although estimates of the number of botnets can vary widely, most experts agree it is a large amount. For example, in 2006, the Chinese National Computer Network Emergency Response Technical Team Coordination Center (CNCERT/CC) reported that 12 million IP addresses in China were controlled by botnets (Du, 2007). They also found more than 500 botnets and more than 16 000 botnet command and control servers outside China.

Botnets and broadband

The increased threat of botnets can partially be explained by the increased use of broadband connections to access the Internet. Further efforts are needed from users, as well as providers, to protect their security and privacy in the online environment. By 2004, broadband Internet connections were already widespread in OECD countries. For example, in Korea 86% of households and 92% of businesses had a broadband connection via a computer or mobile phone in 2004 (OECD, 2005). In the following two years, those numbers have continued to increase. At the end of 2005, there were around 265 million active subscribers to fixed Internet connections in OECD countries. Of these, 60% were using broadband access, and broadband subscriptions have increased by more than 60% a year over the last five years. By mid-2006, there were more than 178 million broadband subscribers in the OECD area. European countries have continued to advance, with Denmark, the Netherlands and Iceland overtaking Korea and Canada in terms of broadband penetration rates over the past year (OECD, 2007).

The broadband transition to faster upload bandwidth via fibre could make the botnet problem much more severe. The potency of one infected computer on a fibre connection could be equivalent to 31 infected computers on DSL and 44 computers on cable networks.[21] This will be one of the key areas of concern for policy makers dealing with telecommunication networks and security in the near future.

Spam and botnets

There is a correlation between botnets and spam due to changes in spamming techniques over the last few years. Spam commonly refers to bulk, unsolicited, unwanted and potentially harmful electronic messages (OECD, 2006). Attackers have found convenience in co-operating with spammers by using their e-mail lists to send mass quantities of spam – which often contain other malware as an e-mail attachment – through botnets (Sophos, 2006a). For example, the second most common malicious code family reported from January - June 2006, Bomka, was a Trojan downloadable from a link provided in a spam e-mail that used social engineering techniques to persuade the user that the link was the site of a video clip (Symantec, 2006). The problem of spam and malware is also cyclical and self-sustaining. Information systems compromised by malware are used to distribute spam and a proportion of the spam that is distributed is designed to distribute malware to new victims whose information systems will be used to undertake further online malicious activity.

It is important to note that not all spam contains malware, and it is often difficult to determine how much spam *directly* contains malware. Manual analysis conducted by The Information and Communication Security Technology Center (ICST) in Chinese Taipei over the course of two years on 417 suspect e-mails found that of those 417 analysed, 287 (68%) contained malware attachments (Liu, 2007, p. 3).[22] Other data shows that in 2006, only 1.5%, or 1 in every 67.9 e-mails analysed, contained a virus or Trojan; and according to the same report, in 2005 the annual average was 2.8%, or 1 in every 36.1 (MessageLabs, 2006). It is likely that the disparate nature of these findings can be explained by a lack of comparable techniques to determine when spam contains malware.

Recently, the Messaging and Anti-Abuse Working Group (MAAWG) reported that the percentage of email identified as "abusive"[23] has been oscillating between 75% and 80% (Messaging Anti-Abuse Working Group, 2007). They attribute the fluctuation to service providers dealing with new schemes introduced by abusers to escape service providers' detection methods, including filters. Nonetheless, it is widely accepted that the vast majority of spam is sent from botnets. The effectiveness and wide availability of compromised information systems with high speed broadband connections means that spam levels are at their highest levels ever despite many initiatives to reduce and prevent spam being distributed.

Although civil enforcement against spam, such as the case described above, is important, most instances of malware are inherently criminal, and criminal law enforcement agencies are best suited to expertly shut down their criminal operations.

Box 1.4 FTC v. Dugger

In one recent case, the US Federal Trade Commission (FTC) sought to stop the underlying use of botnets to send spam (FTC v. Dugger). The FTC alleged that the defendants relayed sexually explicit commercial e mails through other people's home computers without their knowledge or consent. They further alleged that the defendant's conduct violated the CAN SPAM Act. Under the final order, the defendants were barred from violating the CAN SPAM Act and required to turn over USD8 000 in profits made through use of the botnet. The defendants were also required to obtain the authorisation of a computer's owner before using it to send commercial e-mail and to inform the owner how the computer will be used.

The role of blacklists in combating botnets

Blacklisting is a loosely used term typically referring to the practice of using so-called DNS Blacklists (DNSBL) to filter incoming Internet traffic. Mail servers may be configured to refuse mail coming from IP addresses, IP ranges or whole networks listed on a specific DNSBL. There is a wide variety of blacklists that may be used in different combinations.

Most of the lists are free and run by volunteers, though their operations may be funded through external sources. Each DNSBL has its own criteria for including an IP address in the list and its own procedure for getting an address off the list. Spamhaus, an international non-profit organisation funded through sponsors and donations, maintains several well-known blacklists – though they prefer the term block lists – which they claim are used to protect over 600 million user inboxes. One of their lists contains the addresses of “spam-sources, including spammers, spam gangs, spam operations and spam support services”; another list focuses on botnets which run open proxies. It should be noted at this point that blacklisting, while potentially powerful, has drawn its own criticisms – regarding, among other things, vigilantism of blacklist operators, listing false positives, the collateral damage that may come with blacklisting certain IP addresses or ranges, and the financial motives of some list operators. Furthermore, blacklists have faced legal challenges from spammers, who on occasion were successful in obtaining court verdicts against being blacklisted. According to interviewees in a recent empirical study, most ISPs use blacklists (Eeten and Bauer, 2008).

Blacklisting and ISPs[24]

Blacklisting does provide an incentive to invest in security because it directly impacts an ISP's business model. For example, one medium-sized ISP reported a security incident where 419 spammers[25] set up over 1 000 e-mail accounts within their domain and then started pumping out spam. That got the ISP's outbound mail servers blacklisted, which resulted in a high volume of calls to their customer centre by customers who noticed their e-mail was no longer being delivered. That number doesn't include the incoming abuse notifications, of which there were purportedly "even more." In another example, a security officer at a large ISP explained that being blacklisted led to a much more proactive approach to remove bots from their network, including the purchase of equipment that automates the process of identifying infected machines on the network (Eeten and Bauer, 2008). In mid-2007, this particular ISP identified around 50 customers per day and, if the customer did not resolve the problem, the connection was suspended.

There are various levels of blacklisting used to incite a response from an ISP. At the lower end, there is blacklisting of individual IP addresses, *i.e.*, an individual customer. This has "exactly zero impact on the ISP," said a security expert. Only when the number of listed IP addresses reaches a certain threshold might the problem get an ISP's attention. According to the expert, ISPs mostly ignore listed individual IP addresses, because of the relatively high costs of dealing with them (*e.g.* through customer support). Furthermore, particular IP addresses get taken off the blacklist as spammers or attackers move on to other infected machines.

More powerful incentives are the blacklisting of whole IP ranges and of outbound mail servers. These typically do get the ISPs' attention and lead to remedial action on their end, though the effectiveness varies with the degree of vigilance applied by the ISP. The most extreme form is blacklisting an entire network (*i.e.*, all IP addresses of an ISP). This is only used against semi-legitimate ISPs who do not act against spam, and against known spam-havens.

Blacklisting and Domain Name Registrars

Registrars offering hosting and e-mail services are subject to blacklisting along the same lines as the ISPs. Blacklist operators also watch registrars and their responsiveness to abuse complaints. In extreme cases, blacklists may include the registrar itself. A case in point is the recent dispute between the blacklist operator Spamhaus and the Austrian registry/registrar Nic.at. Spamhaus had requested Nic.at to remove several domain names it said were associated with phishing by the "rock phish" gang. Nic.at did not comply with these requests, citing legal constraints. The registrar argued that it could not legally remove the sites, unless Spamhaus provided clear proof that the domain names had been registered using false information (Sokolov, 2007). The conflict escalated when Spamhaus added the outbound mail server of Nic.at to one of its blacklists – listing them as "spam support" – so that the registrar's e-mail was no longer accepted by the multitude of servers using this popular blacklist. About ten days later Spamhaus changed the listing of Nic.at to a symbolic listing – no longer actually blocking the IP addresses, but keeping them listed as "spam support." Several of the offending domains had been removed, but Nic.at denies that it had complied with Spamhaus' request and asserts that the hosting providers took action (ORF, 2007; Spamhaus, 2007).

Notes

1. The 1992 OECD *Guidelines for the Security of Information Systems and Networks* defined an information system as computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programmes, specification and procedures for their operation, use and maintenance.
2. See the Glossary of Malware Terms at the end of this book.
3. For example, W32.Sober@mm (also known as Sober) was the primary source code of the "Sober" family. Sober.X is a variant of Sober. (See Symantec, 2006, p.67).
4. Host refers to a computer at a specific location on a network.
5. See Chapter 2 for a discussion of digital certificates.
6. Servers are generally more powerful computers which provide services to (and accept connections from) many clients however home PCs and corporate workstations can also act as servers, particularly when they become compromised. Common types of servers include web, e-mail and database servers.
7. Script Kiddie refers to an inexperienced malicious actor who uses programmes developed by others to attack computer systems, and deface websites. It is generally assumed that script kiddies are kids who lack the ability to write sophisticated hacking programmes on their own and that their objective is to try to impress their friends or gain credit in underground cracker communities.

8. Malware may also exploit vulnerabilities in hardware, however, this is rare compared to the number of software vulnerabilities which are available at any given time to exploit.

9. See the Glossary of Malware Terms at the end of this book.

10. Social engineering refers to techniques designed to manipulate users into providing information or taking an action which leads to the subsequent breach in information systems security.

11. See Box 1.2 for additional detail of propagation vectors.

12. Bluejacking consists in sending unsolicited messages to Bluetooth connected devices. Bluesnarfing enables unauthorised access to information from a wireless device through a Bluetooth connection.

13. While Bluetooth can have a range of 100 metres for laptops with powerful transmitters, it has a more limited range for mobile phones, usually around 10 metres.

14. A Smartphone is a cellular phone coupled with personal computer like functionality.

15. A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves, or for connecting to a higher level network and the Internet.

16. These transactions are possible as is demonstrated by the Japanese market. See BBC (2007)b).

17. For example, some financial institutions that wish to implement transaction signing and avoid providing customers with a separate smart card reader, may in future provide support for transaction signing through the use of a customer's own mobile telephone PDA. In this way, the mobile PDA also is likely to be targeted to subvert the transaction signing process. As discussed in the glossary, transaction signing is only effective if the keyed hash for the transaction is calculated on a device that can be trusted.

18. Note that the virus was transmitted to the device through a Windows computer on the production line. See *http://www.apple.com/support/windowsvirus/*.

19. In this paper, the term "bot" refers to a malware-infected computer that a malicious actor can remotely control and turn into a "robot" or zombie machine. Thus "botnets" should be understood as networks of such bot machines. However, the term "bot" can be encountered in other contexts as it generally refers to a variety of software programme or script that

executes automated tasks. It is most widely used in the context of Internet Relay Chat (IRC) where users can create and use bot scripts for online gaming, co–ordinating file transfers, and automating channel admin command (EggDrop is one of the oldest of such benign IRC bots). The fact that botnets often rely on IRC bots for command and control by botmasters might explain why the term "bot" is so popular in the literature and discussions related to malware.

20. This is the same protocol that enables both encrypted (https) and unencrypted (http) web based communications to occur. Blocking this traffic would prevent web access to a network.

21. One infected computer on a fibre connection with 100 Mbit/s of upload capacity could theoretically cause as much damage as 390 infected computers with upload speeds of 256 kbit/s. The average advertised upload speeds for broadband in the OECD in October 2006 was 1 Mbit/s for DSL, 0.7 Mbit/s for cable and 31 Mbit/s for FTTx.

22. Note that this data is based on self-selected spam that fits a certain category or type and therefore is representative of a smaller sample set. Furthermore, this data does not include the mass mailing worms/viruses.

23. MAAWG uses the term "abusive" because definition of spam can vary greatly from country to country.

24. This text has been extracted from the original report. See Eeten, M. J. van and J. M. Bauer (2008), pp. 33-34.

25. This is an advance-fee fraud in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. Among the variations on this type of scam are the Nigerian Letter (or 419 fraud). The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.

Chapter 2. Malware Attacks: Why, When and How?

Types of malware attacks

The numerous types of malware can be used separately or in combination to subvert the confidentiality, integrity and availability of information systems and networks. Likewise, a range of different attacks can be conducted to reach different goals, such as denying access to critical information systems, conducting espionage, extorting money (*e.g.* ransom), or stealing information (*e.g.* ID theft). Malware can also be used to compromise authenticity and non-repudiation, or conduct attacks on the Domain Name System (DNS).[1]

Denying access

Denying access to digital data, network resources, bandwidth, or other network services (denial of service – DoS) is a common goal of attacks using malware. Popular targets include companies that conduct business online and risk losing significant revenue for every minute their website or network is unavailable, and governments who rely on websites to provide essential services to their citizens. These attacks are usually used for sabotage (for example, to hurt a competitor or an organisation against whom the attacker holds a grudge or grievance), extortion, or for politically and ideologically motivated purposes (Messmer and Pappalardo, 2005).

Distributed Denial of Service (DDoS) attacks

The most well known and perhaps most common method to deny access is distributed denial of service attacks (DDoS). DDoS attacks seek to render an organisation's website or other network services inaccessible by overwhelming them with an unusually large volume of traffic.[2] Malware indirectly contributes to DDoS attacks by creating a renewable supply of compromised computers (bots[3]) through which the flood attacks are launched. DDoS traffic may consist of relatively easily identified bogus packets, or properly-formed and seemingly legitimate "requests for service." This flood of traffic is intended to exceed the capacity of either the network bandwidth or the computer resources of the targeted server, or both, thereby making the service unavailable to most or all of its legitimate users, or at least degrading performance for everyone.

Simple DDoS attacks use a distributed network of bots (called a botnet) to attack a particular target. The more complex DDoS attacks use multiple botnets to simultaneously attack the target. In traditional DDoS attacks, botnets are used to send massive amounts of queries and overwhelm a system. However, low and slow attacks, a recent trend noted by some security experts, occur over a longer period of time and use a small amount of bandwidth from thousands, if not millions, of compromised computers. Often the attacker co-ordinates the attack so that not all the bots will attack the target at the same time, but rather on a rotating basis. The victim and the Internet Service Provider may not notice that their network traffic has increased but over time, it becomes a drain on their infrastructure and other resources.

Box 2.1 The Estonian case

In May 2007, a series of cyber attacks were launched against Estonian government and commercial websites. Some attacks involved defacing websites, and replacing the pages with Russian propaganda or bogus information. Up to six sites were rendered inaccessible at various points, including those of the foreign and justice ministries. Most of the attacks were launched using botnets comprised of many thousands of ordinary computers.

Estonia's computer emergency response team (EE-CERT) acted swiftly and, in collaboration with partners from the international community, was able to weather a very serious attack with little damage. The attack was primarily defended through filtering – blocking connections from outside Estonia. For example, Estonia's second largest bank, SEB Eesti Uhispank, blocked access from abroad to its online banking service while remaining open to local users. One major contributor to the stability of their services domestically during the attack was the fact that Estonia has two domestic Internet exchange points (IXPs).[4]

Three weeks after the attacks ended, one researcher identified at least 128 separate attacks on nine different websites in Estonia. Of these 128 attacks, 35 were reportedly against the website of the Estonian Police, another 35 were reportedly against the website of the Ministry of Finance, and 36 attacks were against the Estonian parliament's, prime minister's, and general government websites.

It has further been estimated that some of the attacks lasted more than 10 hours, exceeded 95Mbps, and peaked at about million packets per second. While this may seem like a lot, other attacks considered "big" by security experts usually peak at about 20 million packets per second, 5 times more than the attack against Estonia. This has led experts to conclude that the attack was not optimised for maximum impact on and damage to the network, but rather to make a statement and prove a point.

Source: Lemos, R. (2007); The Economist (2007) and The Sydney Morning Herald (2007).

DDoS attacks have been launched against governments for various purposes including political or ideological ones. For example, Swedish government websites were attacked in the summer of 2006 as a protest against the country's anti-piracy measures. More recent events in Estonia have raised an interesting discussion on what a cyber attack of this nature means for countries.[5]

Indirect attacks on the DNS

Attacks using **"recursive resolvers".** While these attacks use recursive resolvers as their force-multiplier, they need not be directed at DNS targets at all, although that's where they do the most damage. They can just as easily use the DNS to conduct DDoS attacks against other targets. This type of attack uses the DNS as a weapon against something else, whereas the attacks against the DNS root servers, described above, use something else as a weapon against the DNS.

These attacks are often possible due to poor configuration of an organisation's DNS server, which allows it to service DNS requests from anywhere on the Internet – not just from its own network. Recursive DNS attacks are indirectly related to malware only in so far as they use a small number of compromised information systems to send fake DNS requests. Unlike other forms of DDoS attack, it does not depend on a large number of bots to work or be more effective. It is important to note that the purpose of recursive or amplification attacks is not to deny service to the DNS system itself, but rather to the DNS server of a single organisation. This has the impact of making the IP routing unresolved to the entity's domain name and making outbound DNS requests for the organisation difficult because of the consumption of resources at the organisation's DNS server. Although malware is not always directly involved, it is also an example of how a user or entity's configuration can have a negative impact on others' security.

Domain-name tasting. Another trend in which malware may be implicated, but not directly involved, is the practice of domain name tasting. Domain name tasting is the practice of adding a grace period[6] to the registration of domain names so that the registrants can test the profit potential of the domain names. During this period, registrants conduct a cost-benefit analysis to determine if the tested domain names return enough traffic to offset the registration fee paid to the registry over the course of the registration period. Domain name tasting allows registrants to exploit the add-grace period. When a domain name generates unsatisfactory profitability, it is returned before the fifth day for a full refund. Originally, the add-grace period was created to allow registrants to receive a refund in the case of mistake, or grant registrars a refund in the event a registrant's credit card was declined. The process has been exploited to permit the registration of domain names in bulk. Although difficult to prove, it is likely that these "tasted" domains are used to distribute malware.

Box 2.2 A closer look at DNS

The Domain Name System (DNS) is like an address book for the Internet. It helps users to navigate, send and receive information over the Internet. Every computer connected to the Internet uses a unique address which is a string of numbers called an "IP address" (IP stands for "Internet Protocol").[7] Because IP addresses are difficult to remember, the DNS makes using the Internet easier by allowing a familiar string of letters (called the "domain name") to be used instead of the numeric IP address. For example, instead of typing 193.51.65.37, users can type www.oecd.org. It is a "mnemonic" device that makes the addresses for computer hosts easier to remember.

A domain name consists of various parts, the top-level domain (TLDs) and the subdomains. TLDs are the names at the top of the DNS naming hierarchy. Commonly used generic TLDs include .com, .net, .edu, etc. Also, there are currently 244 country code TLDs (ccTLDs), such as .jp, .au, .de, etc. The administrator for a TLD controls the second-level names which are recognised in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognised by the DNS.

The root servers contain the IP addresses of all the TLD registries – both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .fr (France), .cn (China), etc. This is critical information. If the information is not 100% correct or if it is ambiguous, it might not be possible to locate a key service on the Internet. In DNS, the information must be unique and authentic.

The data in the DNS is stored in hierarchical and widely distributed sets of machines known as "name servers", which are queried by "resolvers". Resolvers are often part of the operating system or software on the user's computer. They are used to respond to a user's request to resolve a domain name – that is, to find the corresponding IP address.

Source: Internet Corporation for Assigned Names and Numbers, *www.icann.org/en/general/glossary.htm.*

Attacks that modify data

By its very nature, when malware infects or compromises a computer system, it involves an attack on the integrity of the information system in two fundamental ways. First, the steps involved in compromising the system result in unauthorised changes to the system itself and potentially any data stored, input or accessed via that system, including user input (keyboard or mouse), output (screen or printer), and storage (USB, hard disk or memory). Second, once a system is compromised, the integrity (*i.e.* trustworthiness) of the entire system can no longer be relied upon. Attacks on integrity are generally a precursor to other attacks, such as the theft of sensitive data, or can be a feature of an attack on authentication. However, attacks on integrity may be an end goal. For example, modifying entries in a database to facilitate fraud or deleting a company's customer database for commercial sabotage or modifying settings on a SCADA system used for gas distribution may be designed to lead to a harmful malfunction of that system.[8]

Another currently popular attack that modifies data is compromising a website and inserting an Iframe[9], which infects regular visitors to that site. Iframes can be inserted into legitimate websites to link to malware hosting sites that can then compromise the user.

Attacks on identity

There are substantial differences between statistical information gathered on ID theft by public authorities for policy purposes versus that gathered by private businesses for commercial purposes. Some sources conclude that the scale of ID theft has gone down in the past years, resulting in growing consumer confidence. In contrast, other sources advance figures reflecting an increase in ID theft. Furthermore, some financial institutions, which say that the costs are relatively modest, are not willing to reveal their own financial losses. On the other hand, other private bodies advance figures reflecting an increase in ID theft. To further complicate the landscape, some financial institutions even claim that none of their customers has ever been affected by a phishing attack (Devillard, 2006). Below are some data to illustrate the debate around ID theft:

- In 2006, the Netcraft toolbar, an anti-phishing tool developed by the Netcraft toolbar Community[10], blocked more than 609 000 confirmed phishing URLs, a substantive jump from 41 000 only in 2005 (Netcraft Toolbar Community, 2007). Netcraft views this dramatic surge, mainly concentrated in November- December 2006, as the result of recent techniques implemented by phishers to automate and propagate networks of spoof pages, enabling the rapid deployment of entire networks of phishing sites on cracked web servers.[11]
- In 2006, The Anti-Phishing Working Group reported an increase in cyber attacks from July to November 2006 (APWG, 2006a). In November 2006, 37 439 new phishing sites were detected, a 90%

increase since September 2006. However, in its December 2006 report the APWG notes a decrease in the number of new phishing sites (which dropped to 28 531) (APWG, 2006b).

- The US Federal Trade Commission reported in 2003 that ID theft affected approximately 10 million Americans each year (US FTC, 2003).[12] In 2007, another report found that ID fraud had fallen about 12% from USD 55.7 billion to 49.3 billion (Javelin Research and Strategy, 2007).
- However, the Javelin report was criticised and regarded as trying to persuade the opinion that "business are doing an adequate job in protecting consumers' personal information and that the onus in on consumers to better protect themselves" (Shin, 2007). A recent McAfee survey noted this discrepancy, considering Javelin's percentages as "surprisingly low" and comparing them to Gartner statistics, which, in contrast, in 2007, counted 15 million of Americans as victims of ID theft (McAfee, 2007).

Attacks on single and multi-factor authentication

Attacks on single-factor authentication, such as a username and reusable password, using malware are widespread and highly effective. Such attacks, like attacks on integrity, are precursors to stealing information of value via or from the compromised computer. Single-factor credentials for computer accounts, online banking accounts, virtual private network (VPN) remote access and the like are all vulnerable to capture via keyboard, screen, mouse or from protected storage (or similar areas) within the information system and are then easily replayed by an attacker to access the relevant accounts or systems.

Attacks on some forms of multi-factor authentication are also possible and have occurred. For example, most simple forms of multi-factor authentication, including the use of a hardware token which generates a one-time password and challenge-response with a short time to live are vulnerable to malware attack. For example, a Trojan, once installed on the user's computer simply waits for the user to establish a legitimate login session with their bank using their multi-factor credentials. Then the Trojan conducts a funds transfer in the background without the user's authorisation or knowledge. To the financial institution, the funds appear to have been transferred and authorised by the account user (F-Secure, 2007).

The feasibility of this type of malware attack has been demonstrated as recently as May 2007 and as early as 2005 (Dearne, 2007). For example, a Trojan was able to compromise the E-gold payment[13] system by waiting for the victim to successfully authenticate to E-gold's website, then creating a hidden browser session, and using various spoofing tricks to empty the victim's account. Because the stealing and spoofing started after the authentication is completed, it circumvented any authentication that was put in place. While the e-gold Trojan did not attack multi-factor authentication *per se*, it was an early example of malware able to transfer funds in the background after the user legitimately logs on to their e-gold account which could have defeated any type of multi-factor logon authentication that did not also implement transaction signing (Stewart, 2004).

Box 2.3 The two-factor token attack

A slight variation of the two-factor token attack involving a hybrid phishing and malware attack, reportedly targeted ABN AMRO's online banking customers recently. The attacker sent potential victims an e-mail purporting to be from their bank (*i.e.* ABN AMRO). If recipients opened an attachment to the e-mail, malware was installed on their computers without their knowledge. When the customers next visited their banking site, the malware redirected them to the attacker-controlled website that requested their security details, (*i.e.* their PIN) and one-time password (OTP) generated by the hardware token. As soon as the attackers received these details they were able to log into the customer's account at the real ABN Amro site, before the expiry of the automatically generated number enabling them to transfer the customer's money. As single-factor authentication for high value transactions are replaced by multi-factor authentication, this type of attack will become more commonplace.

Source: Outlaw.com (2007) and The Registar (2007).

Attacks on digital certificates and secure socket layer (SSL)

Digital certificates and Secure Socket Layer (SSL) connections are often used to protect the confidentiality and integrity of data sent over the Internet and to verify the authenticity of the remote host (most commonly to authenticate a remote server). While these protections are useful, they do not provide security at the end points of a transaction, but generally only the channel in between. While an SSL session is established, data needs to be encrypted and decrypted as data are transferred back and forth between the end points. When a users' machine has been compromised by malware[14], the data being sent can be captured *before* encryption occurs – and for data received – *after* it has been decrypted. Efforts to provide a higher level of assurance for some types of digital certificates will not address this problem.

SSL certificates provide a means for consumers to verify the identity of a website. However, there are several problems associated with the current use of SSL certificates for this purpose:

- Errors and warnings due to invalid SSL certificates are frequently highly technical in nature and therefore confusing to users.
- According to one usability study performed, consumers most often ignore the absence of an SSL connection before entering personal data, or ignore warnings provided (Dhamija, 2007).
- When organisations use self-signed certificates, "untrusted signer" warnings may be displayed and generate confusion for users.
- In some cases, malicious site operators have been able to obtain legitimate SSL certificates from Certificate Authorities (Krebs, 2006).[15]

Box 2.4 The problem with digital certificates and SSL

A digital certificate[16] is a mechanism to establish the credentials of a person or entity conducting business or transactions online. It is often used within SSL[17] protected sessions. The use of digital certificates within SSL protected sessions is a means of building trust and confidence in e-commerce and e-government transactions. However, some forms of malware when installed on a user's computer can wait for a legitimate SSL session to be established with a particular website, for example a specific online banking site, and then inject HTML code into the browser interface before the legitimate remote web site page renders on the user's computer.

This has the effect of changing the content and appearance of the web page (even though the remote site has not been modified), while the user's computer still maintains a valid SSL connection with the remote host. A check of the SSL digital certificate, by the user, will show that it is a valid certificate for the remote host. What the user sees on the screen and the data the user is prompted to input, however, differ from the contents of the legitimate remote site.

By manipulating the compromised computer's browser interface, attackers make it virtually impossible for users to know whether or not they have a secure connection with a legitimate remote host – and by inference – whether what they see in the browser window is the content of the legitimate remote host. Therefore, the use of digital certificates within SSL-protected sessions, as a means of reliably verifying the identity of a remote web domain, has been fundamentally undermined.[18]

Why attacks are perpetrated

Extorting money: ransom

Some malware is designed to encrypt or scramble users' data so that the owner cannot retrieve it. Often the owner will be asked to pay a ransom for the "key" used to encrypt their data, and which is often required to reverse that process and restore the data.[19] Although this type of malware is not as prevalent as other types of malware, there were several high profile cases in 2006 that raised attention around the issue (Sophos, 2007a). Such attacks, not only deny the user/owner access to their own data, but harm the confidentiality and integrity of that data by the attacker's unauthorised access to it and encryption of it.

Box 2.5 A ransom example: the Arhiveus

In June 2006, a Trojan horse attacked files in Microsoft Windows users' "My Documents". The files were then encrypted so users could not access them without paying a ransom in return for the restoration of the files.

When users tried to access their files, they were directed to a file containing instructions on how to recover the data. The instructions began:

> *INSTRUCTIONS HOW TO GET YOUR FILES BACK READ CAREFULLY. IF YOU DO NOT UNDERSTAND - READ AGAIN.*
>
> *This is the automated report generated by auto archiving software.*
>
> *Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder My Documents was archived with long password.*
>
> *You cannot guess the password for your archived files - password length is more than 30 symbols that makes all password recovery programmes fail to brute force it (guess password by trying all possible combinations).*
>
> *Do not try to search for a programme that encrypted your information - it simply does not exist in your hard disk anymore. Reporting to police about a case will not help you, they do not know the password. Reporting somewhere about our email account will not help you to restore files. Moreover, you and other people will lose contact with us, and consequently, all the encrypted information.*

In many of these cases the attacker encrypts files such as personal photographs, letters, household budgets and other content. To retrieve their data, users were required to enter a 30 character password which they were told would be available after making purchases from one of three online drug stores.

Source: Sophos (2007b), "Security Threat Report Update July 2007", *www.sophos.com/security/whitepapers/*, accessed 12 December 2007.

Espionage

Malware can be and has been used to gain access to or spy on business and government operations and gather information that could be critical to business operations or national security. Recently, the United Kingdom reported that a number of targeted Trojan attacks had been directed against parts of the UK's public and private critical information infrastructure. These Trojans were assessed to be seeking covert gathering and transmitting of privileged information (NISCC, 2005). Malware of this sort can also be used by companies and other organisations to gather information about their competitors as demonstrated by the below example.

Box 2.6 The case of Michael and Ruth Haephrati

In March of 2006, Michael and Ruth Haephrati were extradited to Israel from Britain where they were charged with creating and distributing a Trojan used to conduct industrial espionage against some of the biggest companies in Israel. Michael Haephrati is said to have developed and refined the programme while his wife, Ruth, managed business dealings with several private investigation companies which bought it and installed it on the computers of their clients' competitors. Specifically, the Trojan horse is believed to have been used to spy on the Rani Rahav public relations agency (whose clients include Israel's second biggest mobile phone operator, Partner Communications), and the HOT cable television group. Another alleged victim was Champion Motors, who import Audi and Volkswagen motor vehicles.

Ruth Brier-Haephrati was formally charged with aggravated fraud, unlawful computer access, virus insertion, installing tapping equipment, invasion of privacy, managing an unlawful database, and conspiracy to commit a crime. Michael Haephrati was charged with lesser offenses as the prosecution regarded him as Ruth's assistant because his job was only to perfect the programme and tailor it to the needs of specific clients.

Source: Messagelabs (2006) and Sophos (2006c).

Stealing information

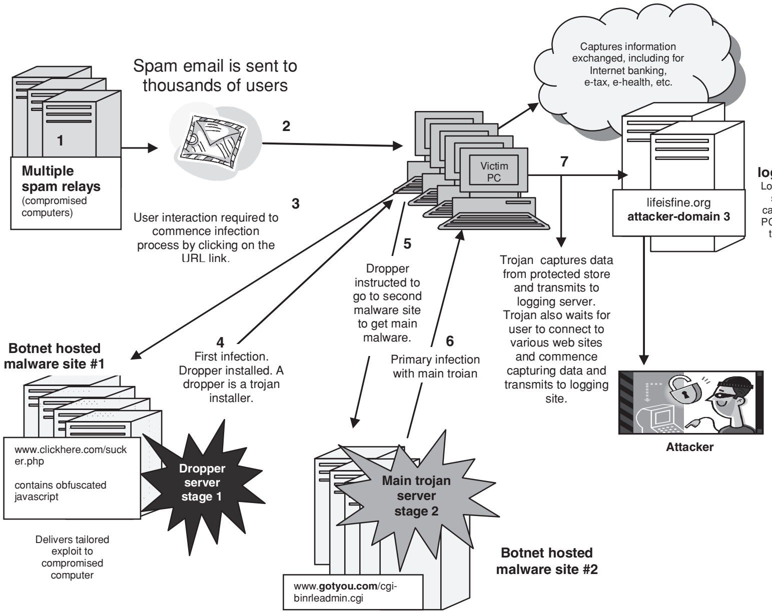
Over the past five years, information theft, and in particular online identity (ID) theft[20], has been an increasing concern to business, governments, and individuals. Although malware does not always play a *direct* role[21], ID theft *directly* using malware has become increasingly common with the rise of backdoor Trojans and other stealthy programmes that hide on a computer system and capture information covertly.

As illustrated in Figure 2.1, online ID theft attacks using malware can be complex and can use multiple Internet servers to distribute spam and malware, compromise users' information systems, and then log the stolen data to another website controlled by the attacker or send it to the attacker's e-mail account. Generally, the attacker operates under multiple domain names and multiple IP addresses for each domain name and rapidly rotates them over the life of the attack (for example see botnet hosted malware sites 1 and 2 in Figure 2.1).[22]

The use of multiple domain names and multiple hosts or bots (and their associated IP addresses) is designed to increase the time available for capturing the sensitive information and reduce the effectiveness of efforts by affected organisations (such as banks), CSIRTs and ISPs to shut down fraudulent sites. Under the domain name system (DNS), attackers are able to quickly and easily change their DNS tables[23] to reassign a new IP addresses to fraudulent web and logging sites operating under a particular domain.[24]

The effect is that as one IP address is closed down, it is trivial for the site to remain active under another IP address in the attacker's DNS table. For example, in a recent case IP addresses operating under a single domain name changed on an automated basis every 30 minutes, and newer DNS services have made it possible to reduce this time to five minutes or less. Attackers may use legitimate existing domains to host their attacks, or register specially created fraudulent domains. The only viable mitigation response to the latter situation is to seek de-registration of the domain (AusCERT, 2006).

Figure 2.1 Online ID theft attack system involving malware

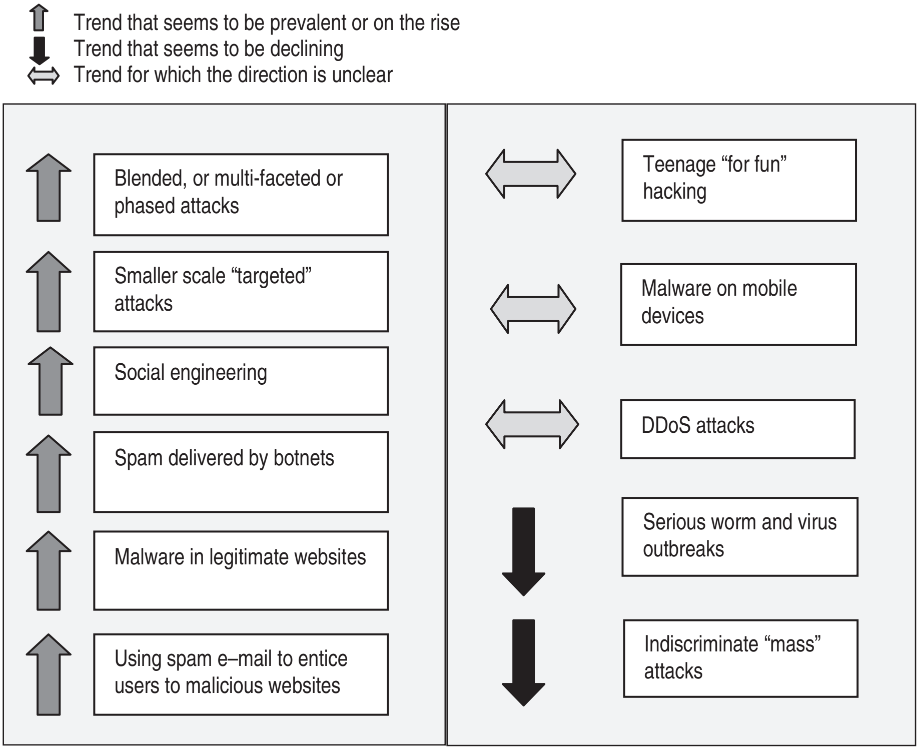

Spam email is sent to thousands of users
1
Multiple spam relays
(compromised computers)
2
Captures information exchanged, including for Internet banking, e-tax, e-health, etc.
Victim PC
7
Botnet hosted logging site
Logging site for stolen data captured when PC connects to the Internet.
lifeisfine.org
attacker-domain 3
3
User interaction required to commence infection process by clicking on the URL link.
5
Dropper instructed to go to second malware site to get main malware.
Trojan captures data from protected store and transmits to logging server. Trojan also waits for user to connect to various web sites and commence capturing data and transmits to logging site.
4
First infection. Dropper installed. A dropper is a trojan installer.
6
Primary infection with main trojan
Botnet hosted malware site #1
www.clickhere.com/sucker.php
contains obfuscated javascript
Dropper server stage 1
Delivers tailored exploit to compromised computer
Main trojan server stage 2
Botnet hosted malware site #2
www.gotyou.com/cgi-binrleadmin.cgi
Attacker

Source: AusCERT (2006) "Haxdoor – An anatomy of an online ID theft Trojan", *www.auscert.org.au/render.html?cid=1920*, last accessed 10 December, 2007.

Malware attack trends

The dynamic nature of malware keeps most security experts constantly on the lookout for new types of malware and new vectors for attack. Due to the complex technical nature of malware, it is helpful to examine overall attack trends to better understand how attacks using malware are evolving. As mentioned previously, the use of malware is becoming more sophisticated and targeted. Attackers are using increasingly deceptive social engineering techniques to entice users to seemingly legitimate web pages that are actually infected and/or compromised with malware. Figure 2.2 illustrates the types of attack that seem to be on the increase, those that are falling out of favour, and those for which the trend remains unclear or not changed.

Figure 2.2 General attack trends


⇧ Trend that seems to be prevalent or on the rise
⬇ Trend that seems to be declining
⇔ Trend for which the direction is unclear
Blended, or multi-faceted or phased attacks
Smaller scale “targeted” attacks
Social engineering
Spam delivered by botnets
Malware in legitimate websites
Using spam e–mail to entice users to malicious websites
Teenage “for fun” hacking
Malware on mobile devices
DDoS attacks
Serious worm and virus outbreaks
Indiscriminate “mass” attacks

Origin of malware attacks

Origin refers to both where the attackers who launch the attack are based and where the computer systems that actually attack the targeted system are located. In most cases, it is easy to see where the attacking computer systems are hosted based on their Internet protocol or "IP" addresses, but this is not usually sufficient to identify the person responsible for launching the attack. For example, "spoofing" is a technique designed to deceive an uninformed person about the origin of, typically, an e-mail or a website.[25]

Moreover, rarely is the attacker located in the same geographic region as the attacking hosts. It is common practice among cybercriminals[26] to use compromised computers (and to a lesser extent anonymous proxies[27]) hosted in a foreign legal jurisdiction to launch their attacks. This protects their identity and provides additional computing resources beyond what they could otherwise afford. Criminals are acutely aware of the significant jurisdictional impediments that hinder or even prevent cybercrime investigations from being conducted if the crimes are sourced internationally.

Malware is now spread around the world and rankings[28] tend to show that a whole host of countries across the developed and the developing world are home to online criminals using malware. Although attacks originating from one country may have local targets, the predominant trend is attacks that originate internationally relative to their targets. In addition, geography may play a role depending on the end goal of the attacker. For example, broadband Internet speeds differ from country to country. If an attacker wishes to maximise network damage, he/she may use compromised computers located in countries where broadband is prevalent. If the goal is to degrade service or steal information over time, the attacker may use compromised computers from a variety of geographical locations. Geographical distribution allows for increased anonymity of attacks and impedes identification, investigation and prosecution of attackers.

Figure 2.3 Malicious actors

The Innovators

Who? Focused individuals who devote their time to finding security holes in systems or exploring new environments to see if they are suitable for malicious code

Why? Challenge

How? Embrace the challenge of overcoming existing protection measures

The Amateur Fame Seekers

Who? Novices of the game with limited computing and programming skills

Why? Desire for media attention

How? Use ready-made tools and tricks

The Copy–Catters

Who? Would be hackers and malware authors

Why? Desire for celebrity status in the cybercrime community

How? Interested in recreating simple attacks

The Insiders

Who? Disgruntled or ex-employees, contractors and consultants

Why? Revenge or theft

How? Take advantage of inadequate security aided by privileges given to their position within the workplace

Organised Crime

Who? Highly motivated, highly organised, real-world cyber-crooks; Limited in number but limitless in power

Why? Profit

How? A tight core of masterminds concentrated on profiteering by whichever means possible –surrounding themselves with the human and computer resources to make that happen.

Source: McAfee Inc. (2006), "Virtual Criminology Report 2007 Organized Crime and the Internet", p.9, *www.mcafee.com/us/threat_center/white_paper.html.*

The malicious actors

Who are the malicious actors?

Research shows that the range of malicious actors developing and deploying malware spans from amateurs seeking fame to serious organised cyber criminals. It can also be assumed that nation states have the same capabilities. Figure 2.3 diagrams the malicious actors from the "Innovators" to “Organised Crime”[29] based on a recent report on criminal activity on line. It is important to note, however, that there is also a whole category of actors whose motivations are political or ideological rather than solely financial.

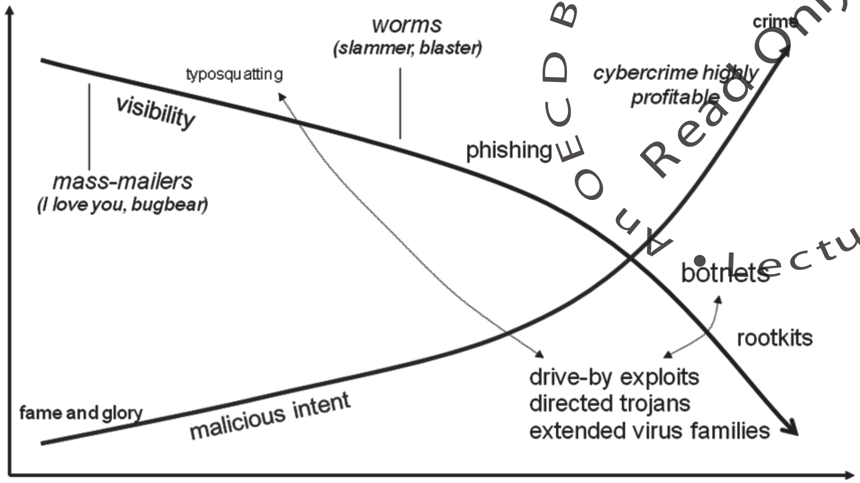
While a certain amount of crime is always “local”, the vast majority of online crime crosses jurisdictional boundaries and international borders thus reducing the criminals’ risk of identification and prosecution. Because many malware attacks are not able to be traced back to the people that conduct them, it is difficult to provide authoritative insight into the nature of groups or individuals involved in the proliferation of the various types of crime. However, some law enforcement and financial institutions are actively involved in monitoring and investigating the money trails arising from fraudulent fund transfers as a result of phishing and ID theft Trojan related attacks. These investigations involve identification of money mules, who are individuals recruited wittingly and often unwittingly by criminals, to facilitate illegal funds transfers from bank accounts.

Figure 2.4 illustrates the evolution of malware in terms of malicious intent of the actors showing a clear evolution from fame seeking “techies” to criminals motivated by financial gain.

What are their capabilities and motivations?

As demonstrated earlier in this report, attacks using malware are becoming increasingly complex. But while the sophistication of the attacks vectors increase, the knowledge required to carry them out significantly decreases. Although this might seem counterintuitive, it can largely be attributed to the increased market for malware. The majority of today’s attackers are motivated adversaries who are capable of purchasing malware or outsourcing attacks to more sophisticated attackers.

Figure 2.4 Visibility of malware vs. malicious intent



Source: Govcert.nl, *www.govcert.nl.*

The malware business model

One expert recently noted that "creating one's own bot and setting up a botnet is now relatively easy. You don't need specialist knowledge, but can simply download the available tools or even source code" (McAfee Inc., 2006). In addition, "off-the-shelf" kits with ready-made Trojans can be downloaded from the Internet. Some versions are guaranteed by the authors to remain undetected by security defences and some even include a "service level agreement" by which the author guarantees, for a certain period of time, to create new versions for the criminal once the original malware is detected. It has been estimated that this service can cost as little as USD 800 (MessageLabs, 2006). In addition, many malicious services, such as botnets, are available for hire.

Malware, and by extension its main propagation vector, spam[30], are increasingly combined as key underpinnings of criminal techniques to make profit in the rapidly evolving "Internet economy". Malware has evolved into "mass market" money-making schemes because it offers such a profitable business model. Malware techniques are becoming increasingly sophisticated, but some users continue to lack appropriate protection. Understanding the malware business model can help industry participants and policy makers alike to more effectively combat malware threats by undermining their economic profitability. The spread of malware is driven by the very real prospect of economic gain although the information targeted by attackers can be sought for a variety of purposes (for pure identity theft or corporate espionage, or to gain access to privileged or proprietary information or to deny access to critical information systems).

As attackers continue to remain successful at launching attacks, the malware economy becomes self-perpetuating. Spammers, phishers, and other cyber criminals are becoming wealthier, and therefore have more financial power to create larger engines of destruction. It is a big business, often led by wealthy individuals, with multiple employees and large bankrolls of illicit cash. In addition to an increased frequency and sophistication of attacks, the amount of damage is significant.[31]

Modern attacks demonstrate an increasing level of convergence, with a combination of spam and social engineering designed to yield the greatest level of profitability to the attacker. In addition, today's attacks often consist of a series of waves each having a specific purpose. A simple attack will aim at building up a list of valid e-mail addresses. It will be followed by e-mail to the harvested accounts containing viruses with a payload that makes a user's system part of a botnet. Once part of a botnet, the machines are often used to disseminate phishing emails which in turn produce the attack's monetary return.

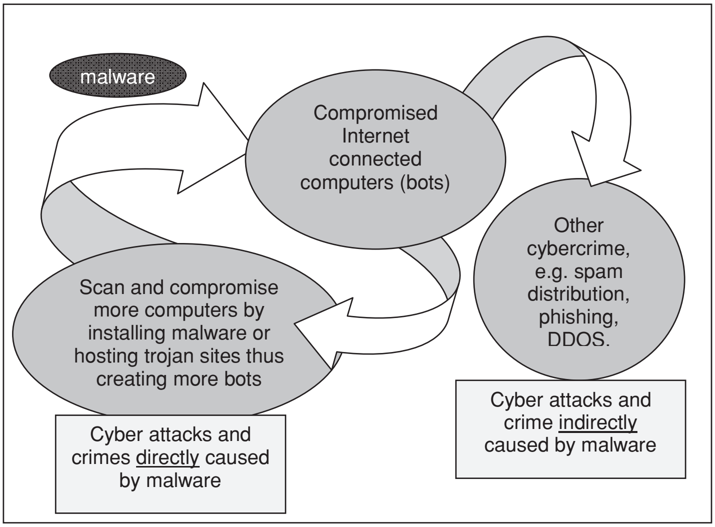
Basic economic rationale for malware

E-mail is not at an economic equilibrium between the sender and the recipient because it costs virtually nothing to send. All the costs of dealing with spam and malware are passed on to the Internet provider and the "unwilling" recipients, who are charged for protective measures, bandwidth and other connection costs, on top of the costs of repairing the computer or having lost money to scams. At the same time, criminals minimise their costs to the extreme: they pay no tax, escape the cost of running a genuine business, and pay commission only to others in criminal circles worldwide and at a comparatively low price.

The cost to malicious actors continues to decrease as freely available email storage space increases. Further, the use of botnets makes it easier and even cheaper to send malware through email. Today's criminals often have access to cheap techniques for harvesting email addresses as well as easy access to malware and outsourced spamming services. Anti-detection techniques are constantly evolving to make it cheaper to operate, and malicious actors can easily switch ISPs if their activity is detected and their service terminated.

Both the malware itself and the compromised computers being used to further launch malware attacks are a low cost, readily available and easily renewable resource. High speed Internet connections and increased bandwidth allow for the mass creation of compromised information systems that comprise a self sustaining attack system as illustrated by Figure 2.5. Furthermore, malicious actors can replace compromised information systems that have been disconnected or cleaned, and they can expand the number of compromised information systems as the demand for resources (namely malware and compromised information systems) for committing cybercrime also grows.

Figure 2.5 Self sustaining attack system using malware


malware
Compromised Internet connected computers (bots)
Other cybercrime, e.g. spam distribution, phishing, DDOS.
Scan and compromise more computers by installing malware or hosting trojan sites thus creating more bots
Cyber attacks and crimes directly caused by malware
Cyber attacks and crime indirectly caused by malware

Note: this figure shows how malware is used to create a self sustaining resource of compromised computers that serve as the backbone of malicious online activity and cybercrime. Information systems connected to the Internet can become infected with malware. Those information systems are then used to scan and compromise other information systems.

Underlying business process

The underlying business processes for spam and malware largely follow the same pattern:

- Developing or acquiring spamming software that can distribute malware.

- Gathering of addresses, targeted or not, and/or developing or acquiring control of a botnet.
- Delivering spam, with or without malware, from other people's computers through botnets.
- Publishing fraudulent websites to capture users' data.

In this pattern, certain groups of attackers are active in the entire value chain, starting with the development of the malware and performing the delivery of the spam and/or malware, all the way to laundering the money into a "clean" bank account. Much of the criminal market, however, is segmented into clusters of expertise with the opportunity to source partners globally, primarily through Internet Relay Chat (IRC) channels, underground bulletin boards, and online forums.

Criminals develop, maintain and sell malware, botnets, spam transmission software, CDs full of addresses harvested from web pages, lists of open proxy servers and lists of open simple mail transfer protocol (SMTP)[32] relays. The lists of addresses or controls of a botnet are then rented out or sold. These lists are often inexpensive at around USD 100 for 10 million addresses. An entire online criminal operation could be carried out at little or no cost, the only hard costs are various "utilities" such as bandwidth, Internet connection, e-mail addresses, or web hosting, and even those can be financed illegally.

While the use of malware to facilitate cybercrime, particularly crimes motivated by illicit financial gain, has increased, the money made through malicious online activity has become increasingly difficult to trace. As in traditional criminal investigations, tracing where the money goes by analysing the cash flows could provide essential information on the attackers. However the victims of online malicious activity are increasingly asked to pay by wire transfers (46% of online scams transactions in the US in 2006), followed by card payment (28%), both much preferred for their speed and the potential to mask tracks easily, by comparison with cheques or cash, which now represent less than 10% of the payments.[33] These types of payments are fast and can be made almost anonymously through the use of multiple financial accounts across borders. Alternative payments systems such as 'e-Gold' or PayPal used by criminals further down the chain make it even more difficult to trace financial movements. Users of these online payment services can open an account using a fraudulent name and deploy a proxy server to shield the originating IP address.

Notes

1. See “Indirect attacks on the DNS” below for further information on types of attacks.

2. It is also possible to cause a denial of service in a network device or application by exploiting vulnerabilities in an operating system or application software. For example, this could be accomplished by an attacker sending specially crafted packets to the device or application where the vulnerability exists. DOS attacks of this type can be rectified, however, by applying the software or firmware patch, or implementing some other work-around. In the case of flood attacks, the ability to mitigate is more difficult and protracted and hence the impact is potentially more serious.

3. See Chapter 1, “The Malware Internet: Botnets” section, for a comprehensive discussion of bots and botnets.

4. An Internet exchange point (IX or IXP) is a physical infrastructure that allows different Internet Service Providers (ISPs) to exchange Internet traffic between their networks by means of mutual peering agreements, which allow traffic to be exchanged without cost. IXPs reduce the portion of an ISP's traffic which must be delivered via their upstream transit providers, thereby reducing the Average Per-Bit Delivery cost of their service. Furthermore, IXPs improve routing efficiency and fault-tolerance.

5. For example, a senior official was quoted by *The Economist* saying “If a member State's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?”; see *The Economist* (2007), “A cyber riot”, 10 May..

6. The Add Grace Period (AGP) refers to a specified number of calendar days following a Registry operation in which a domain action may be reversed and a credit may be issued to a registrar. AGP is typically the five day period following the initial registration of a domain name.

7. The Internet Protocol (IP) allows large, geographically diverse and heterogeneous networks of computers to communicate with each other quickly and economically over a variety of physical links. An IP address is the numerical address by which a host or device on the Internet is identified. Computers on the Internet use IP addresses to route traffic and establish connections among themselves.

8. This is a theoretical proposition only. The authors are not aware that such cyber attacks have occurred involving the use of malware.

9. "IFrame" is the hybrid of *inline frame,* and describes an HTML element which makes it possible to embed another HTML document inside the main document. IFrames are commonly used to insert content (for instance an advertisement) from another website into the current page.

10. The Netcraft toolbar Community is a digital neighbourhood watch scheme in which expert members act to defend all Internet users against phishing frauds. Once the first recipients of a phishing e-mail have reported the target URL, it is blocked for toolbar users who subsequently access that same URL.

11. These packages, known broadly as Rockphish or R11, each included dozens of sites aimed at spoofing major banks.

12. This includes all types of ID Theft, online and offline.

13. E-Gold is a 'digital currency', but which is backed by real gold and silver stored in banks in Europe and the Middle-East. E-Gold can be used as a trusted third party intermediary whereby the money is transferred only once the product or service bought has been received.

14. Most (if not all) Trojan variants being used for illicit financial gain have the ability to capture data transmitted during an SSL session – not just those which also include HTML injection functionality.

15. A certificate authority is an entity, such as Verisign, that issues certificates.

16. A digital certificate is a means of authenticating an identity for an entity when doing business or other transactions on the web or on line. Digital certificates exist as part of public key infrastructures (PKI). PKI uses public key cryptography and an associated hierarchical infrastructure of root Certification Authorities (CAs) and Registry Authorities to process requests for, issue and revoke certificates. Even when a digital certificate is valid, all valid certificates should not be trusted equally. Some certificates are self-signed and hence have no independent third party to verify that they are a legitimate business entity or own a particular domain and others, which may be issued by a CA, have only low assurance levels, *i.e.* the CA has provided only very basic checking to verify that the entity is who it is claiming to be. A certificate contains the entity's name, a serial number, certificate expiration dates, a copy of the certificate holder's public key (used for encrypting messages and verifying digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is authentic and was issued by the CA.

17. SSL is a cryptographic protocol used to provide secure communications on the Internet, for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

18. More recent versions of the Haxdoor Trojan also have the ability to use HTML injection. See AusCERT (2006).

19. It has been assessed that such attacks are not likely to gain popularity as any organisation with a basic level of preparedness should have back-up copies of their data available. However, it may also be that individuals are not aware of this risk, or simply lack basic security education to protect themselves from malware.

20. See OECD (2008b), where Identity Theft is defined as the unlawful transfer, possession, or misuse of personal information with the intent to commit, or in connection with, a fraud or other crime.

21. Identity theft attacks most often use social engineering techniques to convince the user to necessarily disclose information to what they assume is a trusted source. This technique, known as Phishing, does not *directly* rely on the use of malware to work. It uses deceptive or "spoofed" e-mails and fraudulent websites impersonating brand names of banks, e-retailers and credit card companies to deceive Internet users into revealing personal information. However, as many phishing attacks are launched from spam emails sent from botnets, malware is *indirectly* involved as it is used to create botnets which are in turn used to send the spam e–mail used in phishing attacks. Malware would be *directly* implicated when the spam e–mails contained embedded malware or a link to a website where malware would be automatically downloaded.

22. This is a technique known as "fast flux".

23. A DNS table provides a record of domain names and matching IP addresses.

24. See previous sections of Chapter 2 for a discussion on attacks using the DNS and attacks against the DNS.

25. When spoofing is used, identifying the source IP address of an e–mail or website is usually a futile effort. It is also possible to spoof the source IP address of an IPv4 datagram, thereby making real identification of the source IP address much more difficult. It should be noted that this is often not required for an attack to succeed or can be counter-productive for the attacker if the objective is to steal data from a computer. The use of anonymising technologies could pose a more serious problem for identifying attack sources but is not in widespread use by criminals – probably because using other people's compromised computers provides sufficient protection for the attacker.

26. Here we refer to cybercriminals who are conducting attacks full-time for illicit financial gain and may have an area of specialisation or be involved in a variety of business lines such as phishing, Trojans, spam distribution, clickfraud, malware development, etc.

27. In computer networks, a proxy server is a server (a computer system or an application programme) which services the requests of its clients by forwarding requests to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the client. A proxy server that removes identifying information from the client's requests for the purpose of anonymity is called an anonymising proxy server or anonymiser.

28. For example, see Symantec (2007) p. 9.

29 "Organised crime" is used loosely in this context and often refers to a group of profit-motivated criminals who trade services with one another in an open marketplace.

30. As discussed previously in this paper, not all spam contains malware however the majority of spam is sent from information systems that have been compromised by malware.

31. See Chapter 3, "Malware: Why Should We Be Concerned?" for a discussion of the impacts from malware.

32. Simple Mail Transfer Protocol (SMTP) is the de facto standard for e-mail transmissions across the Internet.

33. United States National Consumer League / National Fraud Information Center (2006), p. 2.

Chapter 3. Malware: Why Should We Be Concerned?

The growth of malware, and the increasingly inventive ways in which it is being used to steal personal data, conduct espionage, harm government and business operations, or deny user access to information and services, is a potentially serious threat to the Internet economy, to the ability to further e-government for citizen services, to individual's online social activities, and to national security.

Malware-enabling factors

The capabilities of malware make it a prevalent "cybercriminal tool". However, broader economic and social factors may contribute to its increased occurrences and the robust state of the malware economy. The following describes some of those factors which, while they bring important benefits to society, also facilitate the existence and promulgation of malware.

Broadband Internet and its users

In 2005, the International Telecommunication Union estimated 216 708 600 "fixed" broadband Internet subscribers in the world (ITU, 2007). Furthermore, it is generally agreed that there are an average of 1billion Internet users in the world today. As the number of subscribers and users increases, so does the number of available targets for malware. The increased prevalence of high speed Internet and the availability of broadband wireless connections make it easy for malicious actors to successfully carry out attacks as they can compromise computers at faster rates, use the bandwidth to send massive amounts of spam and conduct DDoS attacks. Furthermore, these "always on" connections allow malicious actors to be mobile and to attack from any location including public places such as Internet cafes, libraries, coffee shops or even from a PDA or mobile phone device (McAfee Inc., 2007). Operating from public places allows attackers to conduct their activities anonymously thus making it difficult to detect and trace their activities.

It is important to note that while broadband technologies are an enabling factor, it is the behaviours associated with these technologies that are problematic. For example, people often fail to adopt appropriate security measures when using broadband technologies and therefore leave their connection open without the appropriate security software installed.[1]

Ever more services available online

Most governments, consumers and businesses depend on the Internet to conduct their daily business. In 2004, the OECD found that, in most OECD countries, over 90% of businesses with 250 or more employees had access to the Internet. Firms with 50 to 249 employees also had very high rates of access (OECD, 2005). Home users rely on the Internet for their day to day activities including shopping, banking or simply exchanging information and conducting e-government and e-commerce transactions. As the amount of these services continues to increase, so does the likely community of users accessing these services on line. This in turn increases the available targets for attack or exploitation which provides further incentive for criminals to conduct malicious activity.

Operating system and software vulnerabilities

The more vulnerable the technology, the more likely it is to be exploitable through malware. For example, the security firm Symantec reported a 12% increase in the number of known vulnerabilities from the first half of 2006 (January-June 2006) to the second half (June-December 2006) which they largely attribute to the continued growth of vulnerabilities in web applications (Symantec, 2007). Microsoft also reported an increase of nearly 2 000 disclosed vulnerabilities from 2005 to 2006. The increase in vulnerabilities corresponds to an increase in incidents. Microsoft reported an increase in the number of machines disinfected by its Malicious Software Removal Tool from less than 4 million at the beginning of 2005 to more than 10 million at the end of 2006 (Microsoft, 2006b).

It is important to note that the absence of known *reported* vulnerabilities in a software product does not necessarily make that product more secure than one that has known reported vulnerabilities – it may simply be that similar effort has not been expended to find them. In addition, tools that find and exploit vulnerabilities are improving; companies are doing more reporting of vulnerabilities and more people or “researchers” than ever are probing software to find vulnerabilities. Finally, the greater complexity of software – more interconnecting functions that need to work with an ever growing universe of other software - further increases the potential for vulnerabilities.

Easy to target average Internet user

As the reliance of home users and small to medium-sized enterprises (SMEs) on the Internet increases, so do the malware threats they face. Consumers and business are increasingly exposed to a new range of complex, targeted attacks that use malware to steal their personal and financial information.

Many Internet users are not adequately informed about how they can securely manage their information systems. This lack of awareness and subsequent action or inaction contributes to the increasing prevalence of malware. Most malware requires some form of user action or acceptance to propagate. Recent surveys from various organisations show that while more users are taking measures to protect their information systems, a large percentage of the population lacks basic protective measures. For example, a 2005 report commissioned by the Australian Government, *Trust and Growth in the Online Environment,* found that only one in seven computers in Australia uses a firewall and about one in three uses up-to-date virus protection software (OECD, 2007b). After hearing descriptions of “spyware” and “adware,” 43% of Internet users, or about 59 million American adults, said they had had one of these programs on their home computer (Brendler, 2007).

The European Commission's Eurobarometer E-communications Household survey, observed an increase in consumer concerns about spam and viruses in 2006 (European Commission, 2007). For some EU Member States, up to 45% of consumers had experienced significant problems. In 40% of the cases, the computer performance decreased significantly, in 27% of the cases a breakdown was observed. In the same survey, 19% of consumers had no protection system at all on their computers. Other data also suggests that home users are the most targeted of all the sectors accounting for 93% of all targeted attacks[2] and thus highlighting that weak user security is one important enabler of malware (Symantec, 2007).

The costs of malware

In many cases, the consequences of inadequate security measures are “external” or borne by others in society. For example, if one user’s computer connected to a network or the Internet is inadequately protected and becomes infected, it has the potential to directly impact the security of other interconnected information systems. One example of this is the use of botnets to launch DDOS attacks against third parties’ websites, mail servers or other network bandwidth or resources.

While many attack trends are increasing, it is nevertheless unclear how these trends relate to the overall damage caused by malware. Detecting a higher number of Trojan variants does not necessarily mean that there is more damage. It could also be a response to improved security defenses. Similarly, signalling that large-scale botnets are shrinking in size does not necessarily mean that the counter measures are effective. It might be that attackers have found smaller and more focused botnets to be more profitable. In short: because malicious attack trends are highly dynamic, it is difficult to draw reliable conclusions from them regarding economic damage.

However, considering the growing proportion of compromised information systems connected to the Internet in any single country and the increasing challenges to detect and remove malware, the impacts of malware on society are, in all probability, rising as a result.

Financial impacts – sample data

Although precise data on online criminal activity and the associated financial losses are difficult to collect, it is generally accepted that malware contributes significantly to these losses.[3] Further, where data on cybercrime and its economic impact are available, businesses and governments are often reluctant to share it publicly.

One association of banks in the United Kingdom estimated the direct losses caused by malware to its member organisations at GBP 12.2 M in 2004, GBP 23.2 M in 2005, and GBP 33.5 M in 2006, an increase of 90% from 2004 and 44% from 2005 (Whittaker, 2007). It is important to note that these direct losses are not fully representative of the actual financial impact as they do not measure diminished customer trust in online transactions, loss in reputation, impact on the brand, and other indirect and opportunity costs that are challenging to quantify. Likewise, they do not include costs, such as labour expenses for analysing malware, repairing, and cleansing infected machines, costs associated with the procurement of security tools (such as anti-virus and anti-malware software), or loss of productivity caused by the inability of employees to interact with a system when affected by an attack.

One recent survey of 52 information technology professionals and managers estimated a slight decline in the direct damages associated with malware, from EUR 12.2 billion in 2004, to EUR 10 billion in 2005, to EUR 9.3 billion in 2006 (Computer Economics, 2007, p.5).[4] This decrease is largely attributed to the suspicion that indirect or secondary losses are actually increasing.[5] Furthermore, the same survey found that most organisations tracked the frequency of malware incidents but not the financial impacts (Computer Economics, 2007, p. 9). Another survey estimated the annual loss to United States businesses at USD 67.2 billion (US Government Accountability Office, 2007).

Although the malware-related costs of security measures are considered proprietary, estimates provided by market participants in the empirical study presented in Part II of this book ranged from 6-10% of the capital cost of operations (Van Eeten, 2008). No clear estimates of the effects of malware on operating expenses were available, although the study found that most organisations did experience such effects (see Part II, "Survey Results on the Costs of Malware"). There was evidence throughout the empirical research of concern that such effects are important, although no specific indication as to their magnitude is available.

The cost to individual consumers may be even more difficult to measure; however, it is likely significant. One example is the United States where consumers paid as much USD 7.8 billion over two years to repair or replace information systems infected with viruses and spyware (Brendler, 2007).

While most of the data are not comparable across studies, and the surveys are often limited in scope, they do illustrate the magnitude of the financial impact, for both businesses and consumers, resulting from malware. Also, the collective public costs of fighting malware – ranging from the costs of maintaining public-private monitoring organisations, to the cost of public education campaigns and law enforcement – add to these private costs. Finally, there are the potentially high indirect costs of malware in the form of slower migration to efficiency enhancing forms of electronic transactions. The research study presented in Part II of this report indicates that the direct and indirect costs of malware could be a double-digit percentage of the revenues of participants in the information and communications market.

The impact on market participants

The following briefly illustrates how some key market participants are affected by malware (Eeten and Bauer, 2008).

Internet Service Providers (ISPs)

Both the costs and revenues of ISPs, and hence their profitability, are affected directly and indirectly by malware. The most immediate cost of malware is customer support and abuse management. These costs may rise further when the ISPs are impacted by blacklists trying to fight infected machines on their network. Forms of malware that increase traffic volume, such as botnets generating massive amounts of spam, if left uncontrolled, cause opportunity costs to the ISP.

The level of these opportunity costs depends on the capacity utilisation of the existing network. If the network has significant spare capacity, the opportunity costs of additional traffic to the ISP will be low. However, if the network is near capacity utilisation, the opportunity costs may be significant as incremental malware-induced traffic may crowd out other traffic in the short run and require additional investment in network facilities, in particular routers and transmission capacity, in the medium and long run.

Malware may also affect an ISP indirectly via reduced revenues if its brand name or customer reputation suffers, for example, because of blacklisting and reduced connectivity. ISPs will invest in preventative measures reducing malware, such as filters for incoming traffic or technology that enable them to quarantine infected customers, only if the cost is less than the direct and indirect cost inflicted by malware.

Electronic-commerce (E-commerce) companies

E-commerce companies are affected by malware in a variety of ways. Many have to deal with DDoS attacks, often requiring them to buy more costly services from their ISPs so as to protect the availability of their services. Furthermore, malware has been used to capture confidential customer data, such as the credit card information registered with customers' accounts with e-commerce companies. Some sophisticated forms of malware have been able to defeat the security measures of online banking sites that rely on so-called multi-factor authentication – *i.e.* on more than just user login credentials.

Even if customer information does not immediately allow access to financial resources, it can be used to personalise phishing e-mails that try to trick customers into revealing financial information. There are also cases where the malware is located on the servers of e-commerce companies, which are unaware that their website hosts malicious content that is distributed to its visitors. Typically, it is the e-commerce customers themselves that are harmed, though directly or indirectly the e-commerce company may also be affected. Financial service providers often compensate damages for their customers. For other companies there can be reputation effects.

Software vendors

Software vendors are affected in direct and indirect ways. Malware uses vulnerabilities in their products to infect machines. The damage resulting from these vulnerabilities does not impact the software vendors directly, though it may have reputation effects and require costly response measures. Developing, testing and applying vulnerability patches is costly, not only on the part of the vendor, but also for its customers.

Software developers typically face difficult development trade-offs between security, openness of software as a platform, user friendliness, and development costs. Investments in security may delay time to market and hence have additional opportunity cost in the form of lost first-mover advantages. On the other hand, if reputation affects work, software vendors whose products have a reputation of poor security may experience costs in the form of lost revenues. These effects are mitigated, however, by the fact that many software markets tend to have dominant firms and thus lock-in customers to specific products.

Domain name registrars

Registrars have become part of the security ecosystem. Their business practices and policies affect the costs of malware and of the criminal business models built around it. Registrars may derive additional revenues from domain name registrations, even if they are related to malware, but they do not incur any specific direct costs. Nonetheless, if their domains are associated with malicious activity, it may result in an increasing number of formal and informal abuse notifications. Dealing with such abuse notifications is costly, requiring registrars to commit and train staff. Suspending domains may also result in legal liabilities.

Furthermore, many registrars may be ill-equipped to deal with malware deregistration requests. Malware domain de-registrations can be very complex to process compared to, for example, phishing domain de-registrations, which are normally a clear breach of trademark or copyright. Some experts report that registrar abuse handling teams will often cite insufficient evidence to process a de-registration request, although evidence sufficient for many incident response teams has been provided. Because of the risk of legal action where a legitimate domain would be incorrectly de-registered, registrars often prefer to support their customer rather than the complainant.

One of the economic costs that registrars face is proving the identity of registrants. Certain domain spaces (.com.au, for example), require strict tests of company registration and eligibility for a name before it can be granted. Evidence suggests that these constraints have lowered fraudulent domain registrations in the .com.au space.

End users

End users form the most diverse group of players, ranging from home users to large corporations or governmental organisations. End user machines, from home PCs to corporate web servers, are the typical target of malware. The economic impact of these infected computers is distributed across the whole value system. Some of the impact is suffered by other market players, not by the owners of the infected machines, although there is also malware directly impacting the owners, for example by stealing sensitive information from the compromised machine.

Erosion of trust and confidence

Society's heavy reliance on information systems makes the consequences of the failure or compromise of those systems potentially serious. Malware is an effective and efficient means for attackers to compromise large numbers of information systems, which cumulatively has the potential to undermine and erode society's ability to trust the integrity and confidentiality of information traversing these systems. The failure to provide adequate protection for the confidentiality and integrity of online transactions may have implications for governments, businesses and consumers. For example, electronic government (e-government) services, such as online filing for taxes or benefits, are likely to include personal data that if compromised could be used to commit fraud. Information systems in small businesses or large public and private sector organisations might be used to access such e-government or electronic commerce (e-commerce) services.

The nature of malware is such that it is not possible to trust the confidentiality or integrity of data submitted or accessed by any computer host compromised by malware. It is often difficult to readily distinguish a compromised host from one that is not compromised and, as a result, in an environment like the Internet, in which malware has taken hold, connections from infected hosts must be treated as potentially suspect. Therefore, the ability to have trust and confidence in online transactions can be further reduced because traditional mechanisms for building trust and confidence in the information economy such as authentication, encryption and digital certificates can also be subverted, bypassed or manipulated by malware.[6]

In recent years, a number of surveys have been conducted which show that consumers are concerned about security and privacy risks associated with providing information online or conducting transactions online. [7] The key point of these surveys is that if security and privacy concerns were better able to be addressed, then many more consumers would use e-commerce, e-banking and various e-government services than currently is the case, thus enhancing the economic benefits and efficiencies expected from the use of these platforms.

There are other studies, however, which show that the convenience and efficiency of the online channel is driving growth in participation in e-commerce and e-banking despite these concerns. In 2006, RSA Security announced the first Internet Confidence Index designed to measure changes in US and European confidence in secure online transactions among consumers and businesses (RSA Security, 2006). At the time, the annual Index, based on data gathered from business and consumer audiences in the United States, the United Kingdom, Germany and France, revealed that the willingness to transact online was on average outpacing trust and that both businesses and consumers were absorbing the risks in order to reap the benefits of online transactions.

These two seemingly contradictory pieces of evidence point out that the role and impact of trust is not yet adequately understood and that indeed it is difficult to measure consumer trust and confidence in the online environment. However, empirical evidence reveals that e-commerce companies benefit greatly from the ability to conduct business online.[8] Given the estimated efficiency gains in the financial sector, for example, the cost savings associated with the enormous volume of transactions translates into a very powerful incentive to move as much volume of these services as possible online. Repeatedly in the study, e-commerce companies indicated that security investment levels were much higher than justified by the direct losses, often by one or two orders of magnitude (Eeten and Bauer, 2008). Clearly direct losses are not seen as indicative of the overall problem. It would be much more devastating, for example, if online fraud eroded customer trust or slowed down the uptake of online financial services.

Risk to critical information infrastructures

Critical infrastructures at the basis of our society, such as power grids or water plants, are now often dependent upon the functioning of underlying IP-based networks for their instrumentation and control. Most industrial control systems that both monitor and control critical processes were not designed with security in mind, let alone for a globally networked environment, but are now increasingly being connected, directly or indirectly (through corporate networks), to the Internet and therefore face a new set of threats. As these systems become based on more open standards - using Ethernet, TCP/IP and web technologies - they become vulnerable to the same security threats that exist for other information systems. Thus, the disruption of critical information infrastructure systems through malware has the potential to impact the public and private sectors and society as a whole.

There have been a few cases where attacks using malware have directly or indirectly affected critical information infrastructure. For example, in Russia, malicious hackers used a Trojan to take control of a gas pipeline run by Gazprom (Denning, 2000). In January 2003 the "Slammer" worm, which caused major problems for IT systems around the world, penetrated the safety monitoring system at a US nuclear plant for nearly five hours (Poulsen, 2003). The US Nuclear Regulatory Commission investigated the incident and found that a contractor established an unprotected computer connection to its corporate network, through which the worm successfully infected the plant's network (US Nuclear Regulatory Commission, 2003). More recently, the United States indicted James Brewer for operating a botnet of over 10,000 computers across the world, including computers located at Cook County Bureau of Health Services (CCBHS). The malware caused the infected computers to, among other things, repeatedly freeze or reboot without notice, thereby causing significant delays in the provision of medical services and access to data by CCBHS staff.[9]

Although governments are often reluctant to disclose instances of attack against the critical infrastructure, it is apparent that protecting the information systems that support the critical infrastructure has become exceedingly important.[10] Despite only a few reported cases, it is widely understood that critical information systems are vulnerable to attack. For example, although the 2003 blackout in the northeast US and Canada was attributed to a software failure, analysis of the incident demonstrated that the systems were vulnerable to electronic attack, including through the use of malware.[11]

Challenges to fighting malware

Protecting against, detecting and responding to malware has become increasingly complex as malware and the underlying criminal activity which it supports are rapidly evolving and taking advantage of the global nature of the Internet. Many organisations and individuals do not have the resources, skills or expertise to prevent and/or respond effectively to malware attacks and the associated secondary crimes which flow from those attacks such as identity theft, fraud and DDoS. In addition, the scope of one organisation's control to combat the problem of malware is limited.

Many security companies report an inability to keep up with the overwhelming amounts of malware despite committing significant resources to analysis. One vendor dedicates 50 engineers to analysing new malware samples and finding ways to block them, but notes that this is almost an impossible task, with about 200 new samples per day and growing (Greene, 2007). Another company reported it receives an average of 15 000 files – and as many as 70 000 – per day from their product users as well as CSIRTs and others in the security community (OECD, 2007b). When samples and files are received, security companies undertake a process to determine if the file is indeed malicious. This is done by gathering data from other vendors, conducting automated analysis, or by conducting manual analysis when other methods fail to determine the malicious nature of the code. One vendor estimated that each iteration of this cycle takes about 40 minutes and that they release an average of 10 updates per day (OECD, 2007b). Furthermore, there are many security vendors who all have different insights into the malware problem.

Most security technologies such as anti-virus or anti-spyware products are signature-based meaning they can only detect those pieces of malware for which an identifier, known as a "signature" already exists and have been deployed. There is always a time lag between when new malware is released by attackers into the "wild", when it is discovered, when anti-virus vendors develop their signatures, and when those signatures are dated onto users and organisations' information systems. Attackers actively seek to exploit this period of heightened vulnerability. It is widely accepted that signature based solutions such as anti-virus programs are largely insufficient to combat today's complex and prevalent malware. For example, one analysis[12] that explores antivirus detection rates for 17 different anti-virus vendors reveals that, on average, only about 48.16% of malware was detected. Circumstantial evidence such as this indicates that attackers are actively testing new malware creations against popular anti-virus programs to ensure they stay undetected.

In addition, malicious actors exploit the distributed and global nature of the Internet as well as the complications of law and jurisdiction bound by traditional physical boundaries to diminish the risks of being identified and prosecuted. For example, a large portion of data trapped by attackers using keyloggers is transmitted internationally to countries where laws against cybercrime are nascent, non-existent or not easily enforceable. Although countries across the globe have recognised the seriousness of cybercrime and many have taken legislative action to help reprimand criminals, not all have legal frameworks that support the prosecution of cyber criminals.[13] The problem however is even more complicated as information may be compromised in one country by a criminal acting from another country through servers located in a third country, all together further complicating the problem.

Law enforcement agencies throughout the world have made efforts to prosecute cyber criminals. For example, the Computer Crime and Intellectual Property Section of the US Department of Justice has reported the prosecution of 118 computer crime cases from 1998 – 2006.[14] Although global statistics on arrests are hard to determine, one company estimated worldwide arrests at 100 in 2004, several hundred in 2005 and then 100 again in 2006 (Greene, 2007). While these cases did not necessarily involve malware, they help illustrate the activities of the law enforcement community. It is important to note that the individuals prosecuted are usually responsible for multiple attacks. These figures are low considering the prevalence of online incidents and crime. They highlight the complex challenges faced by law enforcement in investigating cybercrime.

Furthermore, the volatile nature of electronic evidence and the frequent lack of logged information can often mean that evidence is destroyed by the time law enforcement officers can get the necessary warrants to recover equipment. The bureaucracy of law enforcement provides good checks and balances, but is often too slow to cope with the speed of electronic crime. Additionally, incident responders often do not understand the needs of law enforcement and accidently destroy electronic evidence.

Today, the benefits of malware seem to be greater for attackers than the risks of undertaking the criminal activity. Cyberspace offers criminals a large number of potential targets and ways to derive income from online victims. It also provides an abundant supply of computing resources that can be harnessed to facilitate this criminal activity. Both the malware and compromised information systems being used to launch the attacks have a low cost, are readily available and frequently updated. High speed Internet connections and increased bandwidth allow for the mass compromise of information systems that renew and expand the self sustaining attack system. By contrast, communities engaged in fighting malware face numerous challenges that they cannot always address effectively.

Notes

1. This could be the case for any Internet connection, broadband or otherwise.
2. For the purposes of this measurement, Symantec defines "targeted attack" as an IP address that attacks at least three Symantec sensors in a given sector while excluding the other sectors during that reporting period. See Symantec (2007), p. 85.
3. A 2004 report from the U.S. Joint Council on Information Age Crime showed that 36% or less of organisations polled reported computer-related crimes to law enforcement. See US Joint Council on Information Age Crime (2004), p. 8.
4. In this case, direct damages refer to labour costs to analyse, 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 damages do not include preventive costs of antivirus hardware or software, ongoing personnel costs for IT security staff, secondary costs of subsequent attacks enabled by the original malware attack, insurance costs, damage to the organisation's brand, or loss of market value. [Note: Issues include limited sample sizes, limited responses, inability to accurately estimate the costs of a malware incident, the difficulty in detecting malware incidents, and so on. In all cases, references should be to estimated losses.]
5. Such losses were not measured in the survey.
6. See Chapter 2 for a more detailed discussion of how malware may subvert these security technologies and counter-measures.
7. Australian Government, Office of the Privacy Commissioner (2004); Consumer Reports WebWatch (2005), Gartner (2005); RSA Security (2006); TriCipher (2007).
8. For example, two interviewees from the financial sector estimated that online transactions were in the order of 100 times cheaper than processing those transactions off line, through their branch offices, mail or phone. See Eeten, M. J. van and J. M. Bauer (2008), p.43;

9. "US v. James Brewer", United States District Court Northern District of Illinois Eastern Division (2007).

10. A recent OECD report, *The Development of Policies to Protect the Critical Information Infrastructure*, highlights this point. See OECD (2008c).

11. U.S.-Canada Power System Outage Task Force (2003) p. 131.

12. Information provided to the OECD by CERT.br, the national CSIRT for Brazil.

13. One website provides a survey of cybercrime legislation that documented 77 countries with some existing cybercrime law. See *http://www.cybercrimelaw.net/index.html*.

14. United States Department of Justice Computer Crime & Intellectual Property Section (2007).

Part II. The Economics of Malware

Michel J.G. van Eeten[1] and Johannes M. Bauer[2] with contributions from Mark de Bruijne, Tithi Chattopadhyay, Wolter Lemstra, John Groenewegen, and Yuehua Wu

While malware is a product of criminal behaviour, its ultimate magnitude and impact are influenced by the decisions and behaviour of legitimate market participants, such as: Internet Service Providers (ISPs), software vendors, e-commerce companies, hardware manufacturers, domain name registrars and, last but not least, end users. Part II of this book presents qualitative empirical research into the incentives that drive the security decisions of Internet market participants. The results of this research indicate a number of market-based incentive mechanisms that contribute to enhanced security. But there are also instances in which decentralised actions may lead to sub-optimal outcomes - i.e. *where the consequences of inadequate security measures are "externalised", or borne by others in the market or society at large.*

Part II of this book is an edited version of an original OECD working paper also titled "The Economics of Malware", the content of which is available at: http://dx.doi.org/10.1787/241440230621.

[1] Faculty of Technology, Policy and Management, Delft University of Technology - *m.j.g.vaneeten@tudelft.nl*.

[2] Quello Center for Telecommunication Management & Law, Michigan State University - *bauerj@msu.edu*.

Chapter 4. Cybersecurity and Economic Incentives

The past five years have witnessed the emergence of comprehensive efforts to improve the security of information systems and networks. A recent survey by the OECD (2005a) demonstrates that governments have developed national policy frameworks, as well as partnerships with the private sector and civil society, to combat cybercrime. Measures include Computer Security Incident Response Teams (CSIRTs), raising awareness, information sharing and education.

But improving cybersecurity is not a straightforward problem. Notwithstanding rapidly growing investments in security measures, it has become clear that cybersecurity is a technological arms race that, for the immediate future, no one can win. Take spam, for instance. Several years ago, so-called open e-mail relays were a major source of spam. ISPs and other actors developed measures, such as blacklisting, to collectively combat open relays. By the time adoption of these measures reached a critical mass, spammers had already shifted their tactics. As a result, the significant reduction in the number of open relays had hardly any impact on the amount of spam. The list of such examples goes on and on.

While many would agree that cybersecurity needs to be strengthened, the effectiveness of many security measures is uncertain and contested. Furthermore, security measures may also impede innovation and productivity. Those involved in improving cybersecurity sometimes tend to overlook that the reason why the Internet is so susceptible to security threats – namely its openness – is also the reason why it has enabled an extraordinary wave of innovation and productivity growth.

In the Internet world, the benefits of productivity growth often outweigh the costs of innovation – as in the case of online credit card transactions. From the start of moving their business online, credit card companies have struggled with rising fraud. However, this has not stopped them from expanding their online activities. The benefits of that growth have been consistently higher than the associated costs of the increase in fraud. While growing in absolute terms, the level of online fraud in the United States has been dropping relative to the overall dollar amount of online transactions

(Berner and Carter, 2005). Rather than implementing far-reaching security measures that would restrict the ease of use of their systems, credit card companies have adopted strategies to fight instances of fraud, up to the point where the costs of further reductions in fraud start to exceed the benefits: damages avoided.

All this means that total security is neither achievable nor desirable. In principle, actors need to make their own tradeoffs regarding what kind of security measures they deem appropriate and rational, given their business model. Clearly, business models vary widely for actors in the different niches of the complex ecosystem surrounding information systems and networks – from ISPs at different tiers to software providers of varying applications, to online merchants to public service organisations and to end users. All of these actors experience malware differently, as well as the costs and benefits associated with alternative courses of action. In other words, many instances of what could be conceived as security failures are in fact the outcome of rational economic decisions, reflecting the costs and benefits perceived by the actors during their decision-making timeframe.

What is needed, then, is a better understanding of these costs and benefits from the perspective of individual actors and of society at large. Part II of this report sets out to identify the incentives under which a variety of Internet market participants operate, and to determine whether these incentives adequately reflect the costs and benefits of security for society – *i.e.* whether these incentives generate externalities. To address these issues, the findings are presented of a recent research project on incentives that should help lay the groundwork for future policymaking.

Increased focus on incentive structures

Research in the field of cybersecurity is undergoing a major paradigm shift. More and more researchers are adopting economic approaches to study cybersecurity, shifting emphasis away from technological causes and solutions. Most of this innovative research has yet to find its way into the realm of policy makers, let alone into the policies themselves. While reports like the OECD survey on the culture of security (OECD, 2005a) generally recognise that cybersecurity is more than a technological issue, the proposed measures are still mostly oriented in that direction: developing technological responses and efforts to stimulate their adoption. The technological responses are typically accompanied by legal efforts and intensified law enforcement.

Box 4.1 OECD Guidelines and the Economics of Cybersecurity

In 2002, the OECD released the *Guidelines for the Security of Information Systems and Networks* (OECD, 2002a). A set of nine non-binding guidelines aim to promote "a culture of security" – that is, "a focus on security in the development of information systems and networks, and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks" – among "all participants in the new information society" (see below). The guidelines reflect the shared understanding of OECD member countries as well as a variety of business and consumer organisations.

OECD Guidelines for the Security of Information Systems and Networks

1. Awareness
   Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. Responsibility
   All participants are responsible for the security of information systems and networks.
3. Response
   Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. Ethics
   Participants should respect the legitimate interests of others.
5. Democracy
   The security of information systems and networks should be compatible with essential values of a democratic society.
6. Risk assessment
   Participants should conduct risk assessments.
7. Security design and implementation
   Participants should incorporate security as an essential element of information systems and networks.
8. Security management
   Participants should adopt a comprehensive approach to security management.
9. Reassessment
   Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

The "culture of security" that the guidelines aim to promote will be influenced by the incentive structures surrounding security tradeoffs. The focus on security may certainly be strengthened, but that in itself does not mean that actors will behave in ways that are beneficial to society. In other words, more attention to security does not equal better security decisions as long as economic incentives are ignored.

Box 4.1 OECD Guidelines and the Economics of Cybersecurity (continued)

Chapter 5 provides a more detailed discussion of why this is the case. For now, it suffices to mention a few examples. Take firms' investment in security measures.. Research has demonstrated that a focus on security may mean actively participating in information sharing with other firms. Under certain conditions, this actually leads to decreased investment levels. Also, a firm taking protective measures may create positive externalities for others – that is, benefits for others that are not reflected in the decision by that firm – which may reduce their investments to a level that is below the social optimum.

Another example is the manufacturing of software. According to the *OECD Guidelines* (OECD, 2002b), "Suppliers of services and products should bring to market secure services and products." Even if it was clear what the term "secure software" means, many software markets do not reward such behaviour. Rather, they reward first movers – that is, those companies that are first in bringing a new product to market. This means it is more important to get to the market early, rather than first investing in better security. A final example relates to end-users. The *Guidelines* argue that end users are responsible for their own system. In the case of malware, however, this responsibility may lead to security tradeoffs that are rational for the end users, but have negative effects on others. More and more malware actively seeks to reduce its impact on the infected host, so as not to be detected or removed, using the infected host to attack other systems instead of the host itself.

In short: the development of a "culture of security" is very sensitive to economic incentive structures. Whether such a culture will actually improve overall security performance requires a better understanding of the incentives under which actors operate as well as policies that address those situations in which incentives produce outcomes that are not socially optimal. The research project presented in this Part II of the malware report aims to contribute to this undertaking.

Notwithstanding the necessity of these initiatives, they typically overlook the economic factors affecting cybersecurity – *i.e.* the underlying economic incentive structure. As Anderson and Moore (2006, p. 610) have argued, "over the past 6 years, people have realised that security failure is caused at least as often by bad incentives as by bad design." Many of the problems of information security can be explained more clearly and convincingly using the language of microeconomics: network effects, externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons. Within this literature, designing incentives that stimulate efficient behaviour is critical.

The power that incentive structures can exert on security threats is visible everywhere. Take the distribution of viruses and other malware.

During the second part of the 1990s, when the scale of virus distribution was rapidly increasing and countless end users (home, corporate, governmental) were affected, many ISPs argued that virus protection was the responsibility of the end users themselves. The computer was their property, after all. ISPs further argued that they could not scan the traffic coming through their e-mail servers, because that would invade the privacy of the end user. Mail messages were considered the property of the end users.

About five years ago, this started to change, partly due to the growth of broadband and always-on connections. The distribution of viruses and worms had increased exponentially and now the infrastructure of the ISPs themselves was succumbing to the load, requiring potentially significant investment in network expansion. Facing these potential costs, ISPs radically shifted their position. Within a few years, the majority of them started to scan incoming e-mail traffic, deleting traffic identified as malignant, since this had become a lower-cost solution than infrastructure expansion. *De facto*, ISPs re-interpreted the various property rights associated with e-mail – *e.g.* regarding ownership of the message. Their changed policies have made e-mail based viruses dramatically less effective as an attack strategy.

The economic perspective

An economic perspective on cybersecurity – and malware in particular – presents a potentially fruitful starting point for future policymaking. That's because it leads to a focus on market partcipants' (1) incentive structures and (2) market externalities, or the consequences of inadequate security measures that are borne by other market participants or society in general.

In this chapter and those following, the economic perspective on malware and cybersecurity are examined, building on the innovative research efforts of the past six years (for a brief overview of the existing literature, see Anderson and Moore, 2007; Anderson *et al.,* 2008). It is a first step in this direction, and given the complexity of the problem, more work will undoubtedly be needed.

One promising approach is to complement the existing research with new, qualitative field work. Field research is important because there is limited information in the public domain on how Internet market participants actually make their information-security decisions. And this makes it difficult to calibrate any form of public policy.

Box 4.2 The problem with prevailing research methods

So far, most of the Internet-related economics research has been based on the methods of neo-classical and new-institutional economics. While powerful, these methods are based on rather stringent assumptions about how actors behave – such as their rationality, their security tradeoffs and the kind of information they have – and how they interact with their institutional environment.

Three key limitations of studies founded on these methodological assumptions are:

1. they provide limited insight into how actors actually perceive the cost, benefits and incentives they face;
2. they have difficulty taking into account dynamic and learning effects, such as how a loss of reputation changes the incentives an actor experiences; and
3. they often treat issues of institutional design as rather trivial. That is to say, the literature assumes that its models indicate what market design is optimal, that this design can be brought into existence at will, and that actors will behave according to the model's assumptions.

If the past decade of economic reforms – including privatisation, liberalisation and deregulation – have taught us anything, it is that designing markets is highly complicated and sensitive to the specific context in which the market is to function. It cannot be based on formal theoretical models alone. Institutional design requires an in-depth empirical understanding of current institutional structures and their effects on outcomes. Even with such an understanding, it may not be possible to fully control the setup and working of a market as they are in part emerging from the interaction of multiple actors. However, it should be possible to nudge the system in the desired direction.

Part II presents efforts to: (1) collect evidence on the security tradeoffs faced by Internet market participants; (2) how those participants perceive the incentives under which they operate; (3) which economic decisions these incentives support, and (4) the externalities that arise from these incentive structures. The objective of Part II is to contribute to the debate on the economics of malware from an empirical and analytical perspective. It is not designed to explore and develop detailed policy recommendations.

Chapter 5 reports the findings of the field work. Based on 41 interviews with 57 representatives of Internet market participants, as well as governmental agencies and security experts, we present a variety of incentives faced by Internet Service Providers, e-commerce companies (with a focus on financial service providers), software vendors, domain registrars and end users.

Chapter 6 aggregates the research findings and discusses the externalities that emerge as market participants make incentive-driven security decisions. In some cases, externalities are borne by market participants able to influence the security tradeoffs of those generating the externalities bringing the net market impact closer to the optimum. In other cases, the externalities are simply borne by market participants or by society at large. Part II concludes with a summary of the efficiency and distributional effects of externalities and an overall assessment of the costs of malware.

The annex at the end of Chapter 5 contains a list of the survey participants. Annex B at the end of this report describes the survey in detail.

Chapter 5. Survey of Market Participants: What Drives Their Security Decisions?

Participants in the Internet ecosystem are confronted with malware in different ways; their responses are motivated by the specific incentives under which they operate. To better understand these incentives and their effects, a qualitative field research project was designed. In the course of 2007, the research team conducted 41 interviews with 57 respondents from a broad cross-section of organisations. (For more information on the research design and the interviewees, please see the list at the end of this chapter and Annex B.)

Below, we discuss the findings on the security-related incentives of five major Internet segments: Internet Service Providers (ISPs); e-commerce companies (with a focus on online financial services); software vendors; domain registrars; and end users. Interviews were also conducted with representatives of organisations governing security issues (such as CERTs, regulatory agencies), representatives from security service providers, and other researchers.

Internet service providers

While the term ISP is used to cover a variety of businesses, typically ISPs provide individuals and organisations with access to the Internet. Many ISPs offer related services to their customers, which is why the term sometimes also refers to hosting providers and content providers. For the purposes of this study, we focus our analysis primarily on ISPs that provide Internet access.

The role of ISPs in improving Internet security has been the focus of many recent debates. That’s because it has proven extremely difficult to improve the security of the ISPs’ clients – end users. Reliable estimates are hard to come by, but several of our sources subscribed to estimates available elsewhere that 20-25% of computers worldwide are at risk because their owners are unwilling, or unable, to adequately secure their systems (BBC News 2007; House of Lords 2007a, p. 29; Weber, 2007). Other estimates are considerably lower – *e.g.* Trend Micro published a figure of 7% (Higgins 2007b). Nevertheless, even these lower estimates imply tens of millions of compromised machines. Given the enduring problems around end-user security and its effects on the wider network, it seems inevitable that attention would shift to other players in the ecosystem.

What incentives do ISPs have to reduce the problem of malware? One view is: very few, if any. Recently, the UK House of Lords Science and Technology Committee published a report which states: "At the moment, although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so. Indeed, there is a disincentive, since customers, once disconnected, are likely to call help-lines and take up the time of call-centre staff, imposing additional costs on the ISP." (House of Lords 2007a, p. 30)

ISPs may unwittingly reinforce the impression that they have few, if any, incentives to improve the security of their services. During the inquiry that led to the House of Lords report, ISPs argued that the current approach to self-regulation should not be changed. The resistance of most ISPs to increased government involvement led the committee to conclude that the ISPs were simply maintaining the status quo, rather than reducing the problem. The latter, however, does not follow from the former. The resistance to government involvement does not mean that ISPs are not increasing their efforts to fight malware. In fact, the committee itself also cites evidence from an ISP who in fact disconnects customers whose machines had been infected and then helps them back online. A survey from the EU's European Network and Information Security Agency found that 75% of ISPs report that they quarantine infected machines (ENISA, 2006). This figure does not include any indication of the scale at which ISPs are quarantining infected machines – a point to which we return in a moment. The evidence does, however, clearly question the earlier statement by the committee – and others – that ISPs have no incentives to disconnect infected machines. Either the statement is wrong, or ISPs are assumed to behave irrationally. Our evidence suggests the former.

All ISPs we interviewed described substantial efforts in the fight against malware, even though they are operating in highly competitive markets and there is no governmental regulation requiring them to do so. All of them were taking measures that were unheard of only a few years ago. Most of the interviewees dated this change to around 2003, when it became obvious that it was in the ISPs own interest to deal with end-user insecurity, even though formally it was not their responsibility. Several incentives help explain why the ISPs see these efforts as being in their own interest.

ISP Incentives

Cost of customer support and abuse management

An understanding of these incentives could start with this statement by a security officer of a smaller ISP: “The main [security-related] cost for ISPs is customer calls.” The same view was expressed with minor variations by several other interviewees. A medium-sized ISP told us that an incoming call to their customer centre costs them EUR 8 on average, while an outgoing call – for example, to contact the customer regarding an infected machine – costs them EUR 16. The costs for e-mail were similar. When we mentioned these numbers during subsequent interviews with other ISPs, they confirmed that their costs were in the same range.

The incentive here is that security incidents generate customer calls, thus quickly driving up the costs of customer care. The ISPs may not be formally responsible for the customers’ machines; in reality many customers call their ISP whenever there is a problem with their Internet access. Regardless of the subsequent response of the ISP, these calls increase their costs. An interviewee at a large ISP told us that their customer support desk was a substantial cost for the company, and that the number of calls was driven up by infections of their customers’ machines. He further added that almost all of their outgoing security-related calls had to do with malware.

Of course, many forms of malware do not manifest themselves explicitly to customers. Nevertheless, as security problems rarely come alone, lax security generally tends to increase customers calls. Furthermore, even if customers have not noticed anything wrong, their compromised machines may generate abuse notifications to their ISP from other ISPs who monitor incoming spam or malware from the customer’s IP address. Similar to customer contact, dealing with abuse notifications drives up costs because it requires trained staff. Tolerating more abuse on the network raises the number of notifications that have to be investigated, responded to and acted upon. Acting may mean filtering the customer’s connection or even suspending it altogether, until the problem gets resolved. All the ISPs we interviewed have procedures in place for handling abuse notifications and do in fact filter and suspend connections, though with varying frequency. All of them also mentioned a small number of cases where extreme forms of abuse led to the termination of the contract.

Abuse notifications can come through different channels, most notably through e-mail sent to the abuse desk – typically abuse@provider.com – and through the informal networks of trusted security professionals that exist across ISPs, CSIRTs and related organisations. The latter carry more weight, as they come from known and trusted sources, but all have to be dealt with in some form. Many of these notifications are automated. Several ISPs reported using the so-called AOL Feedback Loop, which sends notifications of any e-mails that are reported as spam by AOL recipients back to the administrator of the originating IP address.

As with customer complaints, not all malware infections will result in abuse notifications. One ISP reported internal research into the degree to which notifications adequately represented the size of the security problems on their networks. They found that only a small percentage of the compromised machines they saw on their network showed up in the notifications. Still, ISPs notifying each other of security problems is an important mechanism. In fact, in some cases, they are critical. In some European countries, ISPs have interpreted the stringent privacy regulations in ways that substantially limit their ability to monitor their own network. In these cases, they rely heavily on notifications coming in from other ISPs, which then allow them to initiate their own investigation. For the ISPs we interviewed, customer contact and abuse notifications are a strong incentive to invest in security both at the network level, as well as at the level of the customer. One medium-sized ISP estimated they were spending 1-2 % of their overall revenue on security-related customer support and abuse management. This also helps to understand why more and more ISPs are offering “free” security software or “free” filtering of e-mail – that is, the costs of these services are included in the subscription rate. One ISP described how about four years ago they started offering virus filters for e-mail as a paid service, but soon thereafter decided to provide them for ‘free’: “After six months, all ISPs [offered these paid security services], so it was no longer a unique selling point. Plus, we could not get more than 10 % of our customers to buy the service... We did not actually do the math, but we figured that by offering it to all our customers within the current rate, we would be better off.... We already paid the AV license. If people have the option to pay for it or not to pay for it, they do not.”

There is another way of responding to these incentives, however: Don’t respond to abuse notifications and avoid customer contact altogether. A class of ISPs is doing exactly this. What is stopping other ISPs, including the ones we interviewed, from doing the same? Here, we came across two interrelated relevant incentives: blacklisting and brand damage.

Costs of blacklisting

Blacklisting is a loosely used term typically referring to the practice of ISPs of using so-called DNS Blacklists (DNSBL) to filter incoming traffic. Mail servers, for example, may be configured to refuse mail coming from IP addresses, IP ranges or whole networks listed on a DNSBL. There is a wide variety of blacklists available and ISPs may use them in different combinations.

According to many interviewees, most ISPs use blacklists nowadays. Most of the lists are free and run by volunteers, though their operations may be funded through external sources. Each DNSBL has its own criteria for including an IP address in the list and its own procedure for getting an address off the list. Spamhaus, an international non-profit organisation funded through sponsors and donations, maintains several famous blacklists – though they prefer the term block lists – which they claim are used to protect over 600 million inboxes. One of their lists contains the addresses of "spam-sources, including spammers, spam gangs, spam operations and spam support services"; another list focuses on botnets, which run as open proxies.

It should be noted at this point that blacklisting, while potentially powerful, has drawn its own criticisms – regarding, among other things, vigilantism of blacklist operators, listing false positives, the collateral damage that may come with blacklisting certain IP addresses or ranges, and the financial motives of some list operators. Furthermore, blacklists have suffered from legal threats; in some cases, spammers on occasion were successful in obtaining court verdicts against being blacklisted (*e.g.* Bangeman, 2006; Heidrich, 2007). Within this report we focus on how blacklisting works as an incentive for ISPs.

Blacklisting provides an incentive to invest in security because it ties in with the incentives mentioned earlier. One interviewee at a medium-sized ISP told us about a security incident where 419 spammers set up over 1,000 e-mail accounts within their domain and then started pumping out spam. That got the ISP's outbound mail servers blacklisted, which resulted in 30 000 calls to their customer centre by customers who noticed their e-mail was no longer being delivered. That number does not include the incoming abuse notifications, of which there were "even more". After this incident, the company changed the procedure through which new customers can set up e-mail accounts; they invested millions in equipment to monitor their network; and they started blocking port 25. "It took us years to get a procedure approved to be able to block port 25. It costs nothing. But the business units did not want us to be able to shut it down, because of their clients. They now understand that it is in the interest of their clients, to avoid blacklisting."

Blacklisting directly impacts the ISP's business model. A security officer at a large ISP explained that being blacklisted led to a much more proactive approach to remove netbots from the network, including the purchase of equipment that automates the process of identifying infected machines on the network. The ISP contacts around 50 customers per day and, if the customer does not resolve the problem, the connection is suspended. When asked how they got the business side of the company to approve this policy, he answered:

"They hated it at first. But at the end of the day, the media fallout by being cut off by AOL and MSN is too big. The big ISPs, they use very aggressive [DNSBL] listings. They take out whole IP ranges. We used to be hit hard and entire ranges of our IP addresses were blacklisted."

There are various levels of blacklisting used to incite a response from an ISP. At the lower end, we find blacklisting of individual IP addresses, *i.e.* an individual customer. This has "exactly zero impact on the ISP," said a security expert. Only when they start to accumulate, might they get the ISP's attention. The expert explained that ISPs mostly ignore listed individual IP addresses, because of the costs of dealing with them – *e.g.* customer support – and because the IP addresses gets taken off of the blacklist as spammers or attackers move on to other infected machines. After a few months, the level of active infected machines on the ISP's network might be equally high, but it is a different set of individual IP addresses that are now blacklisted.

Blacklisting IP ranges and the blacklisting outbound mail servers are a more powerful incentive. These typically do get the ISPs attention and lead to remedial action on their end, although it varies whether or not the ISP remains vigilant. The most extreme form is blacklisting an entire network, *i.e.* all IP addresses of an ISP. This is only used against semi-legitimate ISPs that do not act against spam and known spam-havens.

Costs of brand damage and reputation effects

The "media fallout" mentioned previously by an interviewee indicates a more general concern with brand damage that was mentioned by many interviewees as an incentive to invest in security. With few exceptions, these ISPs want to present themselves as responsible businesses (Arbor Networks, 2007) providing safe services for their customers.

A related incentive is the reputational benefits of offering security services. The increasing attention on Internet security – or rather, to the lack thereof – is creating demand for such services. One interviewee said: "The banks ask us for 'clean pipes.' We do not know what that means exactly, but they ask us anyway. We're looking into what we can do for them." The past years have witnessed the emergence of managed security service providers, either by conventional ISPs taking on security services, by security providers adding Internet access or by new businesses altogether.

It is unclear how strong the incentive is to maintain a reputation for security. For the large and medium-size business market, the ISP's image in terms of security may be a significant factor. For the consumer market, many interviewees argued that customers care about price first and foremost and, thus, Internet access is marketed primarily on price. Furthermore, even if they do care about security, most customers will find it very difficult to assess the security performance of one ISP relative to its competitors. Nevertheless, the more significant finding here is that whether ISPs really care about bad publicity or not, being blacklisted has direct effects on their operating costs, as well as their quality of service. The latter may in fact drive customers away. As one industry insider described it: "A high cost action is to investigate each complaint rigorously. A different kind of high cost action is to do nothing."

Costs of infrastructure expansion

An incentive that was more difficult to gauge, is the effect of malware on the capital expenditures of the ISP – that is, the need to expand infrastructure and equipment as more spam or malware comes through the network. A recent survey found that botnet-based denial of service attacks are growing faster in size than the ISPs are expanding their network – which is worrying the ISPs (Arbor Networks, 2007).

Interestingly, infrastructure expenditures – apart from the costs of security equipment – were hardly identified during interviews as malware-related costs, a point to which we return shortly. As was mentioned earlier, interviewees pointed to customer contact as the highest security-related cost. When asked about infrastructure, a Chief Technology Officer answered: "The network is not affected. We have overcapacity to deal with DDoS. So that is not the problem."

At another ISP, the Chief Information Security Officer told us: "We happen to have overcapacity of the network, so the growth in spam did not require us to expand the capacity." To which one of his colleagues added: "But the number of servers has increased, though." Others have argued that the volume of malware and spam-related traffic pales compared to the traffic from peer-to-peer networks and video streaming sites such as YouTube.com. We should add, however, that the presence of overcapacity may reflect the fact that we only interviewed ISPs in selected OECD countries. It may be different in other regions.

When we presented these findings to an expert in the economics of Internet traffic, he argued that our interviewees may be suffering from "the fallacy of the near." In his view, ISP employees dealing with security-related issues mention customer contact as their biggest cost because they are focused on the security budget, which includes the abuse desk as well as security-related customer support. To them the infrastructure cost "is just a number their accountant writes on a check every month."

However, infrastructure is the main overall cost for any ISP, so any effect of malware on capital expenditures could potentially outstrip other expenditures. These costs do not gradually increase with the amount of malware and spam, but rather as a step function when capacity runs out. It is very difficult to relate these expenditures back to specific traffic patterns of spam and malware infections. Only higher up in the organisation are people in a position to compare the relevant numbers, although at that level the necessary security expertise and data is often missing. The interviewee argued that there are really three groups of people who all see a part of the problem, without being able to cross-connect it: "One group is dealing with malware, one group is dealing with the capital expenditures and engineering build-out and another group is dealing with handling the money." In terms of incentives, however, this lack of awareness implies that infrastructure cost is not a strong driver of the attempts of ISPs to reduce the impact of malware.

Benefits of maintaining reciprocity

An incentive that was mentioned by all interviewees is related to the informal networks of trusted security personnel across ISPs, CSIRTS and related organisations – which we mentioned earlier. When describing how their organisation responded to security incidents, interviewees would refer to personal contacts within this trust network that enabled them, for example, to get another ISP to quickly act on a case of abuse. There is not one informal network, but rather several overlapping ones. An ISP may approach a contact at a national CERT in another country so as to get in touch with the relevant person at an ISP in that country. These contacts are reciprocal. They are also contacted about abuse in their own network and are expected to act on that information. The incentive is that to maintain reciprocity, an ISP has to treat abuse complaints seriously, which is costly. The more abuse takes place on its network, the more other contacts in the network will ask for intervention.

Maintaining reciprocity not only establishes the informal network as a security resource, it also reduces the likelihood of being hit with blacklisting or other countermeasures. As one interviewee explained, "when we get in touch with service providers, we're saying, get this guy off the network or we're null routing your network from ours. If enough people do that, eventually they try to address security. The same thing happens if we have highly infected end-users hitting someone else, via malware or intentionally. What enforces security on a service provider is threats from other service providers." ISPs that are linked to the important informal networks typically get more leeway to deal with security issues before significant blacklisting occurs. One ISP security officer told us that these informal contacts imply cost savings. Less staff time is needed to deal with the fallout of a security incident – *e.g.* going through time-consuming procedures to get off blacklists – and to deal with customer support.

ISP disincentives

Costs of security measures

So far we have discussed incentives that reinforce the benefits of security for ISPs with regard to malware. The incentive structure is mixed, however, and includes disincentives as well. An obvious disincentive is the costs of additional security measures. Typically, the trade-off is between the direct costs of additional measures, which are visible in the short term, versus the costs generated by increasing security problems, such as customer support and abuse management. A security expert at a large ISP told us that for management it is difficult to estimate the amount of money the company may save with a technical solution which is supposed to reduce the costs of the abuse desk or call centre. Another interviewee added that a complicating factor was that managers had encountered over-promising security providers who sold them 'magic boxes' that were supposed to solve everything.

We should mention, however, that the ISP's decisions often were not shaped by formal economic assessments or detailed analysis of their own cost structures. As one insider phrased it, "ISPs very much drive by the seat of their pants. Except for a very few of the largest ones, they are not actually examining the figures." When we asked how certain investments or measures were approved, the "business case" that supported them was typically rather commonsensical in nature, including rough estimates of direct costs and benefits, with the indirect ones not monetised or otherwise specified in any amount of detail.

One interviewee told us that when considering security investments, they "look at the cost of *not* doing it" for which they produce rough estimates. Another ISP explained to us how they decided to set up a so-called 'walled garden experience' for infected users. Rather than disconnecting these users completely, the 'walled garden' provided them with access to security tools and Windows Update. A security officer explained the rationale behind this decision: "It costs a server or two. The rest of the stuff was free, we could reconfigure our existing infrastructure. The investments were the time that I put in. The 'walled garden' has a financial benefit because then the customer does not have to call as often."

Legal risks and constraints

Another disincentive is related to legal constraints. During the interviews, the European ISPs had different answers to the question on how much manoeuvring space the 'mere conduit' provision of the EU E-Commerce Directive allowed them. Monitoring their network more closely for security reasons could potentially lead to liability issues, some of the interviewees felt. In some EU countries, interviewees reported that privacy regulations that potentially treat IP addresses as private data had led their legal departments to set boundaries which affected the ability of the security staff to track malicious activity on their network – for example with regard to tracking individual IP addresses.

One interviewee reported that security staff sometimes were not allowed to use information on malicious activity detected on the network. When asked about the limits of the 'mere conduit' provision, one security officer responded that they never encountered these limits, because the privacy regulations were much more constraining. Rather than monitoring their own network, this particular ISP could act on incoming abuse notifications for specific IP addresses and it relied heavily on this procedure. In a sense, the ISP was monitoring its own network through the incoming notifications from other ISPs, CSIRTs and the like.

Elsewhere there have been reports over liability issues around countermeasures, such as discarding the command and control traffic of a botnet or diverting it to where the botnet's behaviour can be studied more closely (Higgins, 2007a). According to a security researcher "it involves mucking with a customer or peer's Internet address space... Obviously, liability in this area could be considerable." A security manager at a European ISP said "infiltrating is very risky and getting legal support for such matters, very difficult."

Some legal experts argued that these legal risks are non-existent, that they are based on an incorrect understanding of current legislation – *e.g.* that the EU data protection legislation does not at all conflict with network monitoring and other security measures. While that might be true, the reality is that the legal departments of some ISPs apparently interpret the situation – perhaps mistakenly – as rather ambiguous. These ISPs tend to be rather risk averse in dealing with this ambiguity. The transaction costs of clarifying these issues are, *ceteris paribus*, an obstacle to higher security.

Cost of customer acquisition

Other disincentives are closely related to the incentives discussed earlier. An interviewee at a large ISP mentioned brand damage as the reason why the business side of their company initially opposed the security measure to block port 25. They did not want to inconvenience their customers. Anything that might turn people away is a problem, because the cost of acquisition of new customers is high. The burden of proof fell on the security staff to convince management that the proposed measures were protecting the brand. Other ISPs also mentioned going to great lengths to avoid losing customers while managing abuse. That might limit the effectiveness of their response to security incidents.

Rogue ISPs

Some of the security-enhancing incentives discussed above work as disincentives under different business models than those of the ISPs we interviewed. When dealing with abuse complaints becomes too costly, one can either reduce the amount of abuse on the network or one can reduce management of abuse – *i.e.* become less responsive to the complaints themselves. The same holds for customer support. In fact, such a lack of security could be part of the business model. It may, for example, allow an ISP to be cheaper than its competitors. One ISP indicated that a certain segment of its customers was actually “mini ISPs” which predominantly offered hosting services. The mini ISPs’ retail prices were significantly lower than those of the upstream ISP from which they bought access, because they provided very limited support functions. Some of these mini ISPs would not patch their servers properly, thus becoming an easy target for malware. They were not very responsive to abuse complaints either. Our interviewee, being an upstream access provider, would then be contacted by other ISPs to take action against the mini ISP.

Another business model is sometimes referred to as “rogue ISP” or ISPs that are, in the words of one interviewee, “decidedly grey”. These attract customers precisely because of their lax security policies. While these ISPs have more disincentives for improving security than the ones interviewed, they are not fully immune to some of the security-enhancing incentives we discussed earlier, most notably blacklisting. As one interviewee explained: “There are some ISPs in our country that are decidedly grey. They will take anyone and take no action against abuse. People will go there and then they will leave again, because they are unreachable [because of blacklisting].” Even rogue business models are eventually affected by blacklisting. “Suddenly, a Ukrainian ISP started answering our abuse reports,” the interviewee continued. “Chances are that blacklisting had an effect on their business model. They are still not trustworthy, but it’s a lot better.”

An additional incentive for non-responsive ISPs is the pressure put on them by their upstream providers – the ISP “who feeds them the Internet,” as one respondent phrased it. The higher up the stream, the more likely it is to find a provider who is in fact security conscious and sensitive to the incentives discussed earlier, such as maintaining reciprocity and blacklisting. In the example of the mini ISPs, their upstream provider forces them to deal with abuse complaints, because it reflects badly on the upstream provider if they do not. Beyond blacklisting, there is also de-peering – that is, an ISP may disconnect from a misbehaving ISP at an Internet exchange point. For the ISPs we interviewed, this is not an important incentive, because de-peering for security reasons is typically only employed against rogue ISPs, not among regular ISPs. De-peering forces the disconnected ISP to buy transit service for its traffic, which implies much higher operating costs.

Summary of ISP incentives

The balance between incentives and disincentives will vary depending on the ISP. On the whole, recent years have witnessed increased efforts by ISPs in dealing with malware, even in the absence of regulation or other forms of public oversight. The incentive mechanisms we discussed strengthen the ISP's own interest to internalise at least some security externalities originating from their customers, as well as from other ISPs. In short, the current incentive structure seems to reward better security performance for legitimate market players – though it is sensible to keep in mind that in many countries price competition is intense, which is a disincentive with regards to security, other things being equal.

ISP incentives to confront malware	**Disincentives**
• Lower customer support costs • Less blacklisting • Maintaining reciprocity • Maintaining reputation and limiting brand damage	• Costs of security • Legal restraints • Costs of customer acquisition

Other key considerations for ISPs

Automation

Several ISPs explained that they were at some stage of implementing technology that would automate the process of monitoring malicious behaviour on their network and quarantining the infected machines. One system monitored the network, cleaned malware from the traffic and automatically generated a list of 2 500 IP addresses a day of customers who have some form of security problem. When these cases hit a certain threshold, they would be automatically quarantined to only have access to Windows Updates and a range of security services.

While the technologies to automate the process of quarantining would help to scale up the ISPs response, it also brings into focus a critical bottleneck: the costs of customer support would become prohibitive if all infected machines were to be quarantined. A security officer at a large ISP estimated that the number of customers that would be affected at any time would be in the tens of thousands. While this number might go down over time as network security improves, it was obvious that the business side would not accept the cost impacts of such a measure.

Typically, the number of machines that are isolated on a daily basis is relatively modest – tens or, for large ISPs, perhaps hundreds of machines. At this level, the effort is effective in that it reduces the ISP's problems with abuse and blacklisting. But compared to estimates of the total number of infections on each network, these efforts look rather pale. When asked to assess the ratio between the actual number of infected machines on their network and the number of machines for which they receive abuse notifications, most interviewees estimate that the ratio is quite low. Only a small percentage of these machines would show up in abuse notifications and be dealt with. One interviewee called this "the two percent rule." A security expert was highly critical of the effectiveness of the efforts by ISPs: "Unless they are contacting more than 10 % of their customer base on a monthly basis, they are effectively taking no action".

The limit of ISP incentives

A related issue is that the incentives of ISPs do not reflect the whole range of current malware threats. ISPs are predominantly sensitive to malware that manifests itself in ways that make their customers call in, leads to abuse notifications or that causes problems with blacklisting. That means spam proxies and DDoS (denial of service) attacks attract attention and raise costs, while spyware, for example, does not: "People get infected and it is very difficult to track them. Spam and DDoS is noticeable at the network level. But spyware stays on the computer, quietly collecting data." Others have argued that many ISPs are failing to prohibit the forging or spoofing of IP addresses by hosts as well as failing to filter outgoing traffic from IP addresses from which they are not authorised to originate.

Those security problems that are noticeable for the ISP will not always be addressed, either. Several ISPs mentioned "thresholds" of malware effects which needed to be crossed, before they would act on a customer's infected machine. Even then, the situation is often anything but straightforward. "The issue is, how do you help the people who are infected, given the current state of the security products in the market place? We see the traffic, we know there's something wrong, but how do you find what it is with the current products? It's very hard... About 85-90% of the malware is not recognised by AV products, because a small change is enough to dodge the signature."

Dealing with rogue ISPs

Another important caveat is that there are classes of ISPs for which the incentives to improve security are too weak, or which even have strong disincentives to improve it, as discussed above. The ISPs we interviewed treat the existence of such ISPs as a fact. Because it is possible for rogue ISPs to stay outside the reach of legislation and law enforcement, they are going to be present for the foreseeable future. The ISPs we interviewed have learned to live with the presence of the rogue and semi-legitimate ISPs. They have found that they are able to operate quite effectively in this environment through a combination of tactics, including those mentioned earlier, such as informal contacts that address upstream providers and blacklisting.

In the mind of ISPs, no matter what policies, governance structures or incentives are put in place there will always be some providers, outside or inside their own jurisdiction, who will be a source of malware and other forms of abuse. Once this is accepted, then it is also accepted that an ISP has to build defenses and develop procedures for dealing with attacks. "You will always have to accept a certain level of noise, that is, of evil. You try to keep it below a certain threshold of irritation" said a security officer. This is one of the reasons why many ISPs are not impressed by proposals to regulate some set of baseline or best security practices for ISPs. One such proposal was under development by the Dutch electronic communications regulator OPTA but it was shelved for the time being after significant pushback regarding the legal basis for such regulations. The recent report of the UK House of Lords Science and Technology Committee (2007a, p. 31) also advocated making "good practice... the industry norm[, by means of regulation if necessary.]"

The fact that ISPs can work within the insecure status quo does not mean that their responses are static or complacent. The status quo actually contains significant incentives to improve security, which is why we have seen major changes over the past couple of years. Ironically, some of these changes, such as the policy to isolate infected machines, are not really advertised, for fear of dissuading customers from signing up.

E-commerce companies

The multitude of companies that buy and sell products or services over the Internet operate on a wide variety of business models, each with different incentive structures for security. We have chosen to focus on online financial services, since they have been an important target of malware attacks, arguably more than any other sector (Counterpane & MessageLabs, 2006). This includes brick-and-mortar banks that are offering part of their service portfolio online, credit card companies, as well as online-only financial service providers, such as PayPal. The sector has been confronted with a wide range of threats ranging from botnet-assisted phishing spam runs and phishing websites, to keyloggers and Trojans that enable man-in-the-middle attacks during secure banking sessions.

Incentive: increased online transaction volume

A key incentive for all these companies: a growing volume of online transactions. Credit card companies and online financial service providers typically charge a fee per transaction, either a flat amount or a percentage of the transaction. The situation is somewhat different for brick-and-mortar banks. For many of their services, they do not make any money from the transaction itself. Their incentive to pursue online banking is the considerable cost savings that it enables. Two of the interviewees in the financial sector estimated that online transactions were in the order of 100 times cheaper than processing those transactions offline, through their branch offices, mail or phone. Given the enormous volume of financial transactions, costs savings of that magnitude translate into a very powerful incentive to move online as much these services as possible.

How does this incentive affect security decisions? To answer that question, we need to understand how transaction volume interacts with several other incentives: the benefits of trust in the online services; the benefits of usability; the cost of security measures; and the cost of fraud.

Incentive: consumer trust

Within the sector, it is assumed that consumer trust in the security of these services is a necessary condition for their uptake. This rewards investing in security. Beyond this generic consensus, however, views quickly diverge. There is disagreement about how big a role trust plays in driving the use of online services. Furthermore, it is unclear whether the current security problems with online financial services actually reduce that trust.

Several consumer surveys suggest that security problems turn people away from e-commerce and online banking, in particular. The 2006 UK Get Safe Online survey reported that the fear of falling victim to Internet crime deters 24% of respondents from Internet banking and has put off 17% from Internet use all together (GetSafeOnline, 2006). It is difficult to interpret the meaning of these findings when compared to other data. For example, most financial service providers still report significant growth rates in the adoption of their online services (PayPal,2007). These two seemingly contradictory pieces of evidence point out that the role and impact of trust is not yet adequately understood. An industry study of trust in e-commerce (Lacohée *et al.,* 2006) argued that "[w]hile an initial hypothesis may be that people do not engage with online services because they do not trust them, our findings have shown that trust is not as significant a measure as first thought.

What is more important to understand is that people are willing to take risks online, as long as they are informed, and it is clear how consequences will be addressed. People use specific services not because they trust them, but because they in some way provide a benefit to the individual and they know that if something goes wrong, restitution will be made." This suggests that an important factor driving the use of online financial services is not the level of trust in the security of these services, but the more specific expectation that a customer will be compensated in case of fraud. In other words, from a customer's perspective, it seems more important that financial service providers assume liability for online fraud than that they achieve a certain level of – perceived – security.

The trade-offs

Access and usability vs. security

Assuming that increased security increases consumer trust and, in turn, increases the uptake of online services, this effect would still need to be weighed against the effects of increased security measures on the usability of the service. One of our interviewees at a bank with an international presence explained that the national branches of his company positioned themselves differently with regard to this trade-off. While in some countries, two-factor authentication was readily accepted; in other countries the bank thought its customers were less open to such security-enhancing technology. If such measures were to significantly raise the threshold for people to do online banking, then the incentive to increase the volume of online transactions would influence decision making against such measures – even if this meant that fraud losses in those countries might be higher. By balancing usability and security, these companies try to maximise the growth of online financial transactions, while keeping the level of fraud at manageable levels.

Rising online volume vs. losses due to fraud

Another important incentive for security is the fraud losses that accompany the increasing volume of online transactions. In the United States, banks are liable for direct fraud losses under the Electronic Funds Transfer Act of 1978 – also known as "Regulation E". Under this regime, customers are compensated for such losses, unless the bank can prove that the customer's claims are false. In many other jurisdictions, the banks are strictly speaking not liable for such losses. In practice, however, the banking sector has often adopted voluntary codes which specify that customers who suffer losses are compensated – unless there are clear indications that they have colluded in the fraud.

To understand how the cost of fraud influences security decisions, it is important to look at some of the available numbers. The United Kingdom has arguably the best data available. APACS, the UK payments associations, publishes numbers based on actual banking data, not estimates based on samples and extrapolation. As one would expect, direct losses from phishing fraud in the United Kingdom have risen, though with a recent fall: from GBP 12.2 million in 2004 to GBP 33.5 million in 2006 to GBP 22.6 million in 2007 (APACS, 2008). Over the past years, the number of phishing attacks has increased significantly: from 2 369 attacks in 2006 Q1 to 10 235 in 2008 Q1. The broader fraud category of "card-not-present" fraud – which includes phone, Internet and mail order fraud – has risen from GBP 150.8 million in 2004 to GBP 290.5 million in 2007.

Not to downplay the seriousness of these losses, but it is important to realise that the damage of phishing attacks is still well below the numbers for other fraud categories, such as stolen or lost cards (GBP 56.2 million in 2007) and counterfeit card fraud (GBP 144.3 million in 2007). Furthermore, while these numbers are going up in absolute terms, so is the number of customers banking online, as well as the overall volume of online transactions. APACS argues that the rise in card-not-present fraud should be viewed against the increase in the use of online or telephone transactions. While fraud has risen by 122 % from 2001 to 2006, the use of online or telephone shopping itself has grown by 358 %. Unfortunately, the available data is not sufficiently disaggregated to allow APACS to calculate fraud relative to volume. Credit card companies do publish such numbers. In 2006, VISA Europe reported that their overall fraud rate was at "an all time low" of 0.051% (fraud to sales by cards issued). However, card-not-present fraud, which includes online fraud, was the fastest growing type of fraud and now accounted for 40% of cases. PayPal recently reported their direct losses to fraud being 0.41% of overall transactions, but would not give information on the trend of their losses (House of Lords 2007b, p. 196).

Cost and implementation of security measures

While exact figures are hard to come by, the companies we interviewed all said their security investment levels are much higher than their direct yearly losses, often by one or two orders of magnitude. The capacity to deal with incidents is often already more expensive, let alone all of the preparatory measures and security defenses being put in place, such as the introduction of two-factor or three-factor authentication.

The reason for this level of investment is that direct losses are not seen as representative of the overall problem. It would be much more devastating, for example, if online fraud eroded customer trust or slowed down the uptake of online financial services. Furthermore, there are reputation effects for banks that are targeted by attackers as well as for the industry as a whole. Nobody has robust estimates on either of these effects, which makes it difficult for financial companies to calibrate their security investments.

In general, the incentives are to keep fraud at acceptable levels and compensate victims, rather than to eliminate it. The latter would be economically inefficient, not only in terms of direct cost but more importantly because pushing fraud back further might require the introduction of security measures that make the use of online financial services less attractive to customers. A reduction in the growth of the online transaction volume is likely to imply higher costs for banks than the current damage caused by online fraud.

Companies, alone and through sector-wide collaboration, assess risks and prepare new security measures, which can be rolled out when they feel the current defenses are no longer adequate. Exactly when is hard to specify. Some innovations have been put in place rather quickly. Phishing attacks, for example, are increasingly dealt with by contracting out response efforts to security providers who scan for phishing spam and hunt down sites that resemble the official bank website, at which time they initiate notice and takedown procedures. Occasionally, this takes down legitimate web banking sites as well, when the security department is not aware of a marketing initiative from another part of the organisation and thus has not whitelisted the domain name.

Other innovations are deemed too costly and not implemented. In the Netherlands, for example, there has been an ongoing series of successful attacks on the two-factor authentication systems of most banks. Rather than introducing new structural security measures, the banks have made incremental changes to their two-factor authentication systems, which are relatively easy for the attackers to defeat. More structural measures, such as transaction authentication or three-factor identification, would require costly modifications to the back-office systems, as well as requiring customers to learn new and more laborious security methods.

So far, the response has been to make minor revisions to existing systems so as to disable the last successful attack tactic. These measures are often accompanied by a number of other safeguards – such as temporarily slowing down the processing of real-time transactions. The direct financial losses of each attack have been relatively low, which makes the possibility of another successful attack less unpalatable. Ironically, one interviewee mentioned that the relatively modest losses per incident appear to be a deliberate strategy of the attackers. These attacks are trying to stay under the radar of the fraud detection systems – as well as making it less worthwhile for law enforcement officers to devote a large amount of resources to tracking down the criminals.

Summary of incentives for financial service providers

The incentives of financial service providers are such that in many cases the companies compensate customers for the damage they suffered from online fraud. They are willing to internalise these costs because the benefits far outweigh them. In that sense, they internalise the externalities of sub-optimal security investments and behaviours of their customers, as well as the software vendors whose software is exploited to execute the attacks. Interviewees told us that when designing the security of their services, they have to assume that the end user PC is compromised. Many financial service providers claim they compensate all malware related losses. If that claim is accurate, then the security level achieved by the whole value net may not be too far from the optimum. The financial institutions bear the externalities, but they are also in a position to manage the risk through their security measures on online financial services.

Other key considerations

Incomplete information on customer trust

First, one could argue that there are still externalities in the sense that important societal efficiencies could be gained if people had higher trust in these services and would adopt them more quickly. These benefits could outweigh the additional security investments that would be needed. While the magnitude of these externalities is unknown, the financial service providers are the ones who stand to gain most from maintaining high trust in online services and, more to the point, from the increased adoption of these services. In other words, this is a problem of incomplete information, rather than of misaligned incentives.

Incomplete compensation of fraud losses

A second consideration is that not all fraud-related costs to customers are compensated. While the financial institutions compensate victims for their direct losses, this might not cover all the losses that result from the fraud. In cases of identity theft, victims may not get all costs reimbursed and they may struggle for years with the consequences of having their personal information abused, such as blemished credit reports (TechWebNews, 2005).

Shifting liability to merchants/customers

Third, in several countries the banking sector is re-considering the existing liability regime, which might lead to "liability dumping". Financial service providers have already started to push more liability onto the merchants. It seems we might see a similar trend for customers. Late in 2006, the Ombudsman for the German banking sector ruled against a customer who claimed to have been victimised by a Trojan, arguing that the customer provided no proof of a successful malware attack (A-i3 2006; Banktip, 2006). The Ombudsman declared that the customer was not able to provide evidence of a successful malware attack, even though the customer's machine was infected with malware. This appears to shift the burden of proof onto the customer.

In New Zealand, the banking association introduced a new code that has shifted at least part of the liability to customers. The new code allows the banks to request access to the customers' computer to verify that the operating system, the anti-virus software and firewall were all up to date. If this access is refused, or the computer is deemed inadequately protected, the customer's claim may be turned down. Shortly after it was adopted, the code drew severe criticism. In response, several banks and other stakeholders demanded changes that offer more protection to consumers. Currently, the debate seems to focused on the complicated question of determining just what part of the responsibility lies with consumers (South, 2007).

The development of what one could call 're-externalising' fraud losses to the customers is not without risks to the banks themselves, as customer trust in Internet banking is partly based on the expectation that fraud losses are compensated. If customers experience more liability for their online transactions, it might reduce the uptake of these services, which directly affects the banks major incentive: the growth of online transaction volume.

For this reason, a security official at a financial service provider called the attempts to shift part of the liability to customers "a very dangerous path to follow."

Internalising the cost of fraud

Ironically, the existing liability regime might actually be in the best interests of banks. By paying for, or internalising, the damages, whether required by law or voluntarily, banks have retained the freedom to balance the level of security against other factors, most notably the cost of security measures and the usability of online services. This has allowed them to make more cost-effective trade-offs than under a different liability regime. If they shift more liability towards their customers, they then run the risk of inviting more regulatory oversight for consumer protection.

One interviewee told us that while the US banks fiercely opposed the Electronic Funds Transfer Act of 1978 since it placed all liability on them, over time many in the industry realised that the regime was actually economically more rational for them. He called it "a blessing in disguise". Anderson (2007) found that during the period when the British banks operated under a more lenient liability regime for ATM withdrawals than the US banks, they actually spent more on security, as they were doing 'due diligence,' rather than actual risk reduction.

Some financial service providers argue that the current practice of compensating victims might provide a perverse incentive by rewarding customers for not securing their machine. Earlier experiences with ATM fraud suggest the risk of such a perverse incentive is manageable (Anderson, 2007). Should banks pass on the cost of fraud to customers and merchants – or ignore potentially rising forms of damage that are currently not compensated, such as the cost of recovering from identity theft – then this might in the end lead to underinvestment, or even overinvestment, on the part of the banks, since they would be investing on the basis of due diligence rather than actual risk reduction (Anderson, 2007). In either case, the new incentives for financial service providers would shift the level, and type, of their security investments away from the societal optimum.

Software vendors

The very nature of malware focuses attention on software vendors. Malicious code exists because of software vulnerabilities that can be exploited – though we should not forget that there is also a class of malware that is based on social engineering, *i.e.* tricking users into voluntarily installing software that includes malware. The software market is highly differentiated, although there are many linkages between segments, such as operating systems and application software. Nonetheless, each market segment has somewhat different characteristics and hence creates different incentives for software vendors to improve security prior and after release, and for malware writers to exploit vulnerabilities.

In recent years, much has been written about the incentives for software security. The predominant view seems to be that software markets do not reward security. In the words of Anderson and Moore (2007, p. 7): "In many markets, the attitude of 'ship it Tuesday and get it right by version 3' is perfectly rational behaviour."

First, some authors claim that security is a "market for lemons", as consumers cannot tell secure from less secure software. One interviewee told us that he was in fact able to assess the security of the software his organisation bought, but that the different products were more or less the same in terms of security. So there was no real 'secure' alternative.

Second, many segments of the software market tend to have dominant firms because of the combination of high fixed costs and low marginal costs, positive network externalities and customer lock-in because of interoperability and compatibility issues. "So winning market races is all important", Anderson and Moore conclude (2007, p. 7). "In such races, competitors must appeal to complementers, such as application developers, for whom security gets in the way; and security tends to be a lemons market anyway. So platform vendors start off with too little security, and such as they provide tends to be designed so that the compliance costs are dumped on the end users."

The analysis provides a powerful explanation for how we got to the current state of affairs. Its implications are less clear for what happens after the race-to-market has been won by a software vendor. While any generalisation is problematic, recent years have seen substantially increased efforts by many vendors to improve the security of their software. The development and deployment of vulnerability patches has improved. Arguably more important, the development of the software itself is increasingly focusing on security issues. Most of our interviewees agreed on this. They disagreed over the effectiveness of these efforts – some argued it was too little too late, others thought the market was moving in the right direction.

The case of Microsoft

For obvious reasons, one cannot avoid mentioning Microsoft in this context. The company's problems and efforts have been most visible. By now, the story is well known. Given the market dominance of its Windows operating system, it has been a key target for malware writers. When the security problems plaguing the platform mushroomed early this decade, most notably in the form of global worm and virus outbreaks, Microsoft saw itself forced to change its approach. It all but halted development on its new operating system and re-tasked many developers to work on much-needed security improvements for its existing platform, Windows XP. These improvements were released in 2004 as Windows XP Service Pack 2 (SP2). While SP2 contained many vulnerability patches, it also introduced changes in the code base that set out to reduce the potential for vulnerabilities to be exploited. Furthermore, it turned on automatic updates and the Windows firewall by default.

For a variety of reasons, security among them, Microsoft then overhauled the code base for what would become Windows Vista, the successor to XP, at the cost of serious delays in the process. Vista's design introduced better security principles, which inevitably led to numerous compatibility problems when hardware vendors and independent software vendors had to adapt their drivers and programs to the new design. To a significant extent, the problems persisted even after the final release of Vista. Many would agree that these problems have slowed the adoption of Vista, as businesses and consumers wait for these problems to be resolved before switching. All of this implies substantial opportunity costs for Microsoft. There are no publicly available cost estimates, but it seems obvious that the security-related costs of SP2 and Vista are anything but trivial, even for a company of this size.

Microsoft is not alone in this trend reversal, though it might be the most dramatic example. In contrast, there are vendors who operate in markets that have demanded security from the start, such as the defense industry. These vendors have developed along a different path compared to those in the mass consumer market. As a result, their business models make it easier for them to economically justify security investments in the software development process. Just to be clear, the increased efforts in software security do not mean the problem of malware is getting smaller, or even that the frequency with which vulnerabilities diminish is discovered. There is a variety of factors at play, not least of which is end users behaviour, which in combination determine if, how and when more secure software reduces the problem of malware.

Notwithstanding the different business models of software vendors, a number of incentives explain why this trend reversal took place. They point to the complex interplay between incentives and disincentives for security. Our findings do not conflict with the incentives mentioned in the literature. Rather, they confirm and complement them by focusing attention on the incentives for established software vendors, *i.e.* after the "race-to-market" has been won.

Incentives for software vendors

Costs of vulnerability patching

Developing patches for discovered vulnerabilities is costly, even if the fix itself is not hard to write. As one senior software security professional explained: "It's like the Mastercard commercial – two line code change, 20 minutes, finding every other related vulnerability of that type on every affected product version and all related modules, fixing it, testing it, 3 months. Giving the customers a patch they can use that does not break anything, priceless."

Although it is daunting to calculate reliable and comprehensive numbers, the anecdotal evidence we were given suggests that an ongoing process of patch development, testing and release for a complex piece of software – like an operating system or an enterprise database system, which consists of tens of millions lines of code – is easily measured in millions of dollars.

Even more important, some interviewees argued, are the opportunity costs of tasking good software developers with vulnerability patching. One interviewee said: "If you reallocate the developer time for patches to other work, it might not be enough to build a completely new product, but you could build some complex functionality you could charge for. I could build something I could charge money for... if I did not have these defects to remediate."

Patching also imposes costs on the customer who applies the patch. This may include the cost of testing the patch before deploying it within the organisation, the actual deployment for all the relevant systems, as well as the costs of remediation when the patch turns out to "break something" – *e.g.* introduce system instabilities. Several studies have shown these costs to be substantial (*e.g.* August and Tunca, 2006). Strictly speaking, the vendor does not experience these costs, and some have suggested that these costs should be regarded as externalities that the vendor shifts onto its customers (*e.g.* Schneier, 2007).

But there are indirect effects that do affect the vendor. First, patching raises the maintenance costs of the software, which can be considered similar to raising its price and thus lowering demand – although this effect is significantly mitigated in the case of lock-in effects or lack of alternatives. Many enterprises assess the so-called “total cost of ownership” of software, rather than just the price of the licence. It is not uncommon for maintenance costs to be much higher than the price of the licence itself. Second, if patching is too costly for customers, they may not keep their machines adequately patched. The resulting security problems may tarnish the reputation of the software itself – we return to brand damage and reputation effects shortly.

Patches for enterprises vs. home users

In response to these effects, many software vendors have set out to reduce the costs of patching for their customers. For enterprises, patching is a different issue than for home users. The former need to have more control over the deployment of patches as patches potentially disrupt critical systems. In some cases, they might opt to not apply certain patches. “While it would be wonderful if everyone stayed fully updated all of the time,” said one interviewee, “many enterprises choose to do extensive testing first, attempt to avoid blackout periods, and take into account many other considerations specific to their business before an update can be deployed. Enterprises that regularly deploy updates will be less vulnerable to malicious attacks, so with all of that in mind, each business must make the risk trade-off that is appropriate for them.”

The vendors we spoke to described efforts to better support their business customers in this regard. Microsoft, for example, introduced Windows Server Update Services (WSUS), which allows IT administrators to control the deployment of patches across the computers in their network. Furthermore, vendors try to improve the information they provide with patches, so that businesses can make an informed risk assessment regarding if, when and how to deploy a patch.

Several interviewees also indicated that enterprise customers asked for bundled patches, which are tested and released together on a regular schedule (*e.g.* weekly, monthly or quarterly), rather than single-issue fixes that are released as soon as they are ready. “We do not do single fix patches, it’s not economical and you cannot keep the quality up”, said one interviewee, adding that some of their customers even wanted the frequency of patch releases reduced to twice a year, so as to decrease the costs on their end.

For home users, reducing the costs of patching has mainly consisted of developing easier, more user-friendly mechanisms to deliver and install patches. Microsoft developed "Automatic Updates" and turned it on by default in XP SP2. The vendor reported that over 350 million Windows machines worldwide receive the monthly "Malicious Software Removal Tool" through Automatic Updates or Windows Updates (Microsoft, 2007). In the environment of open source software, Firefox – an Internet browser with the second-largest market share, after Microsoft's Internet Explorer – has enabled automatic updates by default since version 1.5. Rather than bundling patches, the developers of Firefox release the patches as soon as they are ready. The default setting of the browser is to download and install them at the earliest opportunity. The developers recently reported that under this new model, 90 % of Firefox users installed a recent security patch within six days (Snyder, 2007).

Is patching always required?

The costs of patching could also work as a disincentive for those software vendors seeking to avoid these costs. As a result, vulnerabilities remain un-patched for too long, assuming they get patched at all, or the quality of the patches might be too low. The urgency of this issue increases if attackers, as has been reported, are moving way from exploiting the operating system and toward third-party applications and hardware drivers (Lemos, 2006).

However, not providing vulnerability patches does not seem to be a tenable strategy for an established vendor whose product is actively being targeted by malware writers. On the other hand, even substantial efforts in patch development can leave a software product vulnerable – *e.g.* because patches are more complicated to develop and test for products that are tightly integrated into a larger software package. An analysis of the known vulnerabilities for Internet Explorer found that for a total 284 days in 2006, there was exploitable code available for known, un-patched critical flaws in Internet Explorer 6 and earlier versions (Krebs, 2007).

If a vendor's market position requires it to perform costly patch development, then these costs might provide incentive for more investment in security early during the development process. This would be done in the hope of reducing the number of vulnerabilities after release – or perhaps more accurately, the frequency with which these vulnerabilities are discovered.

Patching vs. secure software development

While vulnerability patching is generally seen as desirable, although not by everyone (Rescorla, 2004), many have argued that it does not really solve the underlying problem. Finding and patching vulnerabilities might not make the software product itself more secure. Some research suggests that for many products, the discovery rate of bugs is more or less constant over time – in other words, finding and fixing a vulnerability does not reduce the chance of an attacker finding a new vulnerability to exploit (Rescorla, 2004). Furthermore, patch development consumes resources that could have been used to make software more secure before it is released.

This is a valid criticism. However, several interviewees made the case that costly patching procedures still provide an incentive for more up-front investments in secure software development. One argued that the more powerful incentive for secure software development is the fact that back-end patching costs are much higher than the costs of preventing the vulnerability during development. Another interviewee told us: “The argument to make for writing better code is cost avoidance, even if you charge for support (and we do). The way you get a good margin on it is if you can charge for maintenance but you do not have to constantly produce patches because those are expensive; that cuts into your margin.”

We did not come across economic analyses that directly compare the costs of secure development with those of patching. It is unclear whether vendors even have this kind of data available. One interviewee told us: “I cannot add up what we’ve spent on the front-end... Most of secure development is good development, not some special security add-on.”

It seems clear, however, that the costs of secure software development are substantial. It requires more resources and can affect time-to-market of a new product – a critical factor in many software markets, though here too the effect may be tempered by customer lock-in. Furthermore, secure development often involves costly assurance processes. One interviewee described the so-called “Common Criteria” evaluations for major releases of their products. These evaluations are made by external consultants and were estimated to cost between USD 500 000-1 million each – not including the time-consuming involvement of internal staff.

Even in the absence of hard numbers, the interviewees were adamant that there are significant cost savings to be made by investing in secure software development. After Microsoft started its “Security Development Lifecycle” initiative, it published some preliminary numbers, which appeared to support the idea that the new approach resulted in significant reductions in the number of vulnerabilities found after release (Microsoft, 2005). In addition to reducing the direct costs of patching, there are reductions in opportunity costs that potentially are even higher. In the words of one interviewee: "I worry about the opportunity cost of taking good developers and putting them on tasks for security patches for avoidable, preventable defects. That's why we put a lot of work up-front to avoid that. We have training, we have automated tools – anything you can do earlier in the cycle is goodness. It's never been hard to justify those costs."

Cost of brand damage and reputation effects

An additional explanation for the increased security efforts of software vendors are the reputation effects that they suffer for poor security – or enjoy for good security. The strength of these effects are notoriously difficult to estimate. Some have suggested that they provide a fairly weak incentive (Schneier, 2007). Whether that is true or not, it does seem to play a role. The major security-related changes within Microsoft were driven by the major worm and virus outbreaks in 2002 and 2003. The key difference between those security incidents and ones that preceded them was scale and the resulting damage. Neither affected Microsoft directly. The reputation effect of those incidents seems to be the most plausible explanation for the changes in the company's course.

As mentioned earlier, Microsoft has invested in mechanisms to make it easier for its customers to patch their machines, even though they do not suffer the customer's patching costs directly. Furthermore, so far Microsoft has allowed pirated versions of Windows to download security patches. This appears to value the reputation of the platform more than denying services to non-customers. Keeping their customers patched as much as possible helps to reduce the scale of security problems that the platform is associated with.

The incentive of reputation effects might be stronger in open source communities, where reputation is a very valuable resource (*e.g.* Watson, 2005). It might help to understand why early in the development of what would become the Firefox browser – shortly after the code of Netscape Communicator had been open-sourced in 1998 – the developers made a number of security-conscious choices. The security performance of the browser played a key role in the positive evaluations of software reviewers.

Software vendor trade-offs and disincentives

While there are indeed incentives that help us to understand the intensified efforts toward security, they are also counteracting disincentives, which complicate the drive towards more secure software. These disincentives help us to understand why despite increased efforts, making software more secure is difficult under current market conditions.

Improving functionality

"Part of the reason for the mess is that people want fancy gadgets and do not care as much about security, and that's exactly what they got," one software security professional told us. The 'gadgets' referred to in this statement are the functionalities provided by software products. Even vendors with an established market position will at some point want customers to buy a newer version of their product or a complementary product. Another interviewee said: "No-one buys your product only because it is secure, they buy it because it allows them to do new things." The drive of the market to produce ever more powerful software has generated numerous innovations. At the same time, it has made it much harder to build secure software.

Functionality versus security is not necessarily a zero-sum trade-off. New functionality can be security related, for example, or it might be implemented securely. In practice, however, they can be difficult to reconcile. The history of software development is rife with examples where trade-offs in the design of software have favoured functionality over security. Many of the much-maligned features of Microsoft's Internet Explorer, such as its deep integration into the Windows platform, started out as functionality – *e.g.* the ability of a website to silently install code on a user's system, which would increase the functionality of the system without requiring the user to understand and manage the process of installing software. There have been many beneficial uses of this functionality, but it also has turned out to be a huge security risk. In response, IE7, the latest version of Internet Explorer, has reversed many of these design decisions.

There is an intrinsic tension between adding functionality and making software more secure. Security benefits from simplicity and a limited amount of code (*e.g.* Barnum and Gegick, 2005; Bernstein, 2007). Many of today's major software products are neither. The need to expand functionality with each release only exacerbates the situation. Of course, secure software development practices set out to mitigate this problem, by reducing the "attack surface" of a certain functionality and manage the remaining risks or, if the functionality is inherently insecure, to exclude it from the product.

Box 5.1 Microsoft's Vista: An attempt to balance compatibility and security

During the development of Vista, Microsoft decided to change the default way user accounts were set up. This required Microsoft developers to create a viable standard user mode with restricted privileges. They introduced User Account Control (UAC) for this purpose. Their enterprise customers, many of whom wanted to run their desktops under standard user accounts, applauded this development, as it promised to reduce their total cost of ownership. The problem was that it created serious compatibility issues with the existing third-party software, much of which still presumed administrator privileges. While vendors were informed about the upcoming changes, many did not actually adapt their code to work with these features. One interviewee explained that it was not attractive for vendors to comply with the new restrictions, because they had to invest in changing their code just to get the same functionality that they already had before Vista.

When Vista was released, a substantial number of these compatibility issues were unresolved, even though Microsoft itself developed auto-mitigation measures to deal with many application compatibility problems that the vendors did not resolve themselves. Users experienced poor or missing device drivers and incompatible software programs. Many complained about the constant security prompts and warnings that UAC confronted them with. Because many programs did not run properly in standard user mode, they constantly had to ask for elevated privileges, which triggered the UAC prompts. This was exacerbated by the fact that UAC was not implemented very elegantly and thus generated more prompts than needed. As one interviewee explained, the move to UAC "is considered a paradigm shift that can translate into worse user experience if the user is running software that has to elevate every day."

Microsoft anticipated these problems to a certain extent. They felt that the compatibility problems of end users were worth the price of moving the software industry toward building products that could operate under a standard user model. But without a way to force the third-party vendors to adapt their software, this would be "a dangerous game to play," said one interviewee, as Microsoft itself will receive part of the blame for these problems. UAC is one example.

Other security improvements in Vista suffer from the same incentive problem: They only work if the independent software vendors adapt their code. If using the security feature is not turned on by default, the vendors might simply ignore it, which means that the feature does not actually improve security for end users. If the feature is turned on by default or if it cannot be turned off, then users will experience serious compatibility issues. These compatibility issues likely translate into a postponed adoption of Vista, especially by enterprise customers, as they wait for these problems to be sorted out before they move to the new platform. For Microsoft, postponed adoption means that pushing the market towards these security improvements imposes substantial opportunity costs.

On the whole, the benefits of compatibility and inter-operability create strong path dependencies, which can only be broken away from at high cost.

One could argue that as the security-related costs of users go up, the market will reward security-related functionality that can reduce those costs. There are several well-known counter-arguments to this – including lock-in effects, lack of alternatives, weak market signals for security and the information asymmetry between vendor and customer. That said, there appears to be a market demand for certain security improvements, most notably those that reduce the total cost of ownership. Some software products, both proprietary and open source, are actively marketed as being more secure and less costly to maintain than their alternatives or predecessors. Whether the market over time can distinguish between empty claims and security improvements that actually achieve cost-savings is not yet clear.

Ensuring compatibility

As discussed above, software products benefit from positive network externalities. The value of a software platform – such as an operating system – increases non-linearly with the number of users. There are two sides to this: the more users there are, the more vendors will want to develop software for that platform; and the more software there is for the platform, the more users will want to adopt it. Anderson and Moore (2007, p. 5) concluded that all of this implies that platform vendors will impose few security restrictions so as to appeal to third party software vendors – *i.e.* to maintain compatibility and inter-operability of software. How these incentives play out of for a specific vendor depends on the type of product they provide and the position they have in the market.

For a dominant platform, maintaining compatibility is key when moving from one version to the next. As one industry insider told us: “The only thing [Microsoft] cared about in the transition from Windows 95 or Windows 98 to Windows XP was application compatibility, otherwise people would never move to XP.” This had all kinds of effects on security and the problem of malware.

To achieve maximum compatibility, the default installation of XP set every user up with administrator privileges, which means that people typically operated their machine under a user account that allowed unrestricted control over the machine. From a security standpoint, this is undesirable, because it means that once a machine is successfully attacked during use, malware has full access to the machine and can, for example, apply changes to the operating system and install root kits that are incredibly difficult to detect and clean up. Better security practice would be to set up an administrator account to be used only when new software needs to be installed or system changes need to be made. The rest of the time, users should run by default as standard users, with restricted privileges. This reduces the “attack surface” – *i.e.,* the amount of code, interfaces, services, and protocols available to an attacker.

In response to the default user setup of XP, third-party vendors assumed that all users would run with administrator privileges and they designed their programs accordingly. In turn, because so much software assumed the user ran with administrator privileges, running the system as a regular user with limited privileges was not really viable. “The end user was pretty much forced to run as administrator”, said one interviewee. While they might not have much of a choice, end users were accustomed to having full control over their machine, unbothered by security restrictions.

Large organisations did sometimes set up the desktops of their employees with restricted regular user accounts. This is a costly set up, however, because it requires a lot of support staff to manage these installations. Even minor changes needed administrator privileges and thus a support staff action. Of course, if you set up your users as administrators, the support costs are also high, because of the increased security risks. The only way to break out of this self-reinforcing costly path is for everyone to adapt their behaviour.

Allowing for user discretion

An issue that runs throughout the challenge of software security is user discretion – that is, key decisions about how to configure and operate the software product are left to the user. The user – or in enterprise contexts, the IT administrator – decides whether or not to install vulnerability patches, the user decides whether to operate within User Account Control or to turn it off, the user decides how to configure a firewall, and so on.

User discretion allows software products to be adapted to a wide variety of contexts and user preferences. That means the product can reach a wider market and can create more benefits for its users, making it more valuable. Perhaps more importantly, user discretion touches on property rights. Software runs on machines that are not owned by the vendor. In principle, it’s the owners who should be able to decide how to balance trade-offs between functionality, performance, availability and, yes, security – as well as any other value relevant to them. After all, the owners are the first to bear liability for what their system does – whether this affects themselves when patch deployment breaks critical business applications, for example, or others, when their systems are compromised and used to attack other users. “We are not in the business of telling our users what to do,” was how one interviewee summarised it. “We can inform them, educate them and provide them with the appropriate tools, but we cannot make these decisions for them.”

With user discretion comes user responsibility. This is a blessing and a curse for software vendors. The blessing is obvious: many of the current security problems fall within the realm of user behaviour rather than within the realm of software production. This shields vendors from part of the responsibility to resolve these problems. Of course, it is also a curse. The decisions that users make affect the security performance of a product, which in turn affect the reputation of the product and its vendor. There is plenty of evidence demonstrating that in many cases, users lack the information or expertise needed to make rational security trade-offs or that their decisions do not account for the costs they impose on others – including, but not limited to, reputation damage to the software vendor.

There are limits to user discretion. There are hard limits, where software simply does not enable or allow you to take certain actions, and softer limits, where the default configuration of a product tries to guide behaviour in a certain direction. For example, when Microsoft introduced UAC, it turned the feature on by default, but it did include the possibility to turn it off by changing the system settings. Preliminary feedback indicates that, so far, over three quarters of users keep UAC turned on.

Where and how to set such limits is a difficult balancing act for vendors. It implies many trade-offs between user discretion and protecting the integrity and reputation of the product. As one interviewee explained:

"That debate raged on for four years straight, from the team level to the senior VP level and we rehashed that debate fifty times in those four years. You know – what should the defaults be and how much pain can we put the users in to get through to the independent software vendors? Are we being too aggressive with this plan or are we not aggressive enough? It was a huge engineering decision that really took a lot of guts at the VP level to support because we knew we were going to generate some customer dissatisfaction. But the alternative is to say: I hope anti-malware engines can keep up with malware."

Summary of incentives for software vendors

Software vendors work under a mixed set of incentives, which may vary for different market segments. They do experience increasing costs as a result of growing security problems, most notably the direct and indirect costs of patch development and reputation effects. That explains why many vendors have substantially increased efforts to improve the security of their software. The vendors also experience incentives that make it costly and difficult to introduce more secure software, even if they are willing to invest in development.

The net effect of the mixed set of incentives is dependent on the product and the market segment in which the vendor operates. Assuming all other things are equal, the increased efforts mitigate software-related security problems. However, at the same time as security efforts are being increased, malware is becoming more sophisticated, adapting to the new defenses. Notwithstanding the efforts of software vendors, many of our interviewees expected that the situation would get worse still, before it would get better.

Vendors do not bear the full costs of software insecurity – *i.e.* there are externalities. Schneier (2007) has repeatedly argued that all the money that consumers of software products are spending on additional security products and services should be counted as externalities generated by those software products. That might not be fully correct and it may overestimate the size of the problem.

To a certain extent, security problems are connected to users' decisions and behaviours – as is inevitable, given user discretion over the configuration and use of software, as well as social engineering attacks which do not need software vulnerabilities to compromise a system. If somebody decides to buy a cheap or highly functional software product with known security problems plus separate security software, it is that consumer's choice and this should not be treated as an externality. In theory, a well-functioning market would offer software with different degrees of protection and let consumers choose. However, that assumes that everybody has full information and that there are no externalities on the consumer side. As we know, in many software markets consumers experience lock-in effects or a lack of alternatives. So there are externalities generated by the vendors' decisions, but they are probably lower than the total cost of security measures.

Domain registrars

The Domain Names System (DNS) is part of the Internet infrastructure, and as such it is affected by malware in a variety of ways. There have been highly publicised botnet-assisted denial of service (DDoS) attacks on root servers and TLD name server operators, aided by sophisticated tactics that employ the existing DNS infrastructure to amplify the attacks.

In addition to the threats to the DNS infrastructure posed by malware, new attacks that combine phishing with compromised web servers or end user machines – such as so-called "rock-phish" attacks and "fast-flux phishing domains" – have pulled the registrars more directly into the fight against malware. The fight against phishing is led predominantly by market players who are targeted by the attacks – *i.e.* banks, e-commerce companies, etc. – or by security service providers working on their behalf, often assisted by expert volunteers working at ISPs, CSIRTs and other organisations.

The procedures to take down phishing sites are changing constantly, as attackers adapt their strategy in response. Typically, ISPs and registrars are involved in taking down a phishing site. The first takes down the hosting website, while the latter removes, suspends or redirects the domain names used by the attackers. Redirecting a domain name means sending the traffic to another location, typically to allow law enforcement or security specialists to examine it more closely.

Suspension is sometimes preferred over removal, as the latter would allow the attacker to register the name again elsewhere. The response of ISPs and registrars to the notification of phishing sites varies. Some act swiftly, others do not. At the latter extreme, we find bullet-proof hosting, whose business model is based on non-response and keeping malicious sites online as long as possible. Research suggests that legitimate ISPs and registrars, once they are under pressure to act, go through a learning process and develop procedures to deal more swiftly with abuse (Clayton, 2007). At that point, the criminal activity starts to migrate to other, easier targets.

The transaction costs of domain name registration itself are very low – as evidenced by the practice of "domain tasting", where millions of domain names are registered, the overwhelming majority of which are cancelled before the so-called "grace period" expires. For the registrar, this process is profitable because it enables a business model to find profitable domain names through trial and error, which drives up the number of registrations that do make it past the grace period and thus generate revenue. Some interviewees suggested that there is a relation between domain tasting and malware, but within the context of this study we have been unable to find sources to clarify and corroborate that relation.

Incentives of domain registrars

The incentives of ISPs were discussed earlier. What about the registrars? To a significant extent, ISPs and registrars are overlapping categories. Domain name registration is an extremely low margin business, which is why many registrars tie them to complementary conventional ISP-type services, such as web hosting and hosted e-mail services. Some registrars even offer domain names at a slight loss, in order to entice people to register through them, knowing that a portion of them will sign up for complementary services. For the registrars that do not offer complementary services, it becomes a bulk business in order to survive solely on the very small margins of domain name registration.

The overlap between registrars and ISPs means they share similar incentives. It also means that the size of their operations is such that staffing an abuse desk and other security-related positions is seen as a normal cost of doing business. The different parts of the business often share a centralised abuse desk. Furthermore, they need such capabilities for other reasons than just security, most notably to deal with complaints regarding copyright infringement – our interviewees reported that the latter made up a large portion of the incoming complaints.

Of course, there are also smaller registrars, with or without complimentary services, who lack staff to deal with abuse – again, similar to the situation with ISPs. Some of these smaller registrars leave it to the hosting provider to deal with all content-related complaints. Because of the overlap between registrars and ISPs, we refer back to the section on ISPs to get a sense of the incentives that both have in common. We only briefly summarise them here, complementing them with more specific findings for registrars.

Costs of customer support and abuse management

As with any business in a competitive market, registrars have an incentive to reduce operating costs. This includes customer support and abuse management. The number of complaints was reported to have risen substantially in recent years, though part of this growth coincided with growth of the customer base. At the same time, the response process has become partially automated and thereby more efficient. To illustrate: one interviewee reported getting 1 200-1 500 incoming complaints per day for a customer base of several million. Only a minor part of the overall incoming notifications relate to malware. The bulk consisted of complaints about spam or copyright violations.

While the company in question offered complimentary services, most of the incoming complaints were about domain names that were registered through them, but hosted elsewhere. They were contacted because their terms of service did not allow the domain to be used for any kind of abuse – and they have a reputation for enforcing these terms. On the whole, the interviewee estimated that they suspend around 20 domain names per day for abuse-related reasons. Only a few per week were specifically for malware. One explanation offered for this relatively modest number was that for end users who were infected by malware, it is often difficult to tie that infection to visiting a specific hosted domain.

With the core process of registrars being relatively low cost, involvement in notice and takedown procedures can drive up operating costs. Dealing with abuse notifications requires staff. The cost of collaboration therefore provides an incentive that, all things being equal, works against security. This is reinforced by the need to investigate the notification, to understand whether the domain name is indeed associated with malicious activity. Given the dynamic and increasingly sophisticated strategies of phishing gangs, this can be more difficult than it may seem at first glance. Even for the experienced staff at larger registrars, investigating a notification and request to suspend a domain name for malware-related issues can take several hours. Phishing sites are less difficult to investigate and can typically be dealt with within an hour.

The incentives for criminals are to register with registrars who are slow to respond to abuse. The longer the domain name stays active, the more successful their attack can be. This means that not all registrars are equally affected. Those that are swift to suspend, remove or redirect a domain name typically incentivise criminals to look for easier targets. Given the enormous variety of registrars, both for generic and country-code top-level domains, an easier target is usually not hard to find. These registrars do experience consequences for their lack of responsiveness, similarly to the consequences that ISPs suffer. In that sense, the costs of customer support and abuse management work as an incentive to improve security.

Our interviewees explained that it was their experience that if they dealt proactively with abuse, then criminals would avoid them or move elsewhere, which reduced the amount of complaints coming in, as well as associated costs such as blacklisting. The amount of abuse had gone down relative to the growth in their customer base.

Costs of blacklisting

The registrars offering hosting and e-mail services are subject to the issue of blacklisting along the same lines as the ISPs. Blacklist operators also watch registrars and their responsiveness to abuse complaints. In extreme cases, blacklists may be directed at the registrar itself. A case in point is the recent row between the blacklist operator Spamhaus and the Austrian registry/registrar Nic.at. Spamhaus had requested Nic.at to remove several domain names it said were associated with phishing by the "rock phish" gang. Nic.at did not comply with these requests, citing legal constraints. They argued that they could not legally remove the sites, unless Spamhaus provided them with clear proof that the domain names had been registered using false information (Sokolov, 2007).

The conflict escalated when Spamhaus added the outbound mailserver of Nic.at to one of its blacklists – listing them as "spam support" – so that the registrar's e-mail was no longer accepted by the multitude of servers using this popular blacklist. About ten days later they changed the listing of

Nic.at to a symbolic listing – no longer actually blocking the IP addresses, but keeping them listed as "spam support." Several of the offending domains have been removed, but Nic.at denies that they complied with the request and assumes that the hosting providers took action (ORF, 2007; Spamhaus, 2007).

Costs of brand damage and reputation effects

There also appear to be reputation effects, which provide security-enhancing incentives. As mentioned earlier, there are several cases of registrars who were popular among phishers and who at first did not respond to requests to suspend domains. Then they apparently went through a learning process and started to remove domain names quickly in response to requests (Clayton, 2007). It is unclear what precisely prompted this learning process, but their behaviour suggests that the registrar does not want to be associated with the malicious activity.

Another case is the ccTLD of Tokelau, an island with 1 300 inhabitants and a territory of New Zealand. The registrar for the .tk domain is a Dutch-American company, which hands out most domain names for free, making money from showing advertisements on the registered domains. After McAfee announced that over 10% of the .tk domains were suspected of malicious activity, the registrar introduced new measures, which included frequent scanning of the domains for malware (Dot-TK, 2007).

Benefits of maintaining reciprocity

For registrars, maintaining reciprocity is as important as it is for ISPs. We heard numerous examples of registrars with hosting and e-mail services preventing instances of blacklisting through informal contacts with blacklist operators as Spamhaus as well as major e-mail and network providers. One interviewee mentioned that one direct benefit of being responsive to abuse complaints is that it typically keeps sites with security problems off blacklists – or at least ensures a proportionate response from blacklists, such as listing the specific machine associated with the abuse, rather than listing a wider range or subnet in which the offending machine resides. A security expert at an ISP claimed that his organisation sponsored Spamhaus, which effectively gave them a free pass in terms of being blacklisted.

An interesting new example of reciprocity stems from the size of the customer base. According to one interviewee, the larger the hosting provider, the less likely it is to get blacklisted by the large e-mail providers such as AOL, since it affects AOL's customers when they cannot reach websites or mailboxes at the hosting provider. This effect is far less likely with smaller connectivity, hosting and e-mail providers.

Domain registrar disincentives

Legal risks and constraints

As with the ISPs, a number of legal ambiguities surfaced which in some cases translated into disincentives for security. Some interviewees argued they had to be careful with monitoring the hosted sites on their network. One interviewee said:

"The legal liabilities kick in as soon as you have knowledge or should have knowledge that something took place on your network. If you are proactively monitoring all the content of your hosting customers but for whatever reason something is missed, while there is an expectation that you should have caught it, then you could potentially be held liable for that content. So the monitoring that we do is somewhat limited in scope and only applies to areas where there is some sort of a safe harbor legal provision."

Then there are potential liabilities around suspending or removing domain names, as it involves a contractual relation between registrar and registrant. Even if the terms of service of the registrar preclude the domain name being used in relation to spam or other forms of abuse, that still requires the registrar to investigate and build a case showing that those terms have been breached. That can be costly.

Several interviewees in the security community pointed out that security professionals often use a short cut: rather than asking the registrar to adequately investigate and decide on an abuse complaint, they point out that the registrants WHOIS information is false. As one interviewee explained: "For those registrars that are not willing to assume the risk of the liabilities, the WHOIS accuracy policy is a comfortable refuge." Referring back to the case of Spamhaus vs. Nic.at, the request of Spamhaus was indeed to suspend the phishing domains on the grounds that their WHOIS information was false. The response of Nic.at was that they were contractually bound and unable to remove the domain names unless Spamhaus could provide legally meaningful evidence that the WHOIS information was indeed false.

There is also the risk of collateral damage from removing domain names. It could be that the domain name is indeed used for phishing, but that not all activity associated with it is criminal or that the actual owner is unaware of what is going on. The fact that the registrar acted in good faith upon the request of others would in all likelihood not shield it from liability, unless the request had a legal basis, such as a formal request from a law enforcement agency – ignoring for the moment the obvious complications that would arise should different national jurisdictions be involved. Early 2007, registrar GoDaddy.com received a lot of criticism after it removed the

DNS record for the security website SecLists.org at the request of MySpace.com, after the security site published a list of 56 000 MySpace usernames and passwords that had been circulating on the Internet (Utter, 2007).

Even if the domain is actually owned by criminals, that does not mean the registrar is shielded from repercussions. In the past, there have been cases of spammers successfully suing their ISPs for shutting them down, just as they have sued blacklist operators such as Spamhaus – a case which was initially won by the spammer, although that did not affect Spamhaus directly because it is located outside the courts' jurisdiction. In short, the risk of liability drives up the costs of compliance with abuse notifications, especially in combination with more complicated and difficult to diagnose attack strategies, which work against security.

Not everyone agreed that these liabilities form a significant risk. "In a lot of cases the risk of incurring liability vis-à-vis a spammer or malware author is very minimal," said one interviewee. "I believe most registrars operate on that premise. Certainly, I have heard the excuse of liability used by some registrars and I feel that it should not be used to absolve yourself from your responsibility to your customers and your community... The real risk is the cost of defending yourself against court cases. Even in the most ludicrous cases there is some exposure and you need to take those exposures into account into your business model."

Security and customer acquisition

Interviewees expressed mixed views about the relationship between security costs and acquiring and retaining customers. The dominant view appeared to be that proactively fighting abuse actually helped to acquire and retain customers, as it helps build their brand as trustworthy and secure. In addition, active abuse management helped the registrars to mitigate risks of blacklisting, also for customers that were not directly involved in the abuse issue. Non-responsive registrars and hosting providers might experience more severe forms of blacklisting which are correlated with substantial collateral damage within their customer base.

The other side of that story is that proactive abuse management often implies swift action, which might be perceived as hasty or unjustified by the customers involved in the abuse issue. The latter might see themselves as victims of the abuse management, as well as of the actual abuse. In general, the organisations we spoke to take great pains to resolve abuse situations without alienating the customers – with the obvious exception of those customers who are in some manner complicit.

Summary of incentives for domain registrars

Registrars face a mixed incentive structure for security that varies across the different business models. To the degree that registrars operate as ISPs – and many do, as they tie in registration services with hosting e-mail and other complementary services – they face a similar incentive structure. There is some evidence that suggests that registrars are indeed responsive to outside pressure and that improved security provides benefits (*e.g.* Clayton, 2007).

A security officer at an international bank told us he was not worried about the fast-flux networks for phishing, because in his experience registrars were quite responsive in addressing the attacks at the level of the domain name. That still implies, however, that in the absence of outside pressure, the incentives for security are not strong. In light of the large number of registrars currently in operation, this suggests a long learning process, even if we assume that registrars that have improved security will not fall back into complacency.

As was discussed earlier, the abuse complaints that ISPs receive cover only a fraction of the actual amount of abuse on their network. The interviewees confirmed that this is similar for the domain names or hosting services that fall under their purview. “For every abuse situation we are notified about, there are probably several more going on that we do not get notified about,” said one interviewee. In practice, this means that while many registrars may have incentives to improve security, their efforts do not reflect the full extent of the security problems associated with their services and their customers. In other words, there are externalities arising from these services for other market players in the value net.

End users

End users are arguably the most heterogeneous set of market actors, ranging from average home users to SMEs to public institutions to global corporations. Rather than trying to differentiate all of these actors, we briefly discuss two extreme categories – home users and large organisations, public and private – and discuss in general terms the incentive structures under which they operate.

Home users

The rise of botnets has turned the problematic security practices of home users into a collective problem. Home user security has never been strong, but until a few years ago the consequences of this behaviour mainly affected the users themselves. That incentive structure has changed dramatically. By masking its presence to the end user, malware can turn end user machines into attack platforms to be used against many other players in the information network.

The lack of home-user action against the infection of their machines is a combination of:

1. Incomplete information – not knowing that they are infected or unable to evaluate the relevant security risks and defense strategies; and
2. Shortage of incentives: home-users do not have to bear the costs of their decisions on other market participants.

Incomplete information is important, because it further weakens the already misaligned incentive structure. While it is true an infected machine is often mobilised for use against other actors than the machine's owner, it is certainly also true that a significant portion of malware poses a direct threat to the owner – for example, keyloggers that capture access codes to financial accounts, 'ransomware' that renders user files inaccessible until a ransom is paid to the criminal, or Trojans that enable man-in-the-middle attacks during secured online banking sessions.

In principle, these risks could provide a strong incentive for home users to secure their machines. But their lack of understanding of such risks or how to defend against them renders the incentive to act on them rather weak, if not inexistent. The interviewees at ISPs told us that when they contact users whose machines have been compromised, the response is generally quite positive. Their customers had no idea what was going on. Once it is explained, they are often co-operative.

In the abstract, however, the information about risks is not getting through. A security officer at a smaller ISP explained it this way: "At any given point in time, we have 600-800 customers who have a malware, abuse or security problem with their machine. You do not see those numbers in the paper, because a journalist does not think this is a problem; 600 out of 400 000 customers. This is also why end users do not think it is a problem, because the chances of being hit seem so low."

The cost of increasing security provides a further disincentive. The willingness to pay for security services seems low. As quoted earlier, one interviewee summarised their experience as an ISP with offering security software as follows: "If people have the option to pay for it or not to pay for it, they do not." But even after the licence was included in the subscription rate, there was still a large group of people not installing the software package.

A similar phenomenon was related to us by the head of Internet security at a large ISP: they too offered an AV solution as part of the subscription. Even the people who did install it often did not keep it up to date. He blamed it on poorly designed software. That sentiment was shared by a representative of a consumer organisation: "We see that the products consumers get for establishing some degree of security for their PC do not work properly, and they are too complicated to manage. Consumers cannot manage their own security given the tools they are provided with." When asked whether in their view consumers would be willing to pay for better security, the interviewee responded:

"In general terms, they do and they do not. They just expect it to be the default setting. Most products are secure. When you buy a car, it's got seat belts, air bags, brakes. Those things are included in the product. Consumers feel that charging extra for that is a bit ridiculous."

In line with these views, a survey by a consumer organisation found that the majority of their members felt that Internet security was a shared responsibility: the consumers themselves are responsible for their online behaviour, but the technical aspects of security are the responsibility of others, most notably their PC retailers, ISPs, software vendors and the government (Consumentenbond, 2006).

It is difficult to disentangle incentives from incomplete information, but their combined effect is to undermine the willingness, as well as the ability to act. Often this situation is described with a sense of inevitability, as if the home user is a static entity with no learning curve. Surveys suggest that image is incorrect.

Home users are adapting their behaviour, but it is unclear how these changes add up, how to connect the disparate, if not contradictory, pieces of information from the plethora of surveys out there. Even if we ignore the discrepancies between the numbers, it is hard to characterise the current situation. Surveys tell us a large number of people are worried about identity theft, privacy, security, online predators, fraud and other problems. In fact, a significant portion of people are turning away from the Internet altogether (GetSafeOnline, 2006). At the same time, adoption of security measures such as firewalls and AV software is increasing, slowly but surely (Fox, 2007).

Incentive structure for home users

The key question regarding the incentive structure is: how, if at all, are home users confronted with the costs generated by their security trade-offs? Of course, technically, they are confronted with them all the time. The bulk of the spam messages that everyone receives is sent through botnets, to name but one consequence. But the causality between individual behaviour and such aggregate effects is too abstract and complicated to have a feedback effect.

Feedback typically stems from actual security problems that people experience – the victims of fraud, identity theft or, less dramatic, degraded functionality of their machines. According to a 2007 survey by *Consumer Reports*, 1 in 5 people experience a major virus problem, 1 in 11 experience a major spyware problem and 1 in 81 actually lost money from an account (Consumers Union, 2007). Assuming these numbers are correct, that would mean somewhere between 20-30% of all home users have directly experienced the consequences of their security decisions. Potentially, this could be a powerful feedback loop, but the unanswered questions are:

How do people understand these incidents? Do they relate them back to their own decisions? Do they have adequate tools and capabilities to act on their understanding, assuming such tools exist for end users? (The existing security software suites are increasingly ineffective in detecting malware.)

The most direct mechanism (which is currently internalising some of the externalities generated by end users) is the ISP practice of isolating infected users until they resolve the security problem. It would appear that this solution works for relatively modest numbers of infected machines, but, as computer experts say, it does not scale to the actual number of infections.

It is not just ISPs that bear the externalities generated by home users. Most online businesses are confronted with botnets and related security threats, and they have to provision their services accordingly – whether they be an e-commerce company buying DDoS mitigations services from its ISP, or an online bank that has to design its services under the – all too valid – assumption that the customer's machine is compromised. Few of these market parties are in a position to mitigate these risks by influencing the security trade-offs of home users. Thus, defending against these security threats is perceived as the cost of doing business.

Large end users

The situation for large organisations – public and private – is rather different. On average, they have dedicated IT staff and are in a much better position to understand the security risks they face, take precautionary measures, as well as build incident response capabilities. Notwithstanding these advantages, research often reports that both public and private organisations underestimate the risks they face or under-invest with regard to security. Some of our interviewees reported compromised machines in their networks, which they perceived as more or less inevitable. They indicated that their networks were by necessity rather open to accommodate contractors, or the flexible use of services throughout the organisation. One interviewee said his network was like a fortress that kept intruders out, but once someone had gained a foothold inside, there were many opportunities for malicious activity.

While interviewees reported instances of malware on their network, they claimed this malware to be generic and not targeting their organisation specifically. It is unclear how valid this claim is. The way they found out about these compromised machines – *e.g.* through notification by security service providers which were not under contract with them, or during the activities of support desk staff repairing malfunctioning machines – suggests that their risk perception of malware is not based on any formal type of analysis of their own services and networks.

There are many known cases of companies who have suffered embarrassing security breaches – and there are undoubtedly many more unknown ones. That being said, it is rather difficult to determine the appropriate level of investment in light of these threats. While more formal analytic instruments have been developed in recent years to support these decisions, their application requires the input of values and probabilities that are very hard to estimate with any degree of reliability. According to the 2007 CSI Computer Crime and Security Survey, less than half of all organisations use instruments such as ROSI, IRR and NPV (CSI, 2007). Insurance providers have very little actuarial data to base policies on.

While the security practices of large end users undoubtedly leave much room for improvement, it is also important to realise this: many of the claims that businesses underestimate risks and under-invest in security stem from research sponsored or carried out by security providers, whose incentive is to overestimate the problem.

Contrast these claims with the findings from the CSI Survey, which published decreasing loss estimates from respondents for five years in a row – a trend only reversed last year (CSI, 2007). The peak loss was experienced in 2001, with more than USD 3.1 million per reporting organisation. Since then, most likely due to increased awareness and more systematic investment in computer security, the damages have declined to a low of USD 168 000 per reporting organisation in 2006. In 2007, the downward trend reversed as damages per reporting organisation doubled to USD 345 000. It is difficult to assess whether this represents a one-time deviation or a sustained reversal of the downward trend. Most likely, it reflects the technology race between the provision of cybersecurity and ever-more sophisticated and virulent criminal attack techniques. It is also important to note that direct losses are no measure of the complete financial impact felt by society.

Some of the trade-offs

Organisations face all kinds of trade-offs regarding their information security decisions, including malware. Take the issue of patching. We heard estimates that patching mission-critical software systems can cost millions. For that reason, some companies did not patch immediately after release of a vulnerability patch, but waited for months and then applied several patches simultaneously.

There were even examples of organisations that consciously never patched, estimating the risk of disruption to be higher than that of security breaches. In the financial sector, security measures often face a trade-off against availability of the systems and their performance. In a world where the ability to process information in milliseconds affects the bottom line, measures that improve security but slow down transactions are not an obvious choice. A similar trade-off exists between security and availability – that is, the uninterrupted uptime of systems. All of these trade-offs involve difficult assessments of costs and benefits, often in the face of uncertainty and missing information.

What are the externalities?

Even if it is true that large organisations might not fully understand the costs and benefits of information security, the more relevant issue is whether this situation causes market externalities. In the absence of externalities, it is within their purview to pursue whatever security strategy they deem appropriate and bear the consequences of those decisions. In most generic terms, the answer is Yes, there are serious externalities.

Examples of externalities are hospital records that are compromised, financial records of millions of citizens that are "lost," and a job website that has been compromised, allowing the personal information of over a million users to be stolen (Wilson, 2007). The list goes on and on. If we expand the set of security breaches to also include attacks that did not directly involve malware, the enormous potential for externalities becomes clear. As malware develops and proliferates, it seems reasonable to assume that over time it will be implicated in a wider variety of security breaches than those we have already observed.

Brand damage and other incentives

What are the incentives for these organisations to prevent these externalities? There is brand damage. Organisations that have been breached have a strong incentive not to disclose this information. However, many US states have adopted legislation that requires organisations to publicly disclose security breaches. The legislation includes no penalties, but still provides strong incentives because of the prospects of public embarrassment and loss of share value.

Campbell *et al.* (2003) reported that, on average, breaches of confidentiality had a significant negative impact, causing an average decline of market value of about 5 %. A study by Cavusoglu *et al.* (2004) also reported that announcing an Internet security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost an average of 2.1 % of their stock market value within 2 days of the announcement — an average loss in market capitalisation of USD 1.65 billion per breach. While these effects are significant, some experts argue that these are temporary and that, over time, the notifications will have less and less impact, as the number of notifications increases and they lose their news value.

Data breach notification legislation enables other parties to hold the responsible organisation liable for any damages they have suffered. This may be done by individuals affected, but perhaps more realistically by other companies that have more resources to pursue such a course of action. In the case of the security breach at Choicepoint, this led to USD 10 million in civil penalties for security breaches and USD 5 million in redress to customers (FTC, 2006).

More recently we have seen what will undoubtedly be a landmark case, the security breach at the US retailer T.J. Maxx in December 2006. Many parties are suing the retailer for damages following this breach. Among them are the banks that had to reimburse their customers for fraudulent transactions stemming from credit card information that was stolen at T.J. Maxx. Recently, the retailer has reported that the breach has already cost it USD 135 million – and the case is far from over. A security company estimated that in the end, it would cost the company around USD 4.5 billion (Gaudin, 2007).

US security breach notification laws provide incentives that internalise some of the externalities caused by the security decisions of large organisations. Other US legislation also has implications for liability, most notably Sarbanes-Oxley, the Health Insurance Portability and Accountability Act and the Gramm Leach Bliley Act. While there is disagreement over the effectiveness of these laws, issues of liability and compliance have shown to be drivers for increased security efforts (*e.g.* Ernst & Young, 2007; Lords, 2007, p. 152).

Other countries have different regulatory regimes in place. However, there are parallels. Data protection laws could potentially have similar effects. So far, however, these effects, if they are indeed occurring, are certainly less visible. Predictably, the debate is shifting towards the issue of whether to connect sanctions to these liabilities. The UK Information Commissioner recently called for criminal sanctions "for those who knowingly and recklessly flout data protection principles" (Shifrin, 2007).

Summary of end-user incentives

End users have been the focus of considerable debate regarding Internet security. As has been reported before, many externalities emanate from end users' security decisions – or non-decisions. Interestingly, both for home users and large users, there exist incentives that are potentially very strong – that is, the risk of significant damage to themselves resulting directly from their decisions.

The problem is, however, that their risk perceptions are often not consistent with the technological realities in which they operate. To the degree that end users do appreciate the risks they face, there are significant problems when they attempt to act on that information. For home users, security tools are often too complex and partially effective at best. For large public and private organisations, the situation is remarkably similar. While they often have more expertise available, the security challenges are also substantially more complex in light of the complicated array of systems, services and the organisational arrangements around them.

As a result, end users generate externalities, the costs of which are sometimes passed back to them. But in many cases, the costs are passed on, and internalised by, other market players, which consider them part of the cost of doing business in the information industry, or the costs are absorbed by society at large.

Annex 5.A1. List of Interviewees

In 2007, 41 in-depth interviews were conducted with 57 professionals from organisations participating in networked computer environments that are confronted with malware. Below is a full list of those responding.

In each instance, the following questions were asked: how the organisation was confronted with malware; what its responses were; what trade-offs were associated with these responses; and how the organisation was affected by the actions of other market participants.

For details on the research design and its scope and limitations, please see Annex B. Research Design for Economics of Malware.

Alhadeff, Joseph	Oracle [US]
Barbir, Suzana	Telstra BigPond [AUS]
Barrett, Michael	PayPal [US]
Beale, Jeremy	Confederation of British Industry [UK]
Behlendorf, Brian	Mozilla Foundation [US]
Boudewijns, Arno	St. Elisabeth hospital [NL]
Butler, Ben	Go Daddy [US]
Candel, Hans	St. Elisabeth hospital [NL]
Davidson, Mary Ann	Oracle [US]
Dupon, Koen	Consumentenbond (Consumers Union) [NL]
Edelstein, Eric	France Telecom / Orange [FR]
Florijn, Gert	ABN AMRO [NL]
Gorbutt, John	StreamShield [UK]
Hafkamp, Wim	FI-ISAC / Rabobank [NL]
Halfweeg, Jaap	KPN [NL]
Hania, Simon	XS4All [NL]
Hiskey, Steve	Microsoft [US]
Kelly, John	Comcast [US]
Keogh, Steve	Telstra BigPond [AUS]
Lappas, Paul	ServePath [US]
Leguit, Douwe	GOVCERT [NL]
Lord, Peter	Oracle [US]
McIntyre, Scott	XS4All [NL]
Melein, Johan	SIDN (Foundation for Internet Domain Registration) [NL]
Mitchell, Alan	IBM [US]
Molenaar, Danyel	OPTA [NL]
Morrow, Chris	Verizon Business [US]
O'Donnell, Adam	Cloudmark [US]
Oppenheimer, Jay	Comcast [US]

Pinkney, Graeme	Symantec [UK]
Piscitello, Dave	Fellow to the ICANN SSAC [US]
Provos, Niels	Google [US]
Quaresima, Richard	Federal Trade Commission [US]
Rader, Ross	Tucows [CA]
Ramsauer, Thomas	BSI (Federal Office for Information Security) [DE]
Rand, Dave	TrendMicro [JP]
Reed, Chris	Queen Mary University of London [UK]
Reijers, Roeland	GOVCERT [NL]
Renten, Jerry	KPN [NL]
Salsburg, Daniel	Federal Trade Commission [US]
Samson, Michael	NVB (Dutch Association of Banks) [NL]
Schindler, Werner	BSI (Federal Office for Information Security) [DE]
Schoen, Kevin	ACDNet [US]
Schuurman, Jacques	Surfnet CERT [NL]
Silversin, Louis	Federal Trade Commission [US]
Slim, Arjen	Shell International [NL]
Truman, Nick	BT [UK]
Van Daalen, Frits	ABN AMRO [NL]
Van der Heide, Martijn	KPN-CERT [NL]
Veysset, Franck	France Telecom / Orange [FR]
Walsh, Anthony	Shell International [NL]
Ward, Jeremy	Symantec [UK]
Wesson, Rick	Support Intelligence / Alice's registry [US]
Whitaker, Colin	APACS [UK]
Wiggins, Rich	Michigan State University [US]
Williams, Jeff	Microsoft [US]
Woodcock, Bill	Packet Clearing House [US]

Chapter 6. The Market Consequences of Cybersecurity: Defining Externalities and Ways to Address Them

The preceding chapter reported on the efforts and incentives of a variety of Internet market participants. It indicated a number of market-based incentive mechanisms that contribute to enhanced security but also other instances in which decentralised actions may lead to sub-optimal outcomes. A pressing question is: Are participants in the information and communication markets responding adequately to malware, or are improvements possible? Pointing to a variety of reports that show increases in malicious attack trends, one might conclude that markets are not responding adequately. Our analysis revealed a more nuanced picture.

Three major categories of externalities

Real-world markets rarely meet the preconditions of standard economic theory. For example, decision makers rarely have complete information, they operate under conditions of bounded rationality, and they behave opportunistically. For these reasons, individual decisions rarely are as ideal as described by abstract models. Rather, real-world decisions are a process of "muddling through" second and third-best solutions, especially in an environment of rapid technological change. Whether a decision was good or bad is often revealed only after-the-fact.

Assessing the direct and indirect economic cost of malware in real-world conditions is hence an important aspect of designing countermeasures. Since the provision of security entails cost, tolerating a certain level of insecurity is economically rational. Therefore, the level of security realised depends on the costs and benefits of security to individual actors, and on potential collective measures to enhance security. Two key questions are:

1. Are market players taking the full range of costs into account when making security decisions?

2. If costs are externalised (passed on) to other market players or society at large, how serious are they in relation to the internalised (absorbed) costs?

While keeping in mind the scope and limitations of our study, we can offer a number of tentative conclusions with regard to these questions. Across the information market's value net, three relevant situations emerge for key market participants:

Category 1: No externalities; market participants absorb all the costs of their security decisions.

The decision-making unit, be it an individual user or an organisation, correctly assesses security risks, bears all the costs of protecting against security threats (including those associated with these risks) and adopts appropriate countermeasures. The private and societal costs and benefits of security decisions are aligned. There may still be significant damage caused by malware, but this damage is borne by the market player itself. This situation would be economically efficient, but due to the high degree of interdependency in the Internet, it is rare.

That does not mean these situations are non-existent. In principle, end users – be they large organisations or skilled home users – who take adequate security measures and successfully prevent their machines from being compromised generate no externalities for the rest of the market– though some experts might argue that under certain conditions such behaviour creates positive externalities that are not taken into account and thus lead to an sub-optimal level of private investment (Kunreuther and Heal, 2003).

Several interviewees in our field survey claimed that in recent years, they have not had any malware infection within their organisation's network. We were not in a position to check the validity of these claims, but it is not unreasonable to assume that there are cases where malware is successfully fought off, or where the effects of malware infections are, by and large, limited to the owner of the infected system.

Category 2: Externalities are created, but they are borne by agents that can manage them.

This concerns instances in which an individual unit assesses the security risks based on the available information, but due to the existence of (positive or negative) externalities, the resulting decision deviates from the societal optimum. Such deviations may be based on lack of incentives to take costs imposed on others into account. But they can also result from a lack of skills to cope with security risks, or financial constraints faced by an individual or organisation.

As long as somebody else in the market internalises these costs, and this agent is in a position to influence these costs – *i.e.* it can influence the security trade-offs of the agents generating the externality – then the security level achieved by the whole value net may deviate less from a social optimum than without such internalisation. This scenario depicts a relatively frequent case and numerous examples were found that confirm externalities were being internalised by other market players.

The ISP example

ISPs have started to manage the security problems generated by their customers – *e.g.* by quarantining the infected machines of end users. As such, they absorb some of the costs generated by the sub-optimally low investment in security by their own customers. ISPs internalise these costs, because not doing would lead to even higher costs being imposed on them, as they may experience blacklisting, rising customer support and abuse management costs and possible reputation effects.

The key point here is that ISPs are internalising these costs, but that they are also in a position to influence the behaviour of the agents generating the externality – *i.e.* their own customers. For example, if they increasingly suffer blacklisting because of spam from infected end-user machines flooding their network, one of the options they have is to block port 25. That would significantly reduce the degree of blacklisting and the costs associated with it. Of course, such a measure also has costs and implies a trade-off with other objectives, such as the kind of services the ISP can offer its customers. They may opt against blocking port 25 for a variety of reasons. That does not mean, however, that the externality is not a given, but that they can actually influence its magnitude. This is different from, say, an e-commerce company who has to buy DDoS (mitigation services from its ISP because of botnet attacks. That company cannot do anything about botnets, and thus the costs to defend itself against them is simply considered a cost of doing business.

ISPs only internalise a part – some experts would say a minor part – of the externalities caused by their customers. For example, while ISPs are increasingly responsive to incoming notifications of abuse on their network, these notifications typically concern only a small fraction of the total number of infected customer machines. The externalities generated by the remaining machines still affect the wider value net and society at large.

The case of online financial services

Another instance of this type of externality was found in the case of financial services. The incentives of financial service providers are such that in many cases they compensate customers for the damage they suffer from online fraud. In that sense, they internalise the consequences of sub-optimal security investments by their customers, as well as the software vendors whose software is exploited to execute the attacks. Many financial service providers claim they compensate all malware-related losses. If that claim is accurate, then the security level achieved by the whole value net may not be too far from the optimum. The financial institutions bear the externalities, but they are also in a position to manage the risk through security measures they impose on online financial services.

However, there are three important considerations to take into account:

1. It is unclear what the reality is of customer compensation under the current liability regime. Some researchers suggest that many claims are in fact refused and that not all of the victim's damage is compensated, only the direct loss (Schneier, 2005; Anderson, 2007).
2. There is debate within the industry to change the banking codes so as to assign more liability to the customer. New Zealand has already adopted a revised code to this effect. That would change the incentives which might push the level and focus of security investments of the financial institutions away from the social optimum (Anderson, 2007).
3. Even if customer damage is compensated, one could argue that there are still externalities in the sense that important social efficiencies could be gained if people had higher trust in these services and could adopt them more quickly. These benefits would outweigh the additional security investments that would be needed. While the magnitude of these externalities is unknown, the financial service providers are the ones who stand to gain most from maintaining high trust in the e-channel. In other words, this is a problem of incomplete information, rather than of misaligned incentives.

Category 3: Externalities are borne fully by other market participants or by society at large.

An individual unit may correctly assess the security risks given its perceived incentives, but due to the existence of externalities, this decision deviates from the social optimum. Alternatively, an individual unit may not fully understand the externalities it generates for other actors.

Unlike in Category 2, no other agents in the information and communication value net absorb the cost. Or, if they do, they are not in a position to influence these costs – *i.e.* influence the security trade-offs of the agents generating the externality. Hence, costs are generated for the whole sector and society at large. These are the costs of illegal activity or crime associated with malware, the costs of restitution of crime victims, the cost of law enforcement associated with these activities, and so forth.

Furthermore, the externalities may take on the more indirect form of slower growth of e-commerce and other activities. Slower growth may entail a significant opportunity cost for society at large, if the delayed activities would have contributed to economic efficiency gains and accelerated growth. A comprehensive assessment of these additional costs will demand a concerted effort but will be necessary to determine the optimal level of action to fight malware.

The case of lax security by end users

The most poignant cases in this category are the externalities caused by the lax security practices of end users. Some of these externalities are internalised by other market players, but many are borne by the sector as a whole and society at large. These externalities are typically explained by the absence of incentives for end users to secure their machines.

It would be more precise, however, to argue that the end users do not *perceive* any incentives to secure their machines. While malware writers have purposefully chosen to minimise their impact on the infected host and to direct their attacks at other targets, there is also a plethora of malware which does in fact attack the infected host – most notably to scour any personal information that can be used for financial gain. In that sense, end users do have a strong incentive to secure their machines. Unsecured machines cannot differentiate between malware that does, or does not, affect the owner of the machine. If the machine is not sufficiently secured, then one has to assume that all forms of malware can be present. The fact that this incentive is not perceived by the end user is an issue of incomplete information rather than a lack of incentives.

Distributional and efficiency effects

To sum up: Yes, there are significant externalities that arise due to the security decisions of key Internet market participants. But not all of these externalities create sub-optimal outcomes. We need to distinguish between the distributional and efficiency effects of externalities.

When externalities are borne by agents who can manage them (Category 2), they are usually *distributional* in nature. That is, there is a mere shifting of the costs (and benefits) between the actors involved. In the case of ISPs, end-users shift to ISPs most of the cost of secure online connections, but the ISPs are in a position to manage those costs via various actions.

In contrast, overall *efficiency* externalities materialise if the cost of achieving a given level of information security can be reduced for all the participants in the sector. This differentiation is also important in the evaluation of alternative strategies for coping with problems of malware. Some measures, such as a modification of liability rules, may predominantly shift the burden of combating malware from one set of actors to another. In these cases, it will be critical that the resulting attribution of costs and benefits is better aligned with the true cost structure of the value net. Only in this case will efficiency be improved.

Due to the high degree of interrelatedness, nearly all the three observable categories of externalities discussed in the previous section are afflicted with both types of effects. In general terms, however, we would expect that Category 2 externalities have mainly distributional effects, while Category 3 will have distributional, as well as efficiency effects. From a societal perspective, the latter is obviously a more damaging form of market failure. In the case of Category 2, efficiency effects are not a given – *i.e.* these cases need not imply a suboptimal level of security for the value net as a whole. Banks, for example, internalise the security-related externalities generated by end users and others. This does not need to have efficiency effects, because the banks can mitigate the risks of end users and thus can trade-off the damage against the costs of mitigation. In fact, it may have a positive effect on efficiency, if the banks can manage the risks better than the end users themselves.

It is important to keep in mind that many malware-related externalities and costs have their origin in illegal and criminal behaviour: illegitimate market players imposing costs on others. In that sense, the oft-cited analogy to externalities in environmental pollution does not hold. In the example of pollution, there is a market player that benefits from the production process causing that pollution. In that case, the guiding principle of standard economic theory is to internalise the costs of pollution so that the agent adjusts the level of production to be more in line with the social optimum.

In the case of malware, the agent who profits from the malware is outside the security market. Malware increases the costs of security for all, and it causes additional direct and indirect costs for damages or foregone activities. As such, it stands to reason that parts of these externalities should be internalised by measures taken by the sector as a whole or society at large, and not by individual stakeholders. This is currently happening, for example, in the area of law enforcement, but it is not clear whether it is at an optimal level.

Survey results on the costs of malware

Although the malware-related costs of security measures are considered proprietary, estimates provided by players range from 6-10% of the investment in ICT. No clear estimates of the effects of malware on operating expenses were available, although we did find that most organisations did experience such effects. There was evidence throughout the empirical research of concern that such effects are important, although no specific indication as to their magnitude is available. The concern with this broader societal externality seems to motivate several players, especially in industries sensitive to reputation issues, to increase investment in security and to add a "safety margin" when deciding on levels of security.[1]

The information collected in this research project from actors across the information and communication value net allows the conclusion that the direct private and public costs of prevention are substantial. With few exceptions, many actors have had to increase their security-related investments as a response to the higher benefits of security associated with the types of transactions conducted via the Internet and the increasing number of attacks.

However, each actor typically only acts based on the perceived incentives. In literally all cases, there were important costs and benefits that accrued at other stages of the value net and were hence outside the decision-making process. Our research showed that due to feedback effects inherent in market co-ordination, the magnitude of these externalities is probably smaller than hitherto assumed. On the other hand many of these externalities remain uncorrected leaving the system overall in a sub-optimal state.

The collective costs of fighting malware, ranging from the costs of maintaining public-private organisations such as CERTs or CSIRTs, to the cost of public education campaigns and law enforcement, add to these private costs. Finally, all actors pointed to the potentially high indirect costs of malware in the form of slower migration to efficiency-enhancing forms of electronic transactions. Taken together, the direct and indirect costs of malware could be a double-digit percentage figure of the revenues of players in the information and communication value net.

Key findings

Although the research in this report was not designed to develop specific policy recommendations, some general concluding remarks are nonetheless offered.[2] With regard to the interrelationships within the information and communications-related activities, it seems that the incentives of many of the commercial stakeholders are reasonably aligned with minimizing the effects of externalities on the sector as a whole.

The incentives typically have the correct directionality. But in a variety of cases they are too weak to prevent significant externalities. It is important to note, however, that all market players we studied experience at least some consequences of their security trade-offs on others. In other words, there was a feedback loop that brought some of the costs imposed on others back to the agent that caused them.

We found many such feedback loops, which mitigate the externalities arising from less-than-optimal security decisions. All market players we studied experience such feedback, which potentially brings their security trade-offs closer in line with that of society in general. We also noted, however, that in many cases these feedback loops are too weak or too localised to effectively change the security trade-offs that caused the externalities to emerge in the first place.

In terms of policy development, a key strategy would be to strengthen the existing feedback loops and create new ones where possible. That would also keep public policy out of the realm of having to decide how secure is secure enough when it comes to defending against malware.

Given the complexity of the interrelationships, there are no panaceas that could address all the issues in one sweep. From our analysis, we conclude that measures that increase the costs of malware perpetrators will, all other things being equal, help reduce the overall cost of security. But since market participants may then be induced to reduce their investments in security, the damages associated with security breaches may not decline.

Similarly, measures that increase the level of security may increase security related costs without actually lowering the damages related to security breaches. In a highly interrelated system, it is often difficult to assess the overall impact of a policy measure due to feedback and unanticipated effects. It is therefore necessary to search for measures that are robust and have desired overall effects in multiple scenarios. In many cases, this may require a clarification of the rights and obligations of individuals or classes of stakeholders.

Notes

1. For a literature review of the available estimates of the costs of malware and network security in general, see: Bauer, J. M., M. J. G. Van Eeten and T. Chattopadhyay (Forthcoming). *Financial Aspects of Network Security: Malware and Spam*. ITU (International Telecommunication Union), *www.itu.int/ITU-D/cyb/.*

2. For those readers interested in policy recommendations, note the recent study; Anderson, R., *et al*. (2008), "Security Economics and the Internal Market", European Network and Information Security Agency, *www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.*

Part III. Malware: What Can Be Done?

Many would agree that the damage caused by malware is significant and needs to be reduced, even though its economic and social impacts may be hard to quantify. That said, Part III of this book focuses on the factors that should be considered in assessing what action to take, and by whom, against malware. These include: the roles and responsibilities of the various market participants[1]*, and the incentives under which they operate (Chapter 7); the activities already being undertaken by communities more specifically involved in fighting malware (Chapter 8); and finally an assessment of what steps could be taken to create a holistic and comprehensive approach to malware (Chapter 9).*

[1] According to the 2002 *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, “participants” refers to governments, businesses, other organisations and individual users who develop, own, provide, manage, service and use information systems and networks.

Chapter 7. The Role of End Users, Business and Government

Malware affects individuals, business and government in different ways. All those participants can play a role in preventing, detecting, and responding to malware with varying levels of competence, resource, roles and responsibilities, as called for in the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (the "OECD Security Guidelines"). Better understanding the roles and responsibilities of the various participants in relation to malware is important to assessing how to enhance the fight against malware.

Key participants

Among the various participants, those concerned by malware are:

- End users (home users, small and medium–sized enterprises (SMEs), public and private sector organisations) whose data and information systems are potential targets and which have different levels of competence to protect them.
- Software vendors, which have a role in developing trustworthy, reliable, safe and secure software.
- Anti-virus vendors, which have a role in providing security solutions to users (such as updating anti-virus software with the latest information on malware).
- Internet Service Providers (ISPs), which have a role in managing the networks to which the aforementioned groups connect for access to the Internet.
- Domain name registrars and regulators, which determine if a domain is allowed to be registered and potentially have the power to deregister a domain that is used to commit fraud or other criminal activity, including, for example, the distribution of malware.
- CSIRTs (computer security incident response teams), frequently the national or leading ones (often government), which have a role, for

example, in detecting, responding to and recovering from security incidents and issuing security bulletins about the latest computer network threats or vulnerabilities associated with malware attacks; or in co-ordinating nationally and internationally the resolution of computer network attacks affecting its constituency or emanating from its constituency.

- Law enforcement entities, which have a mandate to investigate and prosecute cybercrime.
- Government agencies, which have a role to manage risks to the security of government information systems and the critical information infrastructure.
- Governments and inter-governmental organisations, which have a role in developing national and international policies and legal instruments to enhance prevention, detection and response to malware proliferation and its related crimes.

Incentives and disincentives – Highlights from Part II

Better comprehension of how market players are, or are not, incentivised today is important to understand how they are responding to malware and again to assess how to enhance the fight against malware. Incentives are shaped by the costs and benefits associated with the possible responses of each market player. In some cases, there may be strong incentives for a market player to develop policy and technical approaches to more effectively combating malware. In other cases, incentives may be less obvious or even non-existent. Actors make their own trade-offs regarding what kind of security measures they deem appropriate and rational, given their business model.

Very limited information as to how individual actors actually make their information security decisions is available in the public domain, which makes it difficult to calibrate any form of public policy. Economic decisions with regard to information security depend on the particular incentives perceived by each market player (Eeten and Bauer, 2008).

Box 7.1 Different types of incentives

Incentives are often classified as being either monetary (financial, remunerative) or non-monetary (non-financial, moral).

Financial incentives typically connect degrees of achievement of an objective with monetary payments. They include factors such as: tying the salary of an employee to corporate performance; the ability to make a super-normal profit by pursuing a risky innovation; or the bottom line effects of potential damage to a firm's reputation.

Non-financial incentives work through self-esteem (or guilt) and community recognition (or condemnation). They encompass norms and values, typically shared with peers, and which result in a common understanding as to the right course of action, or the set of possible actions that should be avoided in a particular situation.

These incentives are rooted in economic, legal, and other mechanisms, including the specific economic conditions of the market, the interdependence with other players, formal legal rules as well as informal norms. Ideally, the relevant incentives should assure that private costs and benefits of security decisions match the social costs and benefits. Any policy strategy to combat malware, therefore, needs to take into account the existing incentive mechanisms and examine whether they could potentially be modified to produce more efficient outcomes at the societal level.

To illustrate, an online financial service provider might decide that it is more cost-effective to compensate the damage of customers victimised by malware, rather than to introduce new security technology reducing this damage. Not only may those technologies be more costly than the actual direct damage, they could raise the barriers for customers adopting these services. The incentives under which these service providers operate may make it economically rational to keep the damage of malware at manageable levels, rather than to push it back further.

At the societal level, the key policy question is whether the decisions of actors take into account the costs and benefits that result from their response to malware. There are instances where the incentives of actors do not reflect the costs their decisions impose on others – *i.e.* these costs are externalised. An oft-cited example of externality is the lack of security of a category of end users whose machines are infected with malware but who themselves are not bearing the costs of these infections directly, since the malware does not target the host machine but is used to attack others.

Externalities related to malware

Real-world markets rarely meet the preconditions that are assumed to hold according to standard economic theory. For example, decision makers rarely have complete information; they operate under conditions of bounded rationality and behave opportunistically. For these reasons, real-world individual decisions are often a process of "muddling through" second and third-best solutions, especially in an environment of rapid technological change. Moreover, many malware-related externalities and costs have their origin in the illegal or criminal behaviour of illegitimate players imposing costs on legitimate market participants.

Assessing the direct and indirect economic costs of malware and exploring countermeasures is an important issue. As the provision of security entails cost, tolerating a certain level of insecurity is economically rational. The resulting level of security is dependent on the costs and benefits of security. Relevant questions that need to be addressed include:

- Are market players taking the full range of costs into account when making security decisions?
- What costs are externalised to other market participants or society at large?

Findings regarding incentives and externalities for the different market participants confronted with malware reveal three situations: no externalities; externalities that are borne by agents that can manage them; and externalities that are borne by agents who cannot manage them or by society at large (Eeten and Bauer, 2008). For a detailed discussion of these three categories, see Part II of this report.

Incentive structures for market participants

The research project presented in Part II of this report[1], conducted to better understand current incentive structures and possible externalities, shows that the overall response to malware emerges from the interaction of the market participants and the degree of compatibility (or incompatibility) of their respective incentive structures.

It seems that the incentives of many of the commercial stakeholders are reasonably aligned with minimizing the effects of externalities on the sector as a whole. The incentives vary in strength and in some cases they are fairly weak. However, the research in Part II shows that the market participants studied experience at least some consequences of their security trade-offs on others. In other words, feedback loops bring some of the costs imposed on others back to the agent that caused them – even if in some cases the force of the feedback loop has so far been too weak or too localised to bring their behaviour in line with the societal optimum.

For some participants, an important mechanism to achieve this approximate result is the interdependence between them. In other instances it is reputation effects that align incentives with the socially optimal choice. Both effects may operate independently or jointly, as in the case of ISPs.

For instance, a user with insufficient malware protection may cause an externality whose cost is, in part, borne by the service provider, in part by other ISPs, and in part by society at large (*e.g.* costs of law enforcement, overall reduced trust in e-commerce). An ISP may incur costs to enable its network to isolate single users that might spread malware due to insufficient protection of that user's machine. Part of this externality is thus internalised by the ISP because of the incentives of the provider to protect the integrity of its services and to avoid blacklisting and the negative effects this might entail for its operating costs, its reputation and consequently its revenues and growth prospects.

The impact on society at large

Among other findings, the research in Part II also shows that whereas some external effects are internalised at the level of the whole information economy ecosystem, there are some effects that need to be considered as externalities to society at large.

For example, malware and its effects may tarnish the reputation of industries that rely heavily on electronic transactions, such as banking or insurance. If electronic platforms are used less frequently than would otherwise be the case, then the forgone efficiency improvements can be considered an externality cost to society of malware. Moreover, malware may diminish trust in the working and security of e-commerce overall. Again, if this results in slower diffusion and growth, one could consider the unrealised potential efficiency gains as a cost to society. Such potential gains could occur at the sector level but they could also manifest themselves in lower overall economic growth rates. There is evidence throughout the study of concern that such effects are important, although no specific indication as to their magnitude is available.

Security problems and the related economic costs to society may have two roots:

1. They are the outcome of relentless attacks on the information and communication infrastructure by criminals; and
2. Given an overall external threat level, they may be aggravated by discrepancies between private and social costs and benefits which are the outcome of decentralised decision-making in a highly interrelated ecosystem.

Actors in both the criminal world and within the information and communications system respond to the economic incentives they face. For the market players assessed in the empirical study presented in Part II, a mixed incentive structure exists which includes positive incentives as well as disincentives to take action against malware.

Note

[1] The research in Part II of this report is based on in-depth interviews in five countries with representatives of market participants, including Internet Service Providers (ISPs), e-commerce companies with a focus on online financial services, software vendors, hardware vendors, registrars and end users – complemented by interviews with regulators, CSIRTs, ICANN, security services providers and researchers.

Chapter 8. What Is Already Being Done?

Better understanding of the nature, successes and limitations of ongoing action by communities more specifically involved in fighting malware is also important to assessing how to enhance prevention of, and response to, malware.

Summary of key efforts

Substantial efforts by various participants have been made within OECD countries and APEC economies and at the international level to raise awareness, measure malware, develop or amend legal frameworks, strengthen law enforcement, and improve response. For example:

- Many websites and resources exist to help end users and SMEs secure their information systems.
- Many entities track, measure and sometimes even publish data on their experience with malware and related threats.[1] Furthermore, schemas[2] exist to provide single, common identifiers to new virus threats and to the most prevalent virus threats in the wild to reduce public confusion during malware incidents.
- Several informal networks have been created that are a key element of the response community's ability to respond to incidents resulting from malware. CERT/CC has catalogued 38 national CSIRT teams, 19 of which are in OECD countries, and 16 of which are in APEC economies (CERT Coordination Center, 2006). In addition, they hold annual meetings for national CSIRT teams to gather and share information about numerous issues, including malware.
- Numerous countries across the world have legal provisions against hacking, spam, data interference, and system interference. Furthermore, the Convention of the Council of Europe on cybercrime is the first and only legally binding multilateral treaty addressing the problems posed by the spread of criminal activity

online and 43 countries across the globe are now party to the Convention.

- Law enforcement agencies and organisations across the world have made important efforts to find malicious actors and bring them to justice for the crimes they commit. The law enforcement community has created points of contact networks and other similar schema to help cross-border co-operation in recognition that the majority of these crimes cross legal and jurisdictional boundaries. Law enforcement agencies and business typically use tools which implement the Whois protocol to query database servers operated by the domain name registrars and Regional Internet Registries for data on domain name owners, Internet Protocol address and Autonomous System Number allocations that can identify the asserted physical locations where unlawful activity is taking place, and the relevant service providers (ISPs), which, in turn, can provide information regarding their customers.

- ISPs are operating in highly competitive markets and are taking proactive steps in the fight against malware, such as quarantining infected machines.

- Software vendors have increased efforts to improve the security of their software. The deployment of vulnerability patches has improved. Arguably more important, many software vendors put software development processes in place that are increasingly aware of and focusing on security issues.

- Governments across OECD countries and APEC economies are taking policy, legislative and technical measures to address malware[3]. In particular, they are working, in co-operation with the private sector, to protect their government critical information infrastructure from electronic attack.

These communities have made significant efforts to address the issue of malware and anecdotal evidence suggests a much greater awareness of the problem than only a few years ago. The nature of malicious and criminal online activity, however, is such that these communities are always “catching up” with the malicious activities. This report has shown that eliminating all malware is neither feasible nor economically rational but making it harder for malicious actors to succeed – through prevention and early detection – and making them liable when they do – through better policies, procedures, legal frameworks and law enforcement – are examples of actions that are within the roles and responsibilities of the communities fighting malware and could significantly help close the gap.

Instruments, structures and initiatives that address malware

This following section provides examples (rather than a comprehensive list) of existing instruments, structures and initiatives, at the national and international levels, whose purpose is to help address the issue of malware.

Awareness raising

Awareness is an important line of defense against malware and the crimes resulting from its use. Both the public and private sectors, separately or in partnership, have taken initiatives to educate Internet users about malware.

Australia - E-Security National Agenda (ESNA)

The Australian Government established the ESNA in 2001 to create a secure and trusted electronic operating environment for both the public and private sectors. A review of the ENSA in 2006 found that the online environment is highly interconnected and that e-security threats to different segments of the Australian economy can no longer be addressed in isolation. In this context, the Australian Government announced AUS$73.6 million over four years for new measures to strengthen the electronic operating environment for business, home users and government agencies.[4] In addition, the Australian government is undertaking the following initiatives:

- An annual National E-Security Awareness Week will be held in collaboration with industry and community organisations. The week encourages Australian home users and SMEs to undertake smart behaviour online. A pilot Awareness Week was held in October 2006.
- The enhancement of the Government's e-security website *www.staysmartonline.gov.au* is the key mechanism to disseminate simple e-security information and advice to home users and small businesses on how they can secure their computers and adopt smart online practices.
- The development of an e-security education module for Australian schools to focus on raising e-security awareness of young Australians.
- The establishment of an easy to understand, free National E-Security Alert Service that will be delivered through the Government's e-security website to provide information on current e-security threats and vulnerabilities.

The Australian Government has also developed a number of booklets to encourage Australian consumers and small businesses to protect themselves against e-security threats.[5]

Australia Netalert[6]

Launched in August 2007 by the Australian government, Netalert is an Internet safety initiative that combines an Internet safety information campaign, a National Filter Scheme to provide free access to an Internet content filter to help block unwanted content, and a website and hotline to provide advice about protecting children online, as well as access to the free filters, and information about how they work.

Australia Stay Smart Online website

The Stay Smart Online website provides simple step by step advice to home users and small and medium sized-enterprises (SMEs) on how they can protect themselves on line.

EU Safer Internet Plus Programme[7]

At the EU level, the Safer Internet plus programme promotes safer use of the Internet and new online technologies, particularly for children, as part of a coherent approach by the European Union.

Get Safe Online[8]

The Get Safe Online (GSO) is the UK Government website that aims to provide awareness raising information about safe online practices for home and SME Internet users. The website complements the ITsafe website and focuses on awareness raising activities with links to popular websites. The education material provides information on e-mail, malware, phishing and spyware. The website was initiated by a joint agreement between the UK Government and the private sector, namely sponsors from technology, retail and finance.

Get Safe Online Week (GSOW) was launched in October 2006 and included various awareness raising activities. Activities of the Week included an Internet safety summit with an objective to initiate liaison between government, industry and the public sector with a focus on issues of Internet crime. A Memorandum of Understanding (MOU) was signed that committed signatories to assist in the protection of the public when using the Internet and to promote GSO as a source of free, up to date information and advice.

The service is funded by the UK Government Home Office and uses information provided by the Centre for the Protection of National Infrastructure (CPNI). This Government department provides electronic defence for the UK Government. The aim of the ITsafe website is to advise of the best methods necessary to protect personal and business data. ITsafe is managed by a Government team on behalf of the CPNI by the Central Sponsor for Information Assurance (CSIA).

New Zealand Netsafe[9]

Netsafe is a partnership between The Internet Safety Group (ISG), an independent non-profit organisation responsible for cybersafety education in New Zealand, and the New Zealand Ministry of Education with representation and sponsorship from industry, police, banking and others. The focus of NetSafe is to provide children with information about sexual and other similar instances of abuse online. The site also has information about malware, computer maintenance, peer 2 peer file sharing, IRC security risks, hackers and other e-security information is provided.

The NetSafe website covers topics including online safety for children and teenagers, online security for businesses, Internet fraud and law enforcement, online gambling, copyright, e-commerce and the law. NetSafe also hosts a cartoon website, Hector's World, designed to entertain and educate children about online safety.

United Kingdom ITsafe[10]

The ITsafe initiative is a UK website that provides simple and easy to understand e-security alerts and threats to both home and small business Internet users. Advice and information contained within the website is free and includes varying types of e-security threat alerts and warnings enabling a safer electronic environment for Internet users.

United States Onguard Online[11]

OnGuardOnline.gov is a website maintained by the US Federal Trade Commission and partners such as the US Postal Inspection Service, the US Department of Homeland Security, the US Department of Commerce, and the Securities and Exchange Commission to provide practical tips from the federal government and the technology industry to help users be on guard against Internet fraud. It also provides information on how users can secure their information systems and protect their personal information.

United States StaySafeOnline[12]

StaySafeOnline is a website provided for the public by the National Cyber Security Alliance, a US industry coalition supported by the US Department of Homeland Security to provide cyber security awareness to the home user, small businesses, higher education, and K-12 students. It provides free and non-technical cyber security and safety resources including alerts, tips, and reports to the public so consumers, small businesses and educators have the knowhow to avoid cyber crime.

Untied States – National Awareness Month

The United States Government in collaboration with industry holds an annual National Cyber Security Awareness Month (NCSAM). The month aims to raise awareness about online security and how to adopt safe online practices. The activities and events held in the month focus on home Internet users, SMEs, government, education and the corporate sector.

Teenangels[13]

Teenangels is a US based group of 13-18 year-old volunteers who have been specially trained by the local law enforcement, and many other leading safety experts in all aspects of online safety, privacy, and security including spyware. After completion of the required training, the Teenangels run unique programs in schools to spread the word about responsible and safe surfing to other teens and younger children, parents, and teachers.

Conventions

Council of Europe Convention on Cybercrime

The Convention of the Council of Europe (COE) on Cybercrime is the first and only legally binding multilateral treaty addressing the problems posed by the spread of criminal activity on line. Signed in Budapest, Hungary in 2001, the Convention entered into force on 1 July 2004. Recognising digitalisation, convergence and continuing globalisation of computer networks, the Convention requires its signatories to establish laws which criminalise security breaches resulting from hacking, illegal data interception, and system interferences that compromise network integrity and availability.

This instrument, which cites OECD actions as a means to further advance international understanding and co-operation in combating cybercrime, aims to “pursue … a common criminal policy for the protection of society against cybercrime by adopting appropriate legislation and fostering international co-operation." To achieve these goals, the signatories commit to establish certain substantive offences in their laws which apply to computer crime. Although malware is not *per se* mentioned in the Convention among the illegal activities that signatories must criminalise, it is indirectly covered under closely related listed crimes including illegal access to information systems, computer data, and computer-related fraud.[14]

The Convention encourages a more coherent approach in the fight against cyber attacks. It also includes provisions for a 24 hours per day, 7 days per week online crime-fighting network and facilitates public-private partnerships. The Convention also provides extradition and mutual legal assistance treaties' provisions between signatories where none exist.

To date, the Convention has been ratified by 21 countries and signed by 22 additional countries (Council of Europe, 2001). Some companies in the private sector have taken some initiatives to help ensure a larger impact of the Convention's principles.[15]

Detection and response

Many countries have a watch, warning and incident response function in the form of a CSIRTs or CERT. It is important to recognise that not all CSIRTs and CERTs are alike. Some are public entities residing in the government structure, some are publicly and privately funded entities with multiple mandates and still others are associated with academic institutions.[16] It is widely accepted good practice that governments develop or appoint a CSIRT or CERT with national responsibility.[17]

In some cases, entities within a country are required to report information security incidents to a central government authority competent to handle them. In some cases this entity is a CSIRT/CERT. For example, in Finland it is obligatory that significant violations of information security, faults and disturbances in public telecommunications be reported to the national CSIRT of Finland, CERT-FI.[18] One example of a "significant violation" is considered activation of malware in telecommunication service providers' own systems". In order to fulfil this regulation for external incident reporting, the telecommunications service provider must have adequate internal processes for detection and reporting of as well as recovery from information security incidents and threats. This model has been successful in Finland because the government has proven to the reporting parties to be trustworthy and capable of handling sensitive information and they actively meet with major carriers in one-on-one sessions to share information.

In the United States, all civilian government agencies are required to report information security incidents to US-CERT.[19] In both Finland and the United States a standard incident report form is provided.

International initiatives

Forum of Incident Response Security Teams (FIRST)

FIRST brings together a variety of computer security incident response teams (CSIRTs) from government, commercial, and educational organisations in 37 countries. FIRST aims to foster co-operation and co-ordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.[20] Membership in FIRST enables incident response teams to reach counterparts in other countries that can help them to more effectively respond to security incidents.

Asia Pacific CERT (APCERT)[21]

APCERT is a contact network of computer security experts in the Asia Pacific region established to improve the region's awareness and competency in relation to computer security incidents. APCERT works to enhance co-operation on information security, facilitate information sharing and technology exchange and promote collaborative research on subjects of interest to its members. APCERT also works co-operatively to address legal issues related to information security and emergency response across regional boundaries.

Caribbean Telecommunication Union

The Caribbean Telecommunications Union (CTU) has been involved in the development of an Internet Governance Framework for the Caribbean on behalf of the Caribbean Community (CARICOM). The CTU has held several significant Internet Governance forums at which delegates raised the issue of establishing a Caribbean Computer Emergency Resource Team (CERT) for timely detection of security incidents in regional computer networks, their proper handling and post-detection activities. There is now a growing body of ICT practitioners who have expressed the need for a CERT to be established for the Caribbean. In response, the CTU will be engaging ICT practitioners in the coming months to consider the security requirements of the region and to investigate the need for and the means by which a Caribbean CERT may be established.

The European Government CERT Group (EGC)

The EGC[22] group is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe. To achieve this goal, the EGC members jointly develop measures to deal with large-scale or regional network security incidents, facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities, share knowledge and expertise, identify areas of collaborative research and development on subjects of mutual interest, and encourage formation of government CSIRTs in European countries

Gulf Coordination Council CERT (GCC CERT)

GCC CERT aims to supervise the establishment of national response teams in Saudi Arabia, the United Arab Emirates, Qatar, Bahrain, Kuwait and Oman.

Task Force CSIRT (TF CSIRT)[23]

The activities of TF CSIRT are focused on Europe and neighbouring countries, in compliance with the Terms of Reference approved by the TERENA Technical Committee on 15 September 2004. TF CSIRT provides a forum for the European CSIRTs to communicate, exchange experiences and knowledge, establish pilot services, and assist the establishment of new CSIRTs. Other goals of the TF CSIRT include:

- To promote common standards and procedures for responding to security incidents.
- To assist the establishment of new CSIRTs and the training of CSIRTs staff.

Enforcement

Domestic structures

Under EU legislation the provisions detailed on the next page may be enforced by administrative bodies and/or criminal law authorities. Where this is the case, the Commission has stressed that at national level the responsibilities of different authorities and co-operation procedures need to be clearly spelled out. To date, the increasingly entwined criminal and administrative aspects of spam and other threats have not been reflected in a corresponding growth of co-operation procedures in Member States that brings together the technical and investigative skills of different agencies. Co-operation protocols are needed to cover such areas as exchange of information and intelligence, contact details, assistance, and transfer of cases.

In the United States, both the Federal Bureau of Investigation and the U.S. Secret Service have authority to investigate malware crimes in violation of the Computer Fraud and Abuse Act (Title 18, United States Code, Section 1030). Violations of the Computer Fraud and Abuse Act are prosecuted in US federal courts by the US Department of Justice, through its US Attorney's Offices and the Criminal Division's Computer Crime and Intellectual Property Section. The US Department of Justice also prosecutes malware-related crimes such as criminal violations of the CAN-SPAM Act (Title 18, United States Code, Section 1037), access device fraud (Title 18, United States Code, Section 1029) and Aggravated Identity Theft (Title 18, United States Code, Section 1028A).

International mechanisms

Various international forums focusing on security, privacy or consumer protection issues, devote substantive efforts to tackle the multifaceted nature of cybercrime.

The Contact Network of Spam Authorities (CNSA)[24]

On the initiative of the European Commission, an informal group was created consisting of National Authorities involved with the enforcement of Article 13 of the Privacy and Electronic Communication Directive 2002/58/EC called the Contact Network of Spam Authorities (CNSA). In the CNSA, information on current practices to fight spam is exchanged between National Authorities, including best practices for receiving and handling Complaint information and Intelligence and investigating and countering spam. The CNSA has set up a co-operation procedure that aims to facilitate the transmission of complaint information or other relevant Intelligence between national authorities. The CNSA has drawn up a co-operation procedure to facilitate cross-border handling of spam complaints and is working on the issue of spyware and malware.

G8 24/7 Cybercrime Network

The G8 Subgroup on High-Tech Crime operates a 24/7 network to assist investigations involving electronic evidence and requiring urgent assistance from foreign criminal law enforcement authorities. The 24/7 Network, which includes almost 50 countries, was created among the G8 countries in 1997 to address the unique challenges that high-tech crime investigations pose to law enforcement. The 24/7 Network is designed to supplement (but not replace) traditional mutual legal assistance frameworks by providing a mechanism to facilitate the preservation of electronic evidence. The 24/7 Network has been instrumental in preserving evidence in hacking, fraud, and violent crime investigation and for providing training on topics such as botnets.

Interpol

Interpol[25] is an international police organisation with a mission to prevent or combat international crime. Interpol has decentralised its cybercrime expert teams around the world through the establishment of regional Working Parties on Information Technology Crime for Europe, Latin America, Asia, South Pacific, and Africa.[26] Interpol's European Working Party on Information Technology Crime (EWPITC) has for example compiled a best practice guide for experienced investigators from law enforcement agencies.[27] It has also set up a rapid information exchange system under an international 24-hour response scheme, listing responsible experts within more than 100 countries. This scheme was notably endorsed by the G8 24/7 HTCN.

London Action Plan (LAP)[28]

The purpose of the London Action Plan is to promote international spam enforcement co-operation and address spam–related problems, such as online fraud and deception, phishing, and dissemination of viruses. The LAP includes participation from government, public agencies, and the private sector from over 27 countries.

International Consumer Protection Enforcement Network (ICPEN)

The International Consumer Protection and Enforcement Network (ICPEN) is a network of governmental organisations involved in the enforcement of fair trade practice laws and other consumer protection activities. ICPEN was founded in 1992 by 20 countries and in co-operation with the OECD and the EU; the network now has 29 participant countries. A Memorandum on the Establishment and Operation of ICPEN governs this network. The primary objective of the ICPEN is to facilitate practical action and information exchange among its members to prevent and redress deceptive marketing practices across international borders. To accomplish this, the ICPEN fosters co-operative efforts to address the problems consumers face in conducting cross-border transactions for goods and services. ICPEN co-operation does not include the regulation of financial services and product safety and it does not provide a platform for the procurement of specific redress for individual consumers.

ICPEN has established several working groups including: The Mass Marketing Fraud Working Group, Best Practices Working Group, ScamWatch Working Group that covers some of the issues associated with malware. In addition, their Internet Sweep initiative seeks to find and eliminate fraudulent and deceptive Internet sites.

Legislation

While malware is rarely mentioned as such in legislation, malicious activities that use malware are often covered by numerous existing areas of law including criminal law, consumer protection law, data protection law, telecommunication law, and anti-spam law. A survey by the OECD Task Force on Spam at the end of 2004 indicated that most OECD countries have, in the past few years, set up a legislative framework in order to fight spam that may apply to malware in some cases.

In the European Union, under the e-Privacy Directive and the General Data Protection Directive, national authorities have the power to act against the following illegal practices:

- Sending unsolicited communications (spam).[29]
- Unlawful access to terminal equipment; either to store information – such as adware and spyware programs – or to access information stored on that equipment.[30]
- Infecting terminal equipment by inserting malware such as worms and viruses and turning PCs into botnets or usage for other purposes.[31]
- Misleading users into giving away sensitive information such as passwords and credit card details by so-called phishing messages.[32] Some of these practices also fall under criminal law, including the Framework Decision on attacks against information systems.[33] According to the latter, Member States have to provide for a maximum penalty of at least three years imprisonment, or five years if committed by organised crime.

Some additional recent examples of legal developments include:

- The UK Police and Justice Bill 2006.[34] This law, among other provisions, updated the Computer Misuse Act 1990 (CMA) to prohibit the preventing or hindering access to a programme or data held on a computer, or impairing the operation of any programme or data held on a computer. The law also increased the maximum penalty for such cybercrimes from five to ten years and refined the definition of computer abuse to cover denial of service attacks.

- Germany's August 2007 anti-hacking law, making hacking[35], denial-of-service, and computer sabotage attacks on individuals[36] illegal. The provisions extend criminal liability to the intentional "preparation of criminal offences" by producing, distributing, procuring etc. of devices or data designed for such purposes. Offenders could face sentences of up to ten years in prison for major offenses.

- The United States Congress is considering legislation that would create a law that would establish that the use of spyware to collect personal information or to commit a federal criminal offense is a federal crime. If passed by and signed into law, it would authorise the appropriation of USD 40 million for the prosecution of violations of the new law from 2008 to 2011.[37] In addition, the US Federal Trade Commission (FTC) has actively pursued spyware companies using its authority under Section 5 of the FTC Act. The FTC has brought 11 law enforcement actions during the past two years against spyware distributors. These actions have reaffirmed three key principles. First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures about software and its effects are not adequate, just as they have never been adequate in traditional areas of commerce. And third, if a distributor puts an unwanted program on a consumer's computer, he or she must be able to uninstall or disable it.

Public-private structures

Domestic initiatives

Australia: Internet Security Initiative[38]

The Australian Internet security initiative, administered by the Australian Communications Media Authority, provides information free of charge to Internet service providers about 'zombie' computers operating on their networks. The program operates by forwarding information on bot-infected computers to Australian ISPs.[39] These ISPS then contact their customers to assist them to 'disinfect' their computer.

An initial trial of the Australian Internet Security Imitative commenced in November 2005, with participation of six Internets service providers (ISPs). The trial highlighted that the vast majority of customers are unaware that their computers are infected by malware and are grateful for the assistance in making their computer secure. Since the trial commenced the *Internet Industry Spam Code of Practice f a Code for Internet and Email Service Providers* has come into effect (16 July 2006). The code complements the Australian internet security initiative, as it contains provisions that enable ISPs to disconnect a customer's computer if the problem is not resolved by the customer.

United States

One example of public-private-partnership in the US is in critical infrastructure protection, under the National Infrastructure Protection Plan (NIPP) managed by the US Department of Homeland Security. The framework under the NIPP includes a government entity ("Government Coordinating Council", GCC) made up of government agencies and industry entities ("Sector Coordinating Council", SCC) in each of the determined critical infrastructure sectors, including the Information Technology and Communications sectors. The NIPP is a framework for assessing and managing the risk to each of the sectors, including threat, vulnerabilities, and consequences.[40]

Another example of public-private domestic co-operation is the US INFRAGARD programme to improve and extend information sharing between private industry and the government, including law enforcement, on threats to critical national infrastructure.

Finally, the US National Cyber-Forensics and Training Alliance, is a joint partnership between law enforcement, academia, and industry that collaborates on cybercrime issues. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations.[41]

International initiatives

Council of Europe/Microsoft

In August 2006, the Council of Europe and Microsoft partnered to promote broad implementation of the Convention on Cybercrime.

Anti Phishing Working Group

The Anti-Phishing Working Group (APWG) is a volunteer–run consortium of industry and law enforcement focused on eliminating the results from phishing, pharming[42] and e-mail spoofing of all types. The APWG has over 2 600 members including 1 600 companies and agencies as well as national and provincial law enforcement. It provides a forum to examine phishing issues, define the scope of the phishing problem in terms of costs, and share information and best practices for eliminating the problem.[43] The APWG website provides a public resource for reporting phishing attacks. When phishing is reported, the APWG analyses the information provided and adds it to its online phishing archive. The APWG also works to share information about phishing attacks with law enforcement when appropriate. In addition to phishing, the APWG tracks phishing-based Trojans, keyloggers and other malware.

Messaging Anti-Abuse Working Group[44]

The Messaging Anti-Abuse Working Group is a global organisation focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. With a broad base of Internet Service Providers (ISPs) and network operators representing over 600 million mailboxes, key technology providers and senders, MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives.

Microsoft's Botnet Task Force

Through its international Botnet Task Force, first held in 2004, Microsoft provides training to law enforcement officials from around the world who have been confronted with the task of investigating Botnet abuses (Charney, S., 2005).

PhishTank

PhishTank is a free community site where anyone can submit, verify, track and share phishing data. PhishTank is an information clearinghouse, which provides accurate, actionable information to anyone trying to identify bad actors, whether for themselves or for others (*i.e.*, building security tools). PhishTank is a consortium led by OpenDNS, a commercial provider of public recursive DNS services.

Anti-Spyware Coalition (ASC)

The ASC is a group composed of anti-spyware software companies, academics, and consumer groups which focuses on the development of standard definitions in relation to spyware. On 25 January 2007, ASC published working documents on best practices[45] aimed to detail the process by which anti-spyware companies identify software applications as spyware or other potentially unwanted technologies.

Private sector partnerships

One example of private sector partnerships in the United States is the creation and continued development of the Information Technology Information Sharing and Analysis Center (IT-ISAC). The IT-ISAC is a trusted community of security specialists from companies across the Information Technology industry dedicated to protecting the Information Technology infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to quickly and properly address them.[46]

Standards and guidelines

Institute of Electrical and Electronics Engineers (IEEE)[47]

The IEEE is a non-profit organisation for the advancement of technology. Through its global membership, the IEEE is a leading authority on areas ranging from aerospace systems, computers and telecommunications to biomedical engineering, electric power and consumer electronics among others. Members rely on the IEEE as a source of technical and professional information, resources and services. The IEEE is a leading developer of standards for telecommunications and information technology.

International Standards Organisation (ISO)

The International Organization for Standardization (ISO) is a worldwide federation of one national standards bodies from more than 145 countries. ISO is a non-governmental organisation established in 1947 and based in Geneva, Switzerland. Its mission is to promote the development of standardisation and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing co-operation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements which are published as International Standards and other types of ISO documents.

Some relevant ISO/IEC standards include the following:

- ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management.
- ISO/IEC 19770-1 Software Asset Management: Are You Ready?

In June 2007, the ISO and IEC joint technical committee (JTC) 1 subcommittee (SC) 27 proposed a new work Item on “Guidelines for cybersecurity (27032)”.[48] This standard would provide comprehensive guidelines on cybersecurity[49] to both service providers and users (organisations and end users) and, in particular address behavioural, organisational and procedural issues. More specifically, it would offer ‘best practice’ guidance in achieving and maintaining security in the cyber environment for audiences in a number of areas, and address the requirement for a high level of co-operation, information-sharing and joint action in tackling the technical issues involved in cybersecurity. This needs to be achieved both between individuals and organisations at a national level and internationally.

National Institute of Standards and Technology

Founded in 1901, NIST is a non-regulatory federal agency within the US Department of Commerce. NIST's mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. In November 2005, NIST published the *Guide to Malware Incident Prevention and Handling* as NIST Special Publication (SP) 800-83.[50]

World Wide Web Consortium

The World Wide Web Consortium (W3C)[51] is an international consortium where member organisations, a full-time staff, and the public work together to develop web standards. W3C's mission is “To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web.”

Technical solutions and resources

Sample domestic initiatives

Japan – Cyber Clean Center (CCC)

In 2006, the Japanese government began a project to reduce the number of bot infected computers in Japan with the objective of preventing spam e-mails and cyber attacks in Japan. To accomplish this, Japan has created a bot removal tool known as "CCC cleaner" which can be downloaded free of charge at *www.ccc.go.jp*.

Current results from the project include 31 000 trapped bot programmes (hash unique) and 1 300 bot programmes reflected in the removal tool. To date, a total of 57 000 users in Japan have downloaded the removal tool. Next steps for enhancing the project could include changing the composition of honeypots and broadening the reach of ISPs.

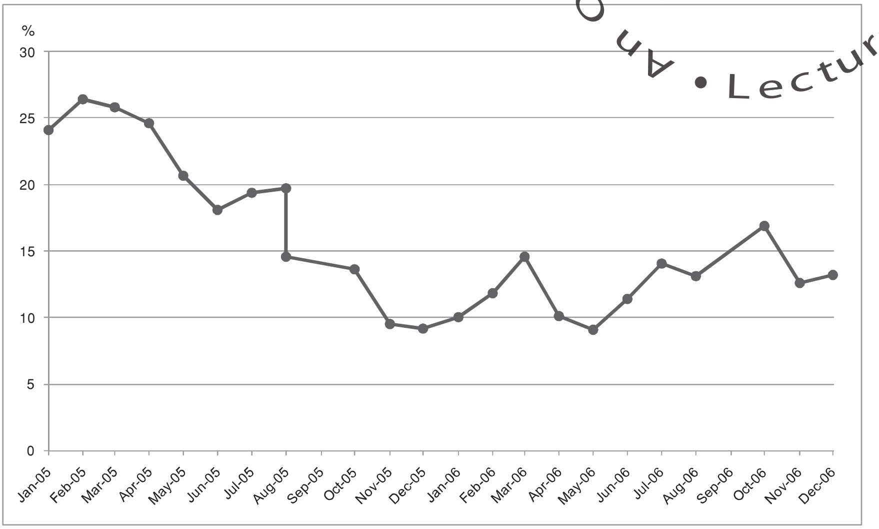
Korea – Automated Security Update Programme (ASUP)

To reduce the damage from vulnerabilities in Microsoft Windows, Korea Internet Security Center (KrCERT/CC) and Microsoft Korea collaborated to develop and deploy the Automated Security Update Programme (ASUP) to home and SME users. The programme seeks to make all Internet connected information systems install Windows security related patches without user intervention once they have installed ASUP. When users visit major Korean websites, such as portals, online game sites, a popup window appears in the screen to confirm the installation of the ASUP. While offering the same functionality as Windows automatic updates, ASUP allows users to just click once to approve ASUP installation without having to modify the configuration of Windows updates.[52] Microsoft Korea has distributed the programme in accordance with Microsoft headquarters centralised patch policy, balancing user convenience and company's philosophy on security.

Sinkhole System

The sinkhole system works to prevent bots from connecting to botnet command and control (C&C) servers by subverting the IP address of the botnet C&C server. When a bot-infected zombie makes a query to a DNS server, the answer to the query (IP address for the botnet C&C server) will be the address of the Sinkhole System. The connection attempt is then redirected to a sinkhole system in KrCERT/CC, rather than to the C&C server. The sinkhole system can track and analyze all activities of connected botnets. As shown in Figure 8.1, after the adoption of this sinkhole system in 2005, the botnet infection rate of Korea has reportedly dropped to almost one third at the end of 2005, compared with that of January or February 2005.

Figure 8.1 Botnet infection rate of Korea (2005-2006)



MC Finder

One additional countermeasure used by KrCERT/CC is the implementation of MC Finder which locates malware on compromised websites. MC Finder identifies an average of 500 exploited websites every month in Korea. KrCERT/CC is sharing the malware patterns with Google and three Korean major portal companies.

Many effective technical solutions and resources have been developed to combat threats relating directly or indirectly to malware. Some examples of such solutions and resources include the following:

Domain Name System Security (DNSSEC)

DNSSEC applies cryptography to the Domain Name System to authenticate the information served, allowing DNS servers and resolvers to verify that DNS responses are coming from the correct place and that they are unadulterated. It does this by providing a security and authenticity mechanism for the DNS known as DNSSEC. DNSSEC uses public keys and digital signatures to authenticate DNS information. Many countries are working to deploy DNSSEC at the ccTLD. For example, Sweden, Bulgaria, and Puerto Rico have moved their country code TLDs to DNSSEC; however, it is important to have government, business, banking, and registry co-operation to successfully implement DNSSEC. There are currently several experimental tests of secure DNS zones. It is recognised that DNSSEC will not eliminate all misuse of the DNS. Some consider that it may reveal private information from DNS databases and therefore pose legal challenges for deployment in some countries.

Domain level authentication

Domain-level authentication is a means to enable a receiving mail server to verify that an e-mail message actually came from the sender's purported domain. In other words, if a message claimed to be from *abc@ftc.gov*, the private market authentication proposals would authenticate that the message came from the domain “ftc.gov”, but would not authenticate that the message came from the particular e-mail address “abc” at this domain. Hypothetically, if a phisher sent e-mail claiming to be from citibank.com, the message would be filtered by ISPs because the message would not have come from a designated Citibank mail server. Consequently, ISPs and other operators of receiving mail servers could choose to reject unauthenticated e-mail or subject such messages to more rigorous filtering.

Spam filtering[53]

Filtering is the most common technical anti-spam technology. The main benefits of filters are the ease of implementation and the flexibility that users have in deciding which messages should be treated as spam. Heuristic filters require that users specify criteria, such as keywords or a sender’s address that will prompt the filter to block certain messages from reaching the consumer’s inbox. Spammers who deliberately misspell words or spell them in a different language easily outsmart the keyword approach. More recent filters learn based on experience. They create statistics about each user’s messages in a recognition table for future reference to distinguish between spam and legitimate mails. The filter then lets through only messages that resemble the user’s previous legitimate mail.

Common Vulnerability Exposure (CVE)[54]

CVE is a dictionary of standardised names for vulnerabilities and other information security exposures freely available to the public. The goal of CVE is to standardise the names for all publicly known vulnerabilities and security exposures. CVE is a community-wide effort sponsored by the US Government.

Common Malware Enumeration (CME)[55]

CME provides single, common identifiers to malware threats in the wild to reduce public confusion during malware incidents. CME is not an attempt to replace the vendor names currently used for viruses and other forms of malware, but instead aims to facilitate the adoption of a shared, neutral indexing capability for malware.

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The actual technical work of the IETF is done in its working groups, which are organised by topic into several areas (*e.g.* routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

World Wide Web Consortium

The World Wide Web Consortium (W3C)[56] is an international consortium where Member organisations, a full-time staff, and the public work together to develop web standards. W3C's mission is “To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web.”

Notes

1. See Annex A. Background Data on Malware.
2. One example of such a scheme is the Common Malware Enumeration (CME), the last notification of which was published on January 19, 2007 (see *http://cme.mitre.org/data/list.html* – it is difficult to know whether the delay in assigning CME references is a result of political problems with the project, a lack of co-operation from vendors, or attacks becoming more targeted and therefore falling outside the original scope of malware that CME addresses). Some experts consider that tracking malware consistently across the industry is as large a problem as it was several years ago or even greater today due to the significant increases in the number of in-the-wild samples. Therefore, the problem of common malware identifiers is an issue that could still need to be addressed practically.
3. See "Instruments, Structures and Initiatives that Address Malware" below.
4. The revised ESNA can be found at *www.dbcde.gov.au/__data/assets/pdf_file/0011/71201/ESNA_Public_Policy_Statement.pdf*.
5. Information available at *www.dcita.gov.au/communications_and_technology/publications_and_reports*.
6. Information available at *www.netalert.gov.au*.
7. Information available at *http://ec.europa.eu/information_society/activities/sip/index_en.htm*.
8. Information available at *www.getsafeonline.org/*.
9. NetSafe at *www.netsafe.org.nz* is an initiative of the Internet Safety Group (ISG).
10. Information available at *www.itsafe.gov.uk*.
11. Information available at *http://onguardonline.gov/index.html*.
12. Information available at *http://www.staysafeonline.org*.

13. Information available at *www.teenangels.org/index.html*.

14. Council of Europe (2001), Articles 2, 3, 8.

15. In 2006, Microsoft offered a substantial contribution to the Council of Europe to finance the Convention's implementation programme.

16. The European Network and Information Security Agency (ENISA) provides a comprehensive directory of CSIRTS/CERTs in Europe at *www.enisa.europa.eu/cert_inventory/index_inventory.htm*.

17. In 2006, CERT/CC began hosting an annual meeting of CSIRTs with national responsibility; see *www.cert.org/csirts/national/conference2007.html*. They also keep a list of CSIRTs with national responsibility at *www.cert.org/csirts/national/contact.html*

18. Finnish Communications and Regulatory Authority (FICORA) 9 B/2004 M; available online at *www.ficora.fi/attachments/englanti/1156489108198/Files/CurrentFile/FICORA09B2004M.pdf*.

19. Federal Information Security and Management Act (FISMA), *www.pearlsw.com/resources/Experts/OMBRequirements.pdf*.

20. Available online at *www.first.org*.

21. APCERT website *www.apcert.org/about/structure/members.htm*.

22. EGC members include: Finland – CERT-FI, France – CERTA; Germany – CERT-Bund; Hungary – CERT/Hu; Netherlands – GOVCERT.NL; Norway – NorCERT; Sweden – SITIC; Switzerland – SWITCH-CERT; United Kingdom - UNIRAS/NISCC.

23. Information available at *www.terena.org/activities/tf-csirt/*.

24. Information available at *http://stopspamalliance.org/?page_id=11*.

25. Interpol includes 186 member countries, *www.interpol.int/public/icpo/default.asp*.

26. Information available at*www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa*.

27. The *Information Technology Crime Investigation Manual*. This manual is digitally available via Interpol's restricted website.

28. Information available at *www.londonactionplan.com*.

29. European Union (2002).

30. European Union (2002), Article. 5 (3).

31. Ibid.

32. European Union (1995), Article 6 (a).

33. European Union (2005).

34. Introduced into UK law in November 2006.

35. The law defines hacking as penetrating a computer security system and gaining access to secure data, without necessarily stealing data.

36. Existing law already limits sabotage to businesses and public authorities.

37. Congressional Budget Office Cost Summary (2007) p.1.

38. Information available at *www.acma.gov.au/WEB/STANDARD//pc=PC_100882*.

39. The following ISPs have now also joined the initiative: Access Net Australia; AUSTARnet, Bekkers, Chariot, iinet, OzEmail, Powerup, ihug, SeNet, Internode, Agile, Neighbourhood Cable, iPrimus, Primusonline, Hotkey, AOL, Reynolds Technology, Riverland Internet and Soul.

40. The NIPP is available at *www.dhs.gov/xprevprot/programs/editorial_0827.shtm*.

41 Information available at www.ncfta.net/default2.asp.

42. Pharming" (or "warkitting") uses similar techniques as a classic phishing attack, but in addition redirects users from an authentic website (from a bank for instance) to a fraudulent site that replicates the original in appearance. When a user connects its computer to, for instance, a bank web server, a hostname lookup is performed to translate the bank's domain name (such as "bank.com") into an IP address containing a series of numbers (such as 193.51.65.37). It is during that process that malicious actors will interfere and change the IP address. See OECD (2008b).

43. Information available at *www.antiphishing.org/index.html*.

44. Information available at *www.maawg.org*.

45. Information available at *www.antispywarecoalition.org/documents/BestPractices.htm*.

46. Information available at *http://www.it-isac.org*.

47. Information available at *www.ieee.org*.

48. This work item is still in a development phase as of April 2008. For more information, see *http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/755080/1054034/2541793/JTC001-N-8620.pdf?nodeid=6542097&vernum=0*.

49. As defined by the proposed standard, cybersecurity refers to "the protection of assets belonging to both organisations and users in the cyber environment. The cyber environment in this context is defined as the public on-line environment (generally the Internet) as distinct from "enterprise cyberspace" (closed internal networks specific to individual organisations or groups of organisations)."

50. Information available at *http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf*.

51. Information available at *www.w3c.org*.

52. During the installation of Windows XP, users are asked to specify the setting of Windows Updates (Use Automatic Windows Updates or Notify Later). To protect users who inadvertently choose the "notify later" option KrCERT/CC developed the AUSP programme with Microsoft Korea. Just by installing the ActiveX control, users get protection from system vulnerabilities.

53. See OECD (2006).

54. Information available at *http://cve.mitre.org/*.

55. Information available at *http://cme.mitre.org*.

56. Information available at *www.w3c.org*.

Chapter 9. Possible Next Steps

This book has only begun to lay the foundation for understanding the malware phenomenon and how it is evolving. Further work in many areas could and should be done to reach a better understanding. Fighting malware is complex and would benefit from more comprehensive measurement, co-ordination and policy solutions. While many ongoing initiatives[1] are contributing important resources to combating malware, there remain a number of areas for improvement.

A global partnership against malware

The need for a consistent approach to a global problem is not new, but malware presents particular complexities due to the wide variety of actors with responsibility for combating malware. The communities involved in fighting malware, whether governments, businesses, users, or the technical community, need to improve their understanding of the challenges each of them faces and co-operate – within their communities and across communities – to address the problem. Furthermore, their co-operation must occur at the global level. It is not enough for one country or one community to effectively self organise if others do not do so as well.

In light of the need for a holistic and comprehensive approach to malware, a common point of departure from which to build co-operation and collective action could be to launch at the international level a global "Anti-Malware Partnership" involving government, the private sector, the technical community, and civil society. Such collaboration across the various communities involved with fighting malware could benefit from the experience gained from developing the OECD's Anti-Spam Toolkit.

Different international public and private organisations including the OECD and APEC could partner and lead the work in their area of competence. They could then produce joined-up policy guidance to fight malware on all fronts (proactive prevention strategies, co-operation for response, legal frameworks/law enforcement, technical measures, economic aspects, measurement of malware, global co-operation).

Areas for improvement and further exploration

Specifically, the “Anti-Malware Partnership” could examine the following elements:

Proactive prevention strategies

This element could examine all or part of the following:

- Reduction of software vulnerabilities (*e.g.* secure software development could be encouraged; governments could maximise their influence as buyers of software by requiring more secure software products as part of their procurement process).

Vulnerabilities can be discovered by researchers either in the private sector or academia or by malicious actors with a motive for profit, or to conduct a targeted attack for espionage or other purposes. Most vendors[2] support the use of ‘responsible vulnerability disclosure’ practices in which researchers inform the vendor about newly discovered software vulnerabilities and delay public disclosure to an agreed time to allow the vendor time to develop an appropriate software fix (patch).

Responsible behaviour by researchers could be promoted, for example by contacting the affected company first rather than going public before a solution is available.

Patching is one way to mitigate against malware, but it is a reactive measure. Building security into the process for developing software would likely be a more effective and comprehensive long-term solution. Software needs to be developed correctly the first time to minimise the occurrence of security defects. The time frame between the discovery of a vulnerability and the time of its exploitation is shrinking.

Increased efforts could be made to develop software that resists compromise through layered protections and separation of privileges. The use of security reviews/validation methodologies for software products could also be promoted, where appropriate.

Governments are large buyers of information systems and software can play a role in fostering the production and procurement of secure systems.

Governments could encourage the building of security in the development and production of software. They could also take advantage of their procurement of software to foster the development of more secure software products.

- Awareness raising and education (*e.g.* further efforts should be made to improve online users awareness of the risks related to malware, and of the measures they should take to enhance the security of their information systems).

Many websites and resources exist to help end users and SMEs secure their information systems but few of those programmes specifically address and explain the problems of malware.[3] Also, the number of resources can be overwhelming to users as information and guidance can vary from entity to entity. Furthermore, some advice is inconsistent and may be inadequate in dealing with the rapidly changing nature of the threat. For example, advice that implies that the only necessary countermeasure is keeping one's anti-virus patches up to date is inadequate.

Awareness efforts could continue to strive to provide information in plain language so it can be understood by all participants, particularly those who have little or no technical knowledge or understanding. Given the continually changing nature of malware, any awareness activities would need to be regularly updated or revised so that they remain effective. This would help to improve home users and SMEs' online behaviour and practices with a view to improve their ability to protect themselves from malware.

- The possibility to include security and abuse management in registrar accreditation procedures and contracts.
- Standards and guidelines (*e.g.* update of security manuals such as the IETF Security Handbook should be encouraged to include new challenges such as those presented by malware).

Standards, guidelines and good practice are important tools for the security community. Those that are specific to malware or targeted at communities with responsibility to fight malware are particularly important to ensure a comprehensive solution to the problem. For example, the Internet Engineering Task Force's Security Handbooks which provide guidance for ISPs and users could be revised and updated to account for the changing nature of malware.

Efforts could be made to continually develop and update standards, guidelines and good practice resources.

- Research & Development (*e.g.* malware detection and analysis, security usability – how people interact with machines, software and online resources).

While this report does not attempt to examine the activities of the research community, it is important to recognise their importance in combating malware. Both government and the private sector have a role in funding and conducting research and development (R&D) on a range of information technology topics, including security risks.

Public and private sector R&D programmes focused on the security of information systems and networks could also consider malware.

Measuring the malware problem

This element could examine and foster efforts to more accurately and effectively measure the existence and impacts of malware.

Many entities track, measure and sometimes even publish data on their experience with malware and related threats.[4] However, vendors, CSIRTs, and the business community all have different data and ways of measuring the magnitude of the malware problem and its associated trends. Furthermore, there are many types of malware and little consistency of naming conventions in the technical community for identical types of malware. While existing data is helpful in understanding parts of the malware problem, it is not easily comparable in real and absolute terms.

Efforts should be made to more accurately and consistently catalogue, analyse, and measure the existence of, affects from and impact of malware.

Better policies and practices

Whois data is an important resource for attributing incidents of malware, and therefore it should remain accurate and accessible to law enforcement.[5] Furthermore, malicious actors often abuse domain name registration policies, such as ICANN's "add-grace period" or the minimal information requirements set out by some domain name registrars (DNRs), to avoid detection by authorities.

Domain name registrars could review their domain name registration policies with a view to preventing, through measures such as more stringent registration requirements, the potential abuse of the domain name system, while preserving privacy.

There are numerous DNRs that all have different policies and practices for addressing malicious online activity. For example, there are 250 country code Top Level Domains (ccTLD) in the world that set their own policies, which are not necessarily harmonised or co-ordinated. These different practices and policies may result in a different outcome each time a DNR is asked to take action against malware.

DNRs could be encouraged to develop common codes of practice at the national and international levels in co-operation with other stakeholders.

As is the case with DNRs, there are thousands of ISPs that all have different policies and practices for addressing malicious online activity. ISPs are perhaps the best placed actors in the chain to help stop some types of malware attacks, such as DDoS and botnets sending spam.

While many ISPs are working to improve security policies, some tend to have a higher than average amount of malicious activity. These different practices and policies may result in a different outcome each time an ISP is asked to take action against malware, which impairs the ability to fight against malware in an effective and consistent manner**.**

ISPs could be encouraged to develop common codes of practice at the national and international levels in co-operation with other stakeholders.

Co-operation for improved response

This element could examine the following:

- Co-operation among CSIRTs (computer security incident response teams) (*e.g.* CSIRTs with national responsibility could share points of contact and work collectively to improve information sharing).
- Codes of practice (*e.g.* a common code of practice for ISPs could be developed at the national and global levels in co-operation with governments; likewise, a common code of practice for DNRs (domain name registrars) could be developed at the national and global levels in co-operation with ICANN, the Internet community as well as others, as necessary).

Information sharing is a critical element of effectively responding to malware; however, it is currently based on well-established, and often personal, bilateral relationships. Real-time sharing of statistics and other incident information between CSIRTs is limited, and CSIRT co-ordination with government varies according to each CSIRTs' scope of responsibilities.

CSIRTs with national responsibility could be encouraged to improve cross-border information sharing mechanisms for effective protection, detection and response against malware.

Personal contacts within informal trust networks enable the security response community to, for example, get an ISP to quickly act on a case of abuse. There is not one informal network, but rather several, which may be overlapping. An ISP may approach a contact at a national CSIRT in another country in order to get in touch with the relevant representative at an ISP in that country. These contacts are reciprocal. They are also contacted about abuse in their own network and are expected to act on that information. CSIRTs play a critical role as the first line of defence against attacks using malware. Possibly one important role of a national CSIRT would be to also be the formal Point of Contact (POC) for handling IT incidents affecting the government and to receive requests for mutual assistance across jurisdictions.

Efforts to establish CSIRTs around the world could continue, especially where they do not exist at the government or national levels, and consideration could be given to designating them as the Point of Contact for national co-ordination and international co-operation against malware.

Improved legal frameworks

Laws and regulations

International harmonisation/interoperation of cybercrime laws is essential. Widespread adoption of the Council of Europe's Convention on cybercrime may be effective in this respect. While 25 out of 30 OECD member countries have signed the Convention, only 9 of those 25 have actually ratified it. Furthermore, out of 21 APEC economies only 3, which are also Members of the OECD, have signed the Convention and of those 3 only 1 has ratified the Convention. The Convention provides a framework for co-operation and is a general commitment to co-operate internationally against cybercrime.

In addition to ratifying the Council of Europe's Convention on Cybercrime, Parties to the Convention could endeavour to anticipate future cyber-threats, and further efforts to develop more detailed co-operative legal frameworks.

Strengthened law enforcement

This element could examine the following:

- Government efforts to provide mutual assistance and share information for the successful attribution and prosecution of cybercriminals.
- Co-operation between CSIRT teams and law enforcement entities.

Resources necessary for specialised cybercrime law enforcement agencies to be able to investigate and prosecute cybercrime in co-operation with other concerned public and private stakeholders. Malicious actors take advantage of the fact that many countries do not have adequate legal frameworks/cybercrime laws and cyber investigation capabilities. They also take advantage of the complex challenges faced by law enforcement and incident response when working outside their jurisdictions which are constrained by geographical boundaries. Cross-border information sharing among law enforcement entities is a critical element of investigating and prosecuting cyber criminals. While mechanisms such as the G8 24/7 Cybercrime Network provide for points of contact among such law enforcement entities, it is unclear how such networks co-operate among themselves.

Because of the highly technical nature of malware, governments should foster regular training for judges, prosecutors and other law enforcement officials.

Malware analysis can play an important role in recovering evidence and generating leads for law enforcement to investigate cybercrime. Malware analysis is often conducted using methods such as hard drive imaging, "real-time" forensics, antivirus testing, and reverse engineering (CERT Coordination Center, 2007). In some cases these practices may not be permitted under laws that protect intellectual property.

Review of laws that prohibit reverse engineering malware could be considered for law enforcement and research purposes, with appropriate safeguards for the protection of owners of intellectual property.

There may be tensions between the protection of privacy and actions to fight malware. For example, CSIRTs may need to share information, such as an IP address, among themselves and with ISPs. However, IP addresses may be considered as personal data in some countries. This may present challenges for sharing the information which may in turn hinder the efforts to, for example, dismantle botnets and conduct investigation into the malicious activity.

Data protection laws could be applied in a way that does not prohibit the sharing, with the appropriate safeguards, of IP addresses and other information that might be necessary for fighting malware.

Technical measures

This element could examine the following:

- Technical measures such as filtering, DNSSEC, sinkholing and many others could be examined to understand how they would help fight malware.
- How users might be provided with better tools to monitor and detect the activities of malicious code, both at the time when a compromise is being attempted and afterwards.

Malware presents complex technical challenges and therefore solutions to combating it need to be supported by technical measures, such as filtering, which may be an effective way to minimise the amount of illegitimate traffic on the network. Some examples of existing technical solutions and resources are provided in Chapter 8.

Further efforts to develop and implement effective technical solutions to detect, prevent, and respond to malware could be encouraged.

Users could be provided with better tools to monitor and detect the activities of malicious code, both at the time where a compromise is being attempted and afterwards.

The economics of malware

This element could examine the following:

- How to strengthen existing security-enhancing incentives of market players.
- Introduction of security-enhancing incentives through alternative forms and levels of legal rights and obligations to the different stakeholders.
- Efficiency of measures to internalise externalities by market players other than those generating the externality.

An economic perspective on malware would provide policy makers and market players with more powerful analysis and possibly a starting point for new governmental policies related to incentive structures and market externalities.

The following could, for example, be topics for further exploration:

- Effectiveness and economic effects of assigning alternative forms and levels of legal rights and obligations (*e.g.* liability) to the different stakeholders. This would include legal constraints for ISPs to monitor and manage their networks (*e.g.* related to privacy, 'mere conduit', 'safe harbour' provisions).
- Effectiveness and economic effects of blacklisting on ISP and end user security.
- Effectiveness and economic effects of global measures to strengthen law enforcement and collaboration in the area of malware.
- Effectiveness and economic effects of technological solutions to the problem of malware (*e.g.* 'security moving into the cloud' and 'tethered devices' for end users).
- Strength of reputation effects and other feedbacks in mitigating the problem of information security.
- Efforts to quantify the magnitude of the overall social externality due to lack of trust in the e–commerce system (growth effects, GDP impact).
- Better assessment of the strength of the trade-offs between usability, availability, functionality, performance, cost and security.
- Malware in next-generation networks and system architectures (*e.g.* more mobile, EoIP-everything over IP-networks, Web 2.0).
- Obstacles to and means to enhance incentives for information security of individual users.

Global co-ordination and cross-border co-operation

This element could examine the following:

- The cross-cutting need for information sharing, co-ordination and cross-border co-operation.
- Suggestions for disseminating the anti-malware guidance at the global level and following up on its implementation.

All of the previously mentioned areas for action illustrate the cross-cutting need for information sharing, co-ordination and cross-border co-operation. However, the communities of actors described above do not always collaborate in an effective manner to combat malware. Information sharing and co-ordination among the private sector, the government and other stakeholders is not always adequate to detect, respond, mitigate and take appropriate enforcement measures against malware. This can be at least partially attributed to the fact that no comprehensive international partnership for collaboration against malware does yet exist despite the significant work underway. (See Chapter 8 for examples of existing international co-operation).

A more holistic approach involving an integrated mix of policy, operational procedure and technical defences could be considered to ensure that information sharing, co-ordination and cross border co-operation are effectively integrated and addressed.

Only a holistic approach involving an integrated mix of policy, operational procedure and technical defences can ensure that information sharing, co-ordination and cross-border co-operation are effectively integrated and addressed.

The success of such a global "Anti-Malware Partnership" would require active engagement from all participants. Such an effort, however, would demonstrate significant advances in the international community's ability to overcome obstacles to addressing a global threat like malware through global co-ordinated action.

Conclusion

There is no simple solution to the complex problems presented by malware. The openness of the online environment and the distributed nature of the Internet while important factors for growth and innovation, also present challenges for securing information systems and networks. Malware has the potential to adversely affect any and all Internet users from enterprises to governments to end users. While malware often propagates through the Internet, it is important to remember that it is software which can be introduced into Internet connected and non-Internet connected computer systems. Malware whether used directly, or indirectly, to conduct malicious activity online erodes trust and confidence in the Internet and the digital economy.

The 2002 *OECD Guidelines for the Security of Information Systems and Networks* provide a list of broad information security principles all of which are relevant and applicable to the fight against malware. The nine principles (Awareness, Responsibility, Response, Ethics, Democracy, Risk assessment, Security design and implementation, Security management, Reassessment) concern participants at all levels, including at the policy and operational levels. *The Guidelines* can and should be applied to the challenges raised by malware today.

The rapidly evolving nature of malware makes international co-operation essential to addressing the problem. This co-operation should be supported and enhanced by accurate and quantitative measurement of the problem and the underlying economics at play. While this paper details many of the problems presented by malware, it is only a first step in moving towards a solution. A holistic and multi-stakeholder proactive approach is needed to take advantage of all opportunities for improvement across the various communities addressing malware.

Notes

1. Information available at *www.w3c.org*.

2. As an example, Microsoft is one. See *www.microsoft.com/technet/community/columns/secmgmt/default.mspx*.

3. Industry organisations, such as APACS, have reported no reduction in the level of phishing due to awareness campaigns and public figures highlighting the problems and scale of the attack. APACS (2006) Vulnerability and threat assessment of authentication mechanisms used for Internet based financial services – 2006 review, page 3 and 4.

4. See Annex A. Background Data on Malware.

5. Civil liberties groups have recommended that ICANN limit the use and scope of the Whois database to its original purpose and to establish its policies based on internationally accepted data protection standards. Public availability of Whois data may also conflict with the EU Data Protection Directive, which limits access and collection rights to the database's original technical purposes.

Annex A. Background Data on Malware

Overview

Although malware as we know it today is a relatively new phenomenon compared to the early days of worms and viruses, it is growing and evolving at impressive rates. Trends in data show that while the categories of malware used to conduct malicious activity (*i.e.* virus verses Trojan) change and evolve over time, the use of malware is steadily increasing.

Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs), software and anti-virus vendors, and more generally security companies are examples of entities that track and monitor the existence of malware. While the data provided below is helpful in understanding elements of the malware problem, it is not easily comparable in real and absolute terms and thus this paper does not attempt to make comparisons or draw conclusions across disparate sets of data. This section is primarily intended to demonstrate the type of information available and different analytical perspectives from the organisations listed below.

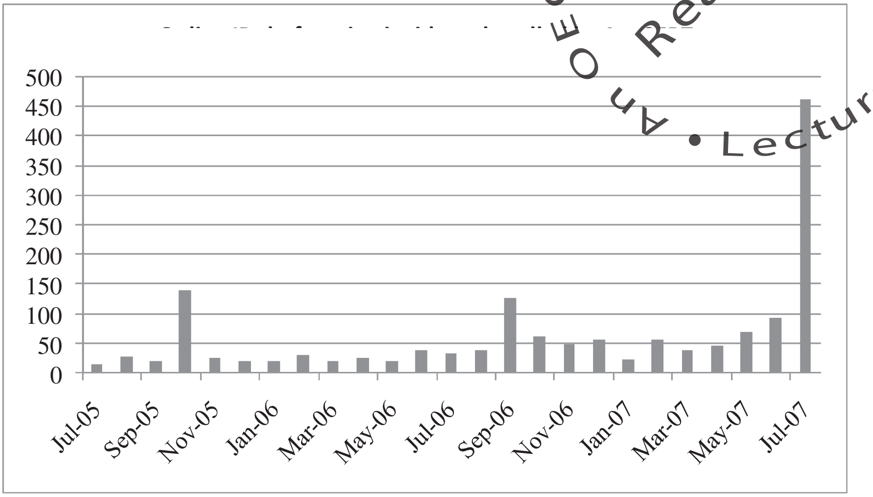
Data provided by CSIRTS

AusCERT

AusCERT is the national Computer Emergency Response Team for Australia. AusCERT provides computer incident prevention, response and mitigation strategies for members.

In Figure A.1, each incident represents a single unique URL or domain name that is hosted by one or more compromised computers for the purpose of stealing sensitive information and access credentials from other computers. Multiple incidents can be associated with one attack, which is the set of compromised computers needed to launch the attack and collect the stolen data. The number of IP addresses associated in a single incident and a single attack is variable but can range from 1 to around 100.

Figure A.1 Online ID theft Trojan incidents handled by AusCERT



Source: AusCERT (2006).

Figure A.1 does not include specific compromised hosts involved in any single attack or incident – only URLs and domain names. Nor does this depict the number of computer infections (compromised hosts) that occur due to each attack of which there are generally many hundreds or thousands.

The high figures for July 2007 are due to the storm Trojan (often incorrectly referred to as a worm). It does not automatically propagate and has P2P botnet C&C functionality, *inter alia*.

CERT Brazil (CERT.BR)

CERT.br is a national CERT which collects public statistics on the incidents that are reported to them voluntarily. For example, a home user can report when he/she received an e-mail that is clearly a fraud attempt, with a link to a malware executable. CERT.br tests to see if the executable is still on line and then reports the occurrence to the host of the site. They also submit a sample of this malware to several antivirus vendors to ensure that it has been widely detected.

CERT.br data is divided into four categories: intrusions, web attacks, denial of service, and fraud.

Table A.1. CERT.BR Incident Reports

Year	Total number of incidents reported	Worm[1]	DoS	Intrusion[2]	Fraud[3]
2004	75 722	42 268	104	248	4 015
2005	68 000	17 332	96	448	27 292
2006	197 892	109 676	277	523	41 776

1. The worm category are reports received of worm/bot propagation, *e.g.* port scans of commons ports used by worms/bots to propagate (445, 135, 5900, etc). These reports are usually sent by firewall administrators and even home user using personal firewalls, etc. It is important to note that the worm category does not try to count machines infected by worms, but incidents regarding worm propagation attempts.

2. Intrusion, according to CERT.BR classification, is a system compromise – this is determined by the system owner/administrator and reported to CERT.BR. For example, a Linux server administrator sends CERT.BR a report saying his/her machine was compromised, a rootkit was found, etc.

3. The fraud category refer to various fraud types: copyright infringements, credit card fraud, traditional phishing and malware related fraud. The last one is the majority of the cases in Brazil.

CERT/CC, United States

The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University collects data on malware from public and private sources. Since 2006, CERT/CC has been collecting, analysing and cataloguing every piece of malware it is able to find that has been distributed via the Internet or which otherwise has found itself onto computer systems. While many malware artefacts have similar functionality, each one is considered to be a unique variant if it generates a unique MD5 or SHA1 hash function.[1] Therefore, some types of self-propagating malware such as viruses and worms which produce many thousands of identical replicas would be counted as a single variant.[2]

Hence the figures below from CERT/CC, while not necessarily complete, are nonetheless significant in their depiction of malware trends, which show an exponential increase in malware artefacts[3] from January 2006 to March 2007. From less than 50 000 in January 2006, the total number of artefacts rose to 350 000 in March 2007, as represented in Figure A.2 below. For each month of the same period, Figure A.3 represents the proportion of those artefacts that were newly discovered by CERT/CC. Although the increase is less steady in Figure A.3, the discovery of new artefacts reached an all time high in March 2007 up to 90 000.

Figure A.2 Total artefacts by month from January 2006 to March 2007

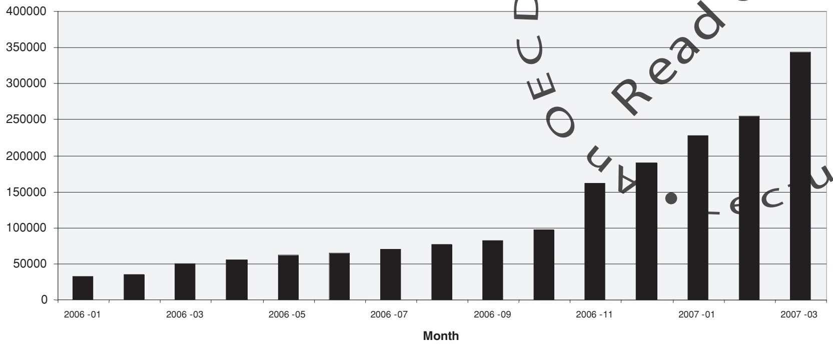
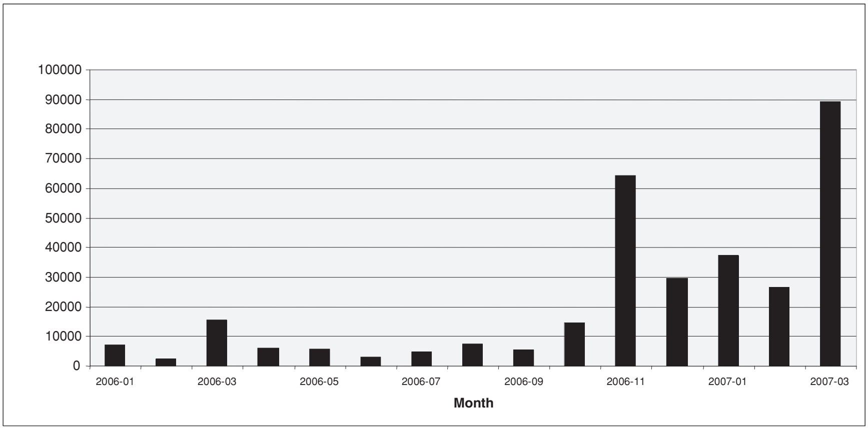


Figure A.3 New artefacts per month from January 2006 to March 2007

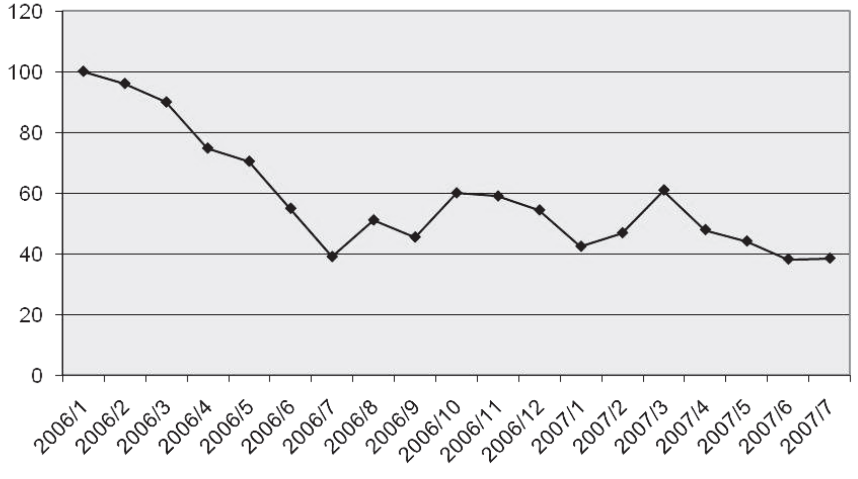


CERT-FI, Finland

CERT-FI is the Finnish national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. Figure A.4 represents the cases handled by CERT-FI Abuse Autoreporter system, their automated abuse case processor. The graph is cases / month, normalised to 100 = 1/2006.

Figure A.4 CERT-FI Abuse Autoreporter monthly case processing volume

(normalised 1/2006 = 100)



KrCERT/CC

KrCERT/CC gathers data from honeynets[4] and incidents reports. Between 2005 and 2006 data from both incident reports and honeypots showed a decrease in the number of worms and an increase in the number of Trojan horses from 2005 – 2006 (see Figures A.5 and A.6).

Figure A.5 Incident reporting to KrCERT/CC by month (2005-2006)

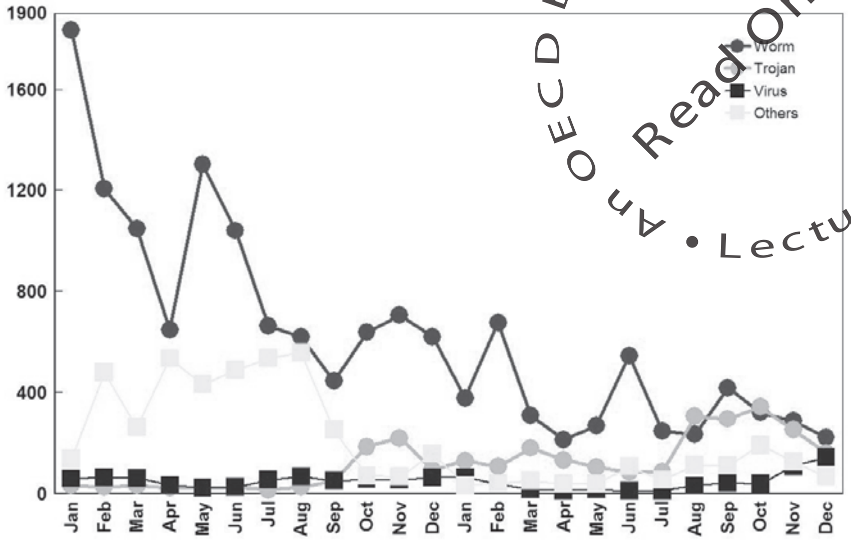
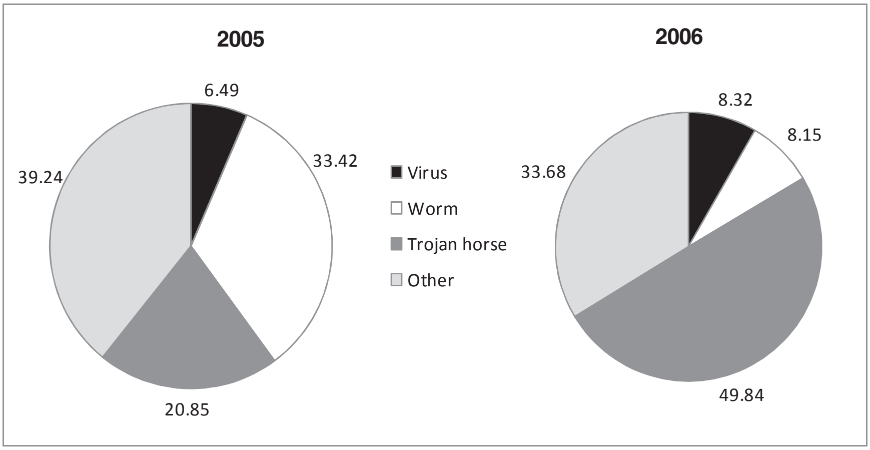


Figure A.6 Information gathered from KrCERTr honeynets

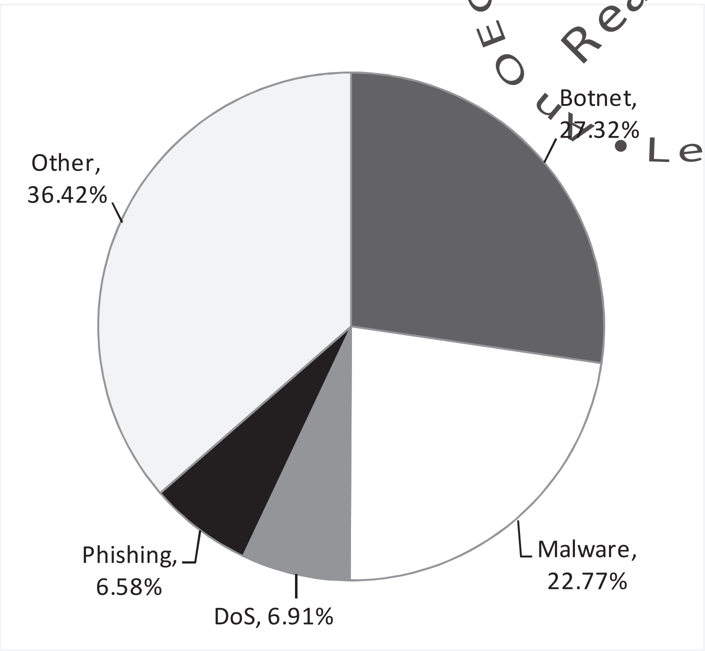


NorCERT, Norway

The Norwegian Computer Emergency Response Team (NorCERT) co-ordinates preventative work and responses against IT security breaches aimed at vital infrastructure in Norway. NorCERT is a department of the

Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet – NSM).

Figure A.7 Incidents handles by NorCERT in 2007

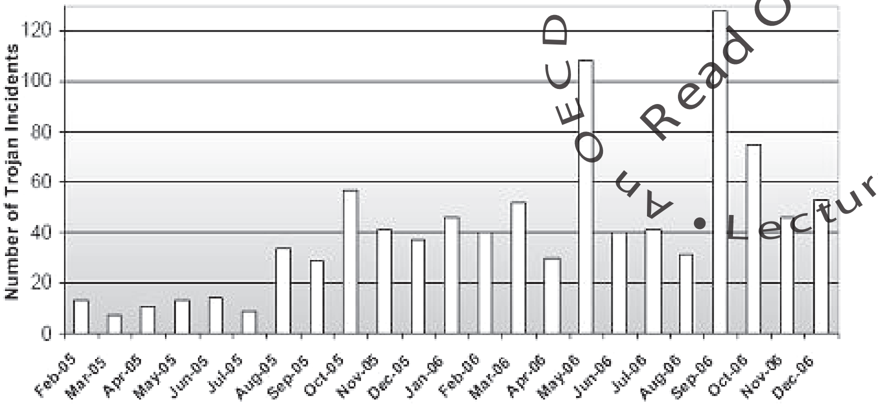


Data from software and anti-virus vendors

Association of payment

APACS, the UK payments association, is a trade association for institutions delivering payments services to end customers. It enables the forum to address co-operative aspects of payments and their development. It is also the main industry voice on issues such as plastic cards, card fraud, cheques, e-banking security, electronic payments and cash. Working Groups address co-operative areas such as developing authentication solutions and responding to attacks on e-banking customers. Figure A.8 tracks the number of Trojan incidents targeting UK banks from February 2005-December 2006.

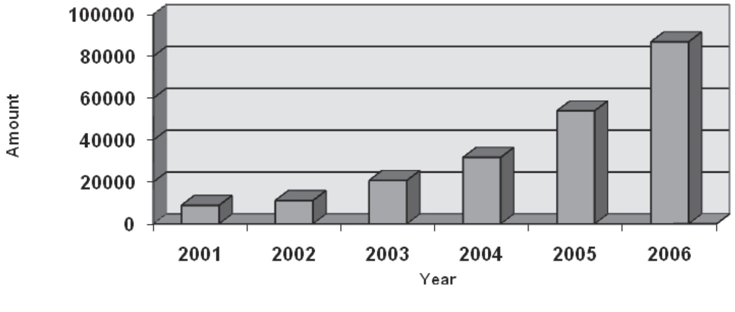
Figure A.8 Trojan Incidents targeting UK banks



Kaspersky Lab

Kaspersky Lab is an international information security software vendor. Kaspersky Lab is headquartered in Moscow. Kaspersky labs reported an exponential increase in previously unknown malicious programmes from 2001-2006, as illustrated in Figure A.9. They also reported a steady increase in the number of Trojan spy programmes designed to steal information from users' online accounts (Kaspersky Labs, 2006).

Figure A.9 Increase in the number of new malicious programmes



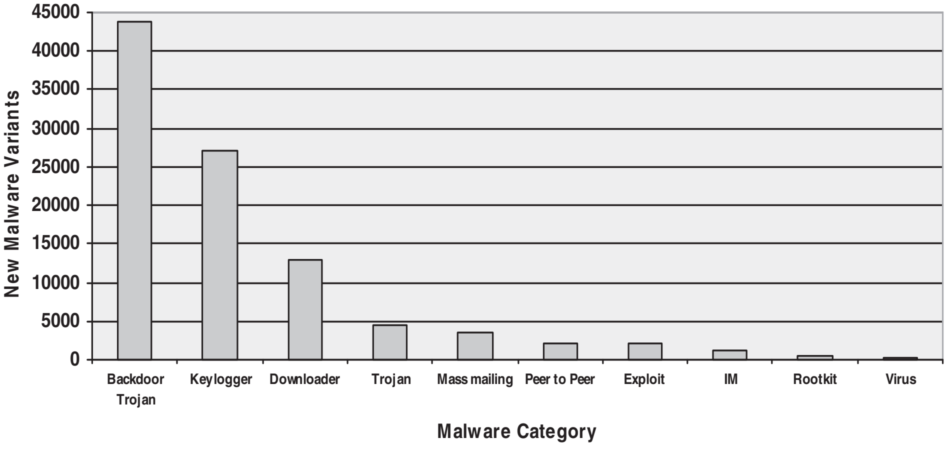
Source: Mashevsky, Y. (2007).

Microsoft

Microsoft gathers data from several anti-malware products and services deployed on information systems running Microsoft products. Based on activity observed from January to June 2006, Microsoft reported the existence of more than 43 000 new malware variants between January and June of 2006 (Microsoft, 2006a). This can at least partially be attributed to the public availability of malware for purchase on the Internet; it is easier for attackers to modify a piece of existing malicious code rather than create a new "family" of malicious code.

Microsoft also reported that among new malware variants backdoor Trojans accounted for the highest number (see Figure A.10). The figures demonstrate that the four most common categories where new variants have been created were of the non-self-propagating varieties, which are typically associated with smaller scale cyber attacks aimed at illicit financial gain, particularly financial fraud.

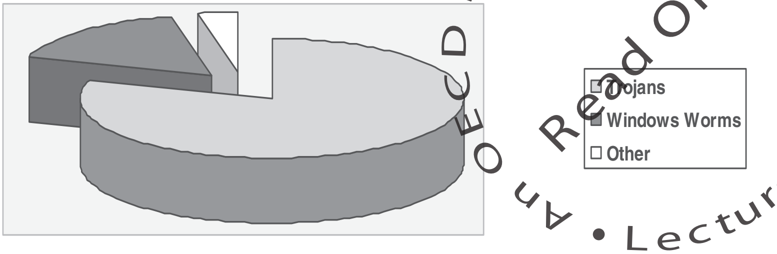
Figure A.10 Microsoft Malicious Software Activity from January - June 2006



SOPHOS

SOPHOS gathers data from 35 million users in 150 countries that deploy its products. SOPHOS attributed 80% of all detected malware in 2006 to Trojans (see Figure A.11).

Figure A.11 Trojans verses Windows Worms and Viruses in 2006



Source: Supra Sophos (2007a).

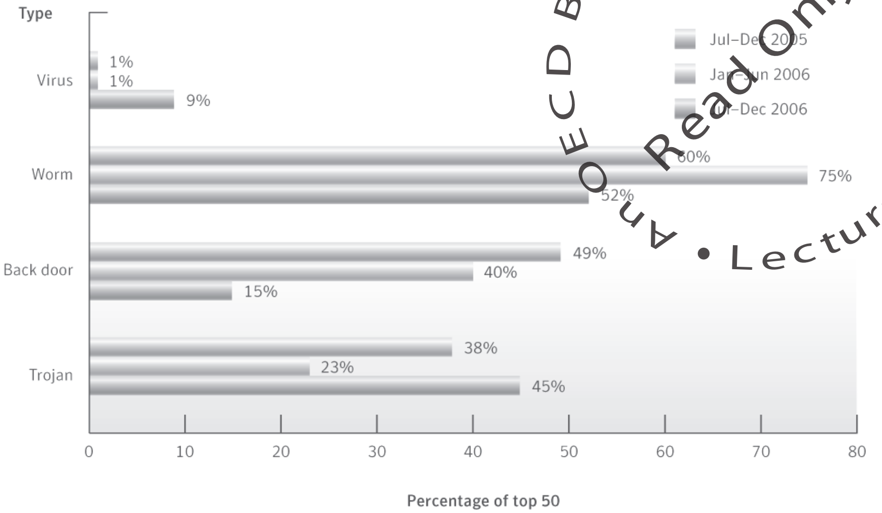
Symantec

Symantec gathers information from 40 000 registered sensors in 180 countries, 120 million desktop computers, and gateway and server antivirus installations, and 2 million decoy accounts in the Symantec Probe Network. Symantec operations are conducted from four security operations centres and eight research centres. Symantec software products are deployed on more than 370 million computers or e-mail accounts worldwide.

Recently, Symantec reported a decrease in the amount of worms[5] and backdoors and an increase in the amount of viruses and Trojans.

In addition to this data, the Symantec Corporation reported an increase in previously unseen malware, or new families. Between July and December 2006, Symantec honeypots discovered 136 previously unseen malware families, an increase of 98 from the previous 6 months (Symantec, 2007). It is important to note that while information gathered from honeypots and honeynets is useful, it is not necessarily representative of a global trend.

Figure A.12 Malicious code types by volume



Source: Symantec (2007).

Observations on the data

The data on malware presented above comes from a variety of very different and incomparable sources (national CSIRTs, software vendors, and security vendors). The definitions, types of incidents, type of damage, time frame, and scope are not harmonised across these various organisations and therefore it is necessary to be prudent in comparing such disparate data.

However, it is more or less possible to highlight certain tendencies that seem to be shared: *i*) an significant and noticeable rise in security incidents related to malware ; and, *ii*) Trojan malware becoming more and more prevalent when looking across types of malware. As has often been reported, there are fewer serious outbreaks of worms and viruses and thus a large part of the increase in malware variants can generally be attributed to non-propagating varieties which usually have a more harmful payload/functionality and tend to be financially motivated.

An agreement by certain stakeholders interested in measuring malware on definitions and common methodology for gathering data would help in more systematically evaluating the extent of this reality and its role in the ever changing universe of the Internet and ICTs.

From some of the data, it is possible to summarise and highlight several points to demonstrate that the problem of malware is becoming more and more significant.

Box A.1 Summary of sample data on malware

Table A.1 Total number of incidents reported ~ + 225%.

Figure A.2 Total artefacts in the last year ~ +250%.

Figure A.6 Decline of Worms related incidents ~ -25%/; Increase of Trojan related incidents ~ + 30%.

Figure A.11 Malicious programmes increase by 800% in the last 5 years.

While it is true that many attack trends are increasing, it is unclear how these trends relate to the overall damage caused of malware. Detecting a higher number of Trojan variants does not necessarily mean that there is more damage. It could also be a response to improved security defenses. Similarly, signalling that large-scale botnets are shrinking in size does not necessarily mean that the counter measures are effective. It might be that attackers have found smaller and more focused botnets to be more profitable. In short: because malicious attack trends are highly dynamic, it is difficult to draw reliable conclusions from the trends themselves.

Notes

1. Attackers often generate a new malware variant from an existing piece of malware by simply changing the manner in which the code is 'compressed and packed', rather than changing the malware code itself. For example, see: *http://us.trendmicro.com/us/threats/enterprise/glossary/c/compression/index.php*. New variants produced in this manner are not each given a new CME number. Multiple variants, which are considered to be identical in functionality and form will have the same CME number, whereas even small variations in malware byte code will produce a new CME number. See: http://cme.mitre.org/cme/process.html

2. This approach is important as counting each infection from a single large worm or virus outbreak can skew the results and does not reflect the actual level of development of new variants by many attackers specifically in order to evade detection by anti-virus products.

3. An artefact is a file or collection of files which may be used by adversaries in the course of attacks involving networked computer systems, the Internet, and related technologies.

4. In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated, (un)protected and monitored, and which seems to contain information or a resource that would be of value to attackers. Two or more honeypots on a network form a honeynet.

5. This drop can largely be attributed to the decline in reports of major worms such as Sober.X, Blackmal.E, and Netsky.P75 since the first half of 2006.

Annex B. Research Design for Economics of Malware

Our evaluation started with an exploration of the incentives at work in the individual organisation and those related to the decisions of other competing or complementary organisations. The reliability of the information is increased if interdependent stakeholders present compatible pictures of the relevant incentives and their effects. Attempts were made to interview several organisations in each segment of the value chain to develop narratives that are as coherent as possible. In a subsequent analytical step, these individual narratives were then integrated to assess the overall incentive structure of the sector and the resulting externalities.

Data collection

In the course of 2007, we conducted 41 in-depth interviews with 57 professionals from organisations participating in networked computer environments that are confronted with malware. Firms from the following components of the value net were approached:

- Internet Service Providers
- E-commerce companies, including online financial services
- Software vendors
- Hardware vendors
- Registrars
- Security service providers
- Different types of end users
- Governance institutions (regulators, consumer protection agencies, CERTs)

A full list of respondents can be found in Annex 5.A1. Our empirical effort extends the preliminary work on firms and end users (*e.g.* Dynes *et al.*, 2005; Camp, 2006; Dynes *et al.,* 2006; Poindexter *et al.*, 2006; *e.g.* Rowe and Gallaher, 2006).

The interviews were carried out using a semi-structured questionnaire, adapted for the specific situation of the interviewee. In each instance, we asked how the organisation was confronted with malware, what its responses were, what trade-offs were associated with these responses, and how the organisation was affected by the actions of other market players. As is common practice in the social sciences, we have treated all interview data as confidential, so as to enable the interviewees to share information with us as freely as possible. Consequently, no interviewee or organisation is identified by name in relation to specific data and all quotes have been approved by the respective individuals/organisations beforehand for publication. All statements in the report are based on interview transcripts and other documents supporting the findings. Although this limits the direct verifiability from readily available public sources, we felt that given the exploratory stage of research in this area, our approach would enable us to get better insights into market-sensitive economic data and decision making.

Scope and limitations

Before turning to the empirical findings, it is important to note the scope and limitations of this study. The global and heterogeneous nature of the ecosystem of Internet services implies that any study of incentives is almost by necessity an exploratory study. The limited time and budget available for this study allowed for a limited number of interviews in six countries. The majority of the interviews took place in the United States and the Netherlands, with additional interviews in the United Kingdom, France, Germany and Australia. The next section presents our findings for five of the market players we interviewed:

- We intended to also describe the incentives for hardware vendors Internet Service Providers
- E-commerce companies, including online financial services
- Software vendors
- Registrars
- End users

, but we were unable to secure sufficient interviews with hardware vendors to provide the basis for such a description. The examination of the incentives was based not only on interviews with the market players themselves, but also on conversations with people who have expertise on the current threats and governance of the ecosystem of information services, such as regulators, CSIRTs, ICANN, security services providers, and researchers.

While these interviews have proven to be highly informative, the findings drawn from them should be read with caution. First of all, it is reasonable to assume that the set of interviewees is influenced by some degree of self-selection. ISPs, for example, are more likely to respond favourably to an interview request about the economics of malware if they have security policies in place that are at least on par with other ISPs, if not better. That said, some of the organisations we interviewed are publicly known for a less than stellar track record with regard to security – which they often explicitly acknowledged during the conversations. Second, the empirical findings report on how stakeholders themselves describe what they are doing and why. In other words, we report on the perceptions of the interviewees, not some independent assessment of their actions and the factors driving them. Whenever possible, we did cross-check information provided to us against the information from other interviews and against publicly available data, such as security reports, surveys and research publications. Third, the interviews touch on many issues that concern proprietary or otherwise confidential data. Interviewees were not always able to share this data with us and if they were, we were constrained in reporting them. Fourth, and last, our interviews involved six different legal jurisdictions. Some incentive mechanisms are generic but others are context-specific. Our approach hence provided us with a sense of the degree to which certain findings were country-specific and therefore could not fully reflect the heterogeneity of all OECD members.

These circumstances make it more difficult to generalise our findings. However, very little empirical field work has been done in this area so far. In light of the rapidly increasing political attention given to the issue of malware and the policy initiatives currently under debate, this is a critical omission. Our study contributes to overcoming this omission. At the very least, it makes clear the urgency of developing a further-improved in-depth understanding of the economics of malware to increase the probability of policy interventions to succeed.

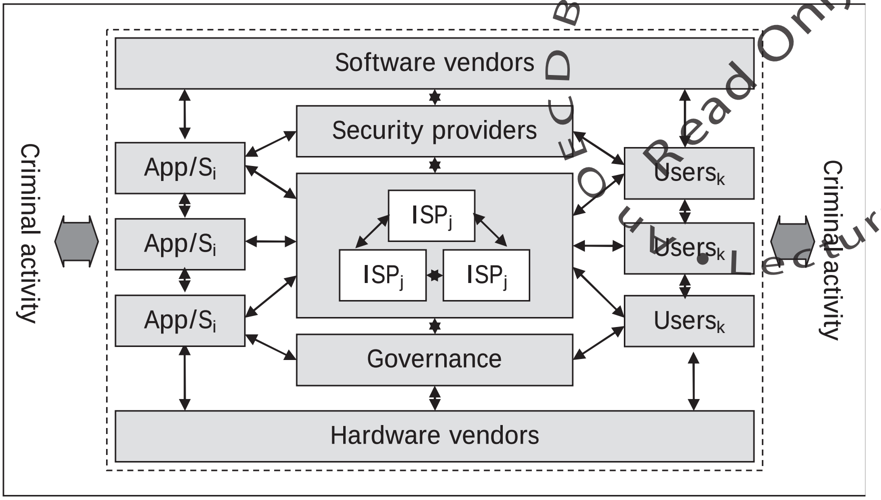
Annex C. A Framework for Studying the Economics of Malware

The information and communication technology (ICT) industries form a complex ecosystem, and their services permeate most other economic activities. Security problems and the related economic costs to society may have two roots: *i*) they are the outcome of relentless attacks on the information and communication infrastructure by individuals and organisations pursuing illegal and criminal goals; and *ii)* given an external threat level, they may be aggravated by discrepancies between private and societal costs and benefits, which are the outcome of decentralised decision making in a highly interrelated ecosystem. Both actors in the illegal and criminal realms, as well as legitimate participants within the information and communications system, respond to the economic incentives they face.

In this complex value net (see Figure C.1), economic decisions with regard to information security depend on the particular incentives perceived by each player. These incentives are rooted in economic, legal, and informal mechanisms, including the specific economic conditions of the market, the interdependence with other players, laws and regulations, as well as tacit social norms.

Within each participant's own purview and constraints each participant responds rationally to a variety of incentives, even though the available information may be incomplete. However, for the economic efficiency of the whole value system, it is critical that the incentives of the individual participants be aligned with the overall conditions required for societal efficiency. In other words, the relevant incentives should assure that the private costs and benefits of security decisions match the societal costs and benefits. In the case of differences between private and societal optimal outcomes, the prevailing incentive mechanisms should ideally induce adjustments toward higher social efficiency.

Figure C. 1 Information industry value net



App/S$_i$ ...	different types of application and service providers
ISP$_j$ ...	different ISPs
Users$_k$ ...	different types of users (small, large, residential, business)

Misalignment between private and social efficiency conditions may take several forms. In case of incomplete information, the perceived incentives of individual players may deviate from the optimal incentives. A related issue is the problem of externalities, systematic deviations between the private benefits or costs and the societal benefits or costs of decisions. Due to the high degree of interdependence, such deviations from optimal security decisions may cascade through the whole system as positive or negative externalities.

As the research on the economics of crime has illustrated, criminal activities may be analysed in a market framework. The activities in the market for cybercrime and cybersecurity are closely interrelated. Before the problem of incentives and externalities can be explored in more detail, we will, therefore, briefly explore the working of these markets and their linkages.

Market analysis of cybercrime

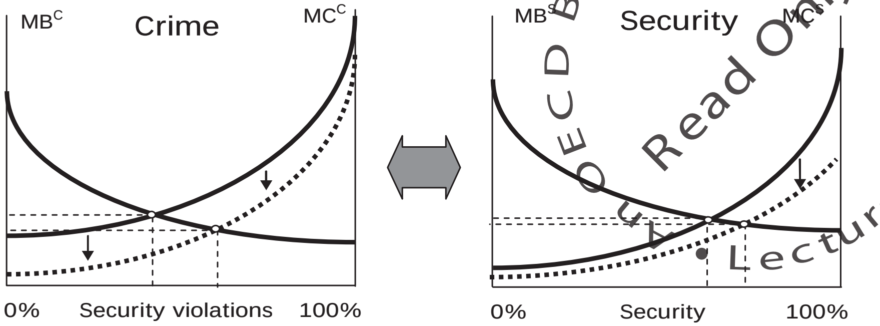
Figures C.2 and C.3 illustrate the interrelated nature of the markets for cybercrime and security. There are different ways to model the market for cybercrime. Becker (1968) and subsequent literature (see Ehrlich, 1996; Becsi 1999, for overviews) suggest using a supply and demand framework to study criminal activity. Franklin *et al.* (2007) also employ an economic framework to study an underground economy based on "hacking for profit." We chose a slightly different representation than these studies, based on marginal analysis. It is reasonable to assume that a higher level of security violations is only possible at increasing cost. Furthermore, it is likely that the additional cost will increase more than proportionally as the extent of security violations increases.

On the other hand, the marginal benefits of additional security violations are a decreasing function of the level of violations. This is an expression of the fact that the most lucrative crimes will be committed first, and that additional criminal activity will only yield lower marginal benefits. Criminals will extend their activities until the marginal cost of additional security violations approximates their marginal benefits. The magnitude of the benefits and costs of crime is dependent on a number of variables, some of which are affected by private and public measures to enhance security. A closer examination of these factors allows comparative assessments of market outcomes. It also sharpens understanding of the principal opportunities to intervene in the market to reduce cybercrime.

Technological change, the increased specialisation and sophistication in the production of malware, and the globalisation of the information and communication industries have all reduced the marginal cost of crime.[1] In turn, this cost decrease has dramatically expanded the supply of crime, as people from countries and regions with low opportunity cost of labour (which increase the net benefits of crime) join criminal activities. Such reduced marginal costs of security violations will shift the marginal cost of crime schedule downwards. Assuming that other things, especially the benefit relationship, remain unchanged, reductions in the marginal cost of crime will result in a higher level of security violations and vice versa.

Technological change and globalisation have also increased the benefits of crime. For example, the wider reliance on e-commerce and credit card transactions has increased the opportunities to exploit technical and personal security loopholes. The globalisation of the Internet has also enabled criminals to reach a larger number of potential victims. These changes shift the marginal benefit curve upwards (not captured in Figure C.2). Other things being equal, this increase in the marginal benefits results in a higher level of security violations. The presence of both effects explains much of the increased level of activity of security violations. In principle, however, opposite shifts of the marginal cost and benefit curves may be achieved by appropriate measures.

Figure C.2 Markets for crime and security



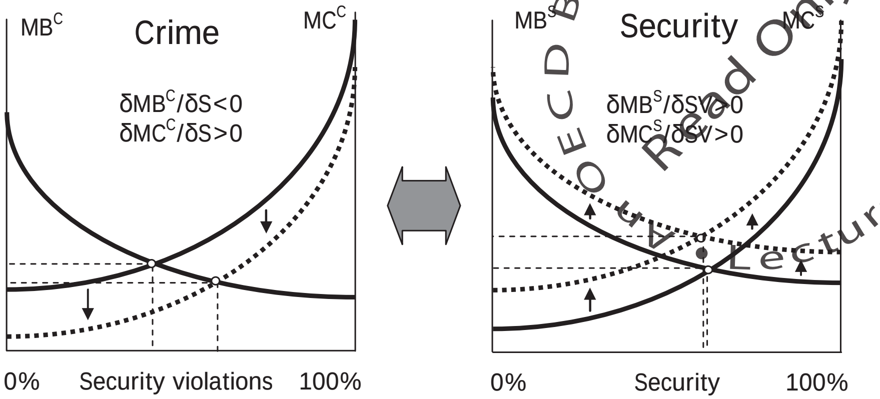
MB^C … marginal benefits of crime
MC^C … marginal costs of crime
MB^S … marginal benefits of security
MC^S … marginal costs of security

The market for cybersecurity

The market for security can be analysed using a similar approach. It is reasonable to assume that higher levels of security can only be achieved at higher marginal costs. On the other hand, the marginal benefits of security will decrease. Unless the benefits exceed the cost throughout, the resulting optimal level of security will be below 100%, at least on an aggregate level.[2]

Changes in the costs of providing security and the benefits of having security will shift the marginal cost and benefit schedules and affect the market outcome. A reduction in the cost of security, for example, due to the availability of more efficient and cheaper filtering software or a new network architecture that might reduce the propagation of malware, will (other things being equal) result in a higher level of security. Likewise, higher benefits of security, perhaps because of the utilisation of more mission-critical applications, will (other things being equal) result in a higher level of security. However, such initial changes may result in subsequent adjustments by other actors, who might reduce their expenditure for security in response, leaving the overall effects on the resulting security level ambiguous at best (see the arguments in Kunreuther and Heal, 2003).

Figure C. 3 Markets for crime and security



MB^C … marginal benefits of crime

MC^C … marginal costs of crime

MB^S … marginal benefits of security

MC^S … marginal costs of security

δMBC/δS<0 expresses the changes of the MBC curve in response to a change in the level of security S. The negative sign implies that the marginal benefits of crime move in the opposite direction from marginal changes in security, *i.e.* increased security reduces the marginal benefits of crime, all other things being equal.

The interaction of cybercrime/cybersecurity

The markets for cybercrime and security are highly interrelated (Figure C.3). Activities in the market for cybercrime affect the market for security and vice versa. Most likely, an increased level of security violations will increase the marginal benefits and the marginal costs of security, shifting both schedules upwards. On the contrary, a lower level of security violations resulting from the market for crime will shift both schedules down. On the other hand, variations in security will have corresponding effects on the market for crime. Increased security will increase the marginal cost of security violations, and it will reduce the marginal benefits of crime.[3] The net impact on the overall level of security is difficult to predict and will depend on the relative strengths of variations in security violations on the costs and benefits of security. A higher level of security violations could result in a lower level of security, an unchanged level of security, or even a higher level of security. *Without any specific policy intervention, the interaction between the two markets may resemble an arms race.*

There is an asymmetry in the effects of one market on the other. On the one hand, an increased level of security violations may, or may not, affect the level of security. But for all actors it will likely result in higher costs for maintaining a certain level of security. On the other hand, a higher level of security will induce changes in the market for crime in that it will increase the marginal cost of security violations and, at the same time, reduce the marginal benefits of crime. Both effects will mutually reinforce each other, thus contributing to a lower level of security violations. Since parameters in each of the markets change continuously, the outcomes of the resulting dynamic mutual adjustment are difficult, if not impossible, to model, although the directions of change seem to be robust.

Benefits of market analysis

A market analysis framework can give high-level insights into the measures available to influence overall outcomes. Such measures can target the market for cybercrime and/or the market for security. Measures such as increasing the cost of cybercrime by increasing the associated penalties, strengthening national and international law enforcement, and increasing the difficulty of registering and maintaining fraudulent domains and websites, will affect the market for crime directly and also have repercussions on the market for security. Most likely, such measures will reduce the overall level of security-related costs. For reasons discussed above, it is less certain that such measures will increase the level of security, since accepting a certain level of insecurity is economically rational.

Measures affecting overall incentive compatibility in the security markets range from forms of industry self-regulation to forms of co-regulation and government intervention. They encompass a wide spectrum of measures, such as: requiring that security features are enabled by default; recommendations to ISPs to adopt best practices with regard to security on their networks; information campaigns to alert users to security risks; and changes in the ways domain names are registered. None of these measures is a panacea, but they help better align individual incentives with societal efficiency requirements.

Economic incentives: what they are, how they work

Economic incentives are the factors that influence decisions by individuals, as well as organisations. A close examination of the incentives that information industry participants have for taking actions against malware is thus critical to a full understanding of the economics of malware.

Such actions include investment in security, investment in technical means to prevent, or at least control, problems caused by malware, response sequences in case an intrusion has happened or an attack is unfolding. The relevant set of incentives is most likely different for each stakeholder. Hence, we attempted to get a detailed account of the incentives as perceived by participants in the information industry. Moreover, the incentives may complement each other, they may form a trade-off, or they may even work at cross-purposes. An important goal of our analysis was, therefore, to examine the aggregate interaction of the individual incentives faced by stakeholders at the sector level. Since systems of incentives have many feedback loops, it is typically very difficult to determine the net effect of a system of incentives. At this initial stage of the field research project, we used a qualitative approach.

Economic incentives shape decisions in for-profit commercial firms, non-profit social groups, public and private sector governance institutions, as well as not-for-profit forms of production and collaboration. Incentives are often classified in monetary (remunerative, financial) and non-monetary (non-financial, moral) terms. Financial incentives include factors such as tying the salary of an employee to corporate performance, the ability to make a super-normal profit by pursuing a risky innovation, or the bottom line effects of potential damage to a firm's reputation. Non-financial incentives encompass norms and values, typically shared with peers, and result in a common understanding as to the right course of action or the set of possible actions that should be avoided in a particular situation. Financial incentives typically connect degrees of achievement of an objective to monetary payments. Non-financial incentives work through self-esteem (or guilt) and community recognition (or condemnation).

In practical decision making, incentives can be seen as the motives for selecting a specific action or the rationales for preferring one course of action over another. As the discussion of reputation effects illustrates, it is sometimes necessary to distinguish between short-term and long-term effects. Characteristic features describing incentives are their power (low-powered to high-powered) and directionality (positive or negative relation to goals of decision).[4] An important question is the relation between the structure and power of the relevant incentives and the objectives of decisions.

The full set of incentives at work typically consists of a bundle of specific, more narrowly defined, incentive mechanisms. These incentive mechanisms may work in the same direction or conflict with each other. If feedback loops between incentives exist it is often difficult to determine their overall net effect. However, it is possible to establish the effect of a single incentive mechanism under the methodological assumption that all other factors remain constant (*ceteris paribus*). For example, for software vendors the reputation mechanism *ceteris paribus* works toward increased information security but potential first-mover advantages in the information industries may, *ceteris paribus*, lower the incentives to invest in information security.

Incentive-compatibility refers to a situation in which an incentive is structured in a way as to contribute to the stated goals of an individual or an organisation. To assess incentive compatibility, the direct and indirect links between an incentive mechanism and the objective being pursued will have to be examined. Incentive compatibility may exist at the level of a single incentive mechanism, the bundle of incentives at work for a specific stakeholder, or the entire sector under consideration. Given the potential for trade-offs and even direct conflicts between incentives, incentive compatibility is much more difficult to ascertain at the level of stakeholders and the industry at large. It is a particular challenge in an industry as highly inter-related as advanced information and communication industries are. To be affected by an incentive mechanism, individuals need to be cognizant of its existence, its directionality, and its power. Incentives that exist on paper but are ignored by the decision makers must either be seen as zero-powered or as irrelevant incentives. Therefore, it is possible to reveal the existing incentive structures of the stakeholders in the information value net by asking experts and decision makers for an in-depth account.

Externalities

Externalities are forms of interdependence between agents that are not reflected in market transactions (payments, compensation). Which phenomena are identified as externalities depends to a certain degree on the specification of legal rights and obligations in the status quo. If these rights and obligations are only vaguely defined they may need clarification by legislatures, courts and in private contractual agreements.[5] If such clarification is afflicted with transaction costs, rational individual actors affected by the externalities will not internalise them if these costs exceed the potential benefits of internalisation. In this case, only a collective actor (*e.g.* a business association, government) may be able to address these uncompensated externalities.

In the formulation of the mainstream economic model, these interdependencies lead to deviations from a socially optimal allocation of resources. Negative externalities result in an overuse or overproduction compared to the social optimum whereas positive externalities lead to an underuse or underproduction of the resource afflicted with the externality (Friedman, 2002). External effects are often classified according to the agents that are involved. Frequently, producers and consumers are distinguished, yielding a two-by-two matrix of producer to producer,

producer to consumer, consumer to producer and consumer to consumer externalities (Just *et al.*, 2004).

An alternative typology distinguishes between technological and monetary externalities (Nowotny, 1987, p. 33). Technological externalities are said to exist if, at constant product and factor prices, the activities of one agent directly affect the activities of another. Pecuniary externalities exist, if the activities of one agent affect the prices that need to be paid (or may be realised) of other agents. Early contributions to the subject, for example, by Marshall (1920) or Pigou (1932), treated externalities as an exception, a rare anomaly in a market system. However, the increasing concern with environmental issues since the 1960s made clear that such interdependencies are pervasive and part and parcel of real world market systems.

This is particularly true for information and communication networks, which raise several new and unique issues. The high degree of interconnectedness amplifies the interdependencies between participants in the network. Both negative and positive effects that are not reflected in market transactions may percolate widely and swiftly through electronic communication networks. In some types of networks, such as peer-to-peer arrangements, agents take on dual roles as consumers as well as producers of information and other services. Many users of cyberspace view it as a commons, in which transactions take place according to a gift rather than marketplace logic. Moreover, often, for example, in the case of Trojans, externalities are generated without the explicit consent or knowledge of an individual user. All these factors influence the prevalence of externalities and complicate possible ways to address them.

Origins of externalities in networked computer environments

External effects may originate at different stages of the value net in networked computer environments. Depending on the origin of the externality, the individual decision-making calculus causing the externality may be different. In any case decision makers focus on costs and benefits relevant to the individual agent and neglect costs or benefits of third parties.[6]

Table 1 provides an overview of the sources and forms of externalities in networked computer environment. The table captures the main stakeholders, but not necessarily all of them. Agents in the column are the sources of externalities whereas agents in the rows are the recipients. Not all agents may cause externalities on all others and some of the effects may be more likely or stronger than others. By definition, an agent cannot exert an externality on itself, although it may create an externality for another agent in the same category. For example, the lax security policy of one ISP may create externalities for other ISPs.

A first source of possible externalities is software vendors. When deciding the level of investment in activities that reduce vulnerabilities, software vendors will only take their private costs and benefits into account (Schneier, 2000). Sales of software are dependent on the reputation of the firm. If this reputation effect is strong, the firm will also be concerned about the security situation of the software users. However, it is likely that such reputation effects are insufficient to fully internalise externalities. This situation is aggravated by the unique economics of information markets with their high fixed costs and low incremental costs, the existence of network effects which create first-mover advantages, and the prevalence of various forms of switching costs and lock-in. These characteristics provide an incentive for suppliers to rush new software to the market (Anderson, 2001; 2002; Shostack, 2005). They may also lead to the dominance of one or a few firms, increasing overall vulnerability due to a "monoculture" effect (Böhme, 2005).

Table C.1. CERT.BR incident Reports

	Software vendors	ISPs	Large firms	SMEs	Individual users	Criminals
Software vendors	Level of trust, reputation	Risk of malevolent traffic	Level of software vulnerability	Level of software vulnerability	Level of software vulnerability	Hacking opportunities
ISPs	Level of trust, reputation	Volume of malevolent traffic	Risk of proliferating attack	Risk of proliferating attack	Risk of proliferating attack	Hacking opportunities
Large firms	Level of trust, reputation	Volume of malevolent traffic	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Hacking opportunities
SMEs	Level of trust, reputation	Volume of malevolent traffic	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Risk of hosting or proliferating attack	Hacking opportunities
Individual users	Level of trust, reputation	Volume of malevolent traffic	Risk of hosting attack	Risk of hosting attack	Risk of hosting attack	Hacking opportunities
Criminals	Level of trust, reputation	Resource use, reputation	Resource use, Costs of crime	Resource use, Costs of crime	Resource use, Costs of crime	Hacking opportunities

Whether they be large corporate users or small and medium-sized firms, security investments by firms to reduce vulnerabilities are likewise afflicted with externalities, as discussed by several authors (Gordon and Loeb, 2002;

Vijayan, 2003; Camp and Wolfram, 2004; Schechter, 2004; Chen *et al.*, 2005; Rowe and Gallaher, 2006). Profit-maximising firms, all other things being equal, will attempt to invest in information security until the (discounted) incremental private benefits of enhanced security are equal to the (discounted) costs of that investment. A firm will therefore not invest until the security risk is fully eliminated but only as long as the expected costs of the threat are higher than the cost of increasing information security. Costs that the firm imposes on third parties will not be considered in this calculus (unless they indirectly affect a firm's decision making, for example, because of reputation effects).

Likewise, benefits that a security investment bestows on third parties will also not be reflected in this decision. Under conditions of imperfect information and bounded rationality, firms may not be able to determine this private optimum with precision but they will try to approximate it. In any case, neither the negative external effects of investments falling short of the social optimum nor the positive externalities of investments that go beyond that optimum are taken into consideration. Individual firm decisions may thus systematically deviate from a social optimum that takes these interdependencies into account.

Individual users are seen by many as one of the weakest links in the value chain of networked computing (Camp, 2006). Larger business users often consider their decisions in an explicit cost-benefit framework. In contrast, small business and individual users often do not apply such instrumental rationality (LaRose *et al.,* 2005; Rifon *et al,.* 2005). Nevertheless, when making decisions as to security levels, they consider their own costs and benefits (but not those of other users). Individual users are particularly susceptible to non-intrusive forms of malware, which do not use up significant resources on the user end (*e.g.* computing power, bandwidth) but create significant damage to other machines. Consequently, the risk of attack for all other users and the traffic volume on networks is increased causing direct and indirect costs for third parties.

ISPs may inflict externalities on other agents in the value chain as well as on each other. Some malware may increase traffic and hence ISP costs only incrementally. In this case, the ISP may have little incentive to incur additional costs to engage in traffic monitoring and filtering. Even if users cause significant traffic increases, an ISP with a lot of spare capacity may not see anything but very incremental cost increases, again limiting the incentive to invest in security upgrades to reduce malware-related traffic.

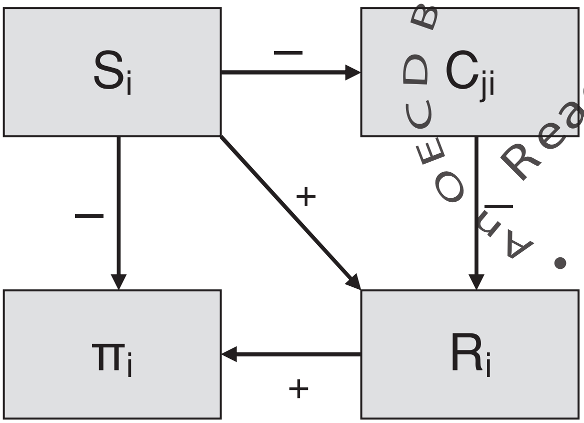
Information security externalities appear in several forms, including direct costs or benefits and indirect costs and benefits. Direct costs include damage caused to other stakeholders (such as corrupted data or websites, system downtimes) and the cost of increased preventative security expenses by other stakeholders (including cost of software and security personnel). Indirect costs include reduced trust within computer networks (for example, if nodes maintain lists of trusted other systems) and of users in information networks, the ability of hackers to increase the effectiveness of attacks by subverting more machines, and the ability of hackers to hide their traces (Camp and Wolfram 2004). They also include the potentially high costs associated with the reduced willingness of consumers to engage in e-commerce.

Externalities in a dynamic framework

In networked computer environments with rapid technological change, externalities need to be understood in a dynamic framework. Most importantly, learning and reputation effects need to be considered. Reputation and learning may happen at different time scales and with different intensity in the various components of the value net. They will also differ within markets, for example enterprise market software as opposed to mass market software. In any case, they may counteract and reduce the magnitude of negative externalities and possibly enhance positive externalities. Moreover, the activities of firms to disclose vulnerabilities will influence the magnitude of externalities.

Figure C.4 illustrates the reputation effect for the case of a software vendor (plus and minus signs indicate whether the two variables move in the same or the opposite direction). Other things being equal lower expenses for system testing and refinement by firm i (S_i) will reduce sunk costs and hence increase the profits (π_i) of the firm. However, costs may be externalised onto other firms, indexed j (C_{ji}). If these costs affect the reputation of firm i (R_i), profits may be reduced, especially if the reputation effect works swiftly. In this case, at least part of the potential externality is internalised and the deviation between private and social optimum is reduced. One form of strengthening the reputation mechanism is trusted-party certification. As Edelman (2006) and Anderson (2001) point out, given present liability rules, these firms face an adverse selection incentive in that they do not face any consequences for issuing wrong certificates.

Figure C.4 Externalities with reputation



S_i security investment of firm i

C_{ji} cost for firm j cause by sub-optimal security investment by firm i

R_i reputation of firm i

π_i profits of firm i

In a dynamic perspective, the incentives to disclose vulnerabilities need to be considered (Cavusoglu *et al.*, 2005). Disclosure exerts a positive externality (Gal-Or and Ghose, 2003; Gal-Or and Ghose, 2005) onto other stakeholders. Under certain conditions, disclosure incentives may be sufficiently strong to shrink the conditions under which deviations between the private and social optimum occur to a minimum (Choi *et al.*, 2005).

Notes

1. Statements as to the effect of changes in individual parameters or factors are typically made under the *ceteris paribus* assumption: that all other things remain equal. This is a widely used simplifying methodological tool to isolate changes in one or more variables in a highly complex interconnected system. Often, many factors will change simultaneously. A full grip on such changes will typically require some form of computer-based modelling or simulation.
2. It is possible that for some services and applications, 100% security levels are required (hence the benefits higher than the cost, even at a level of 100% security) and that the requisite cost will be incurred. It is unlikely, though, that this will hold for all services and applications.
3. More formally, the partial derivatives can be expressed as: $\delta MBC/\delta S<0$, $\delta MCC/\delta S>0$, $\delta MBS/\delta SV>0$, $\delta MCS/\delta SV>0$.
4. Mechanisms operating towards improving an objective are typically referred to as “incentives” whereas those operating in the opposite direction are referred to as “disincentives.”
5. This seems currently the case in many countries. See for example: Spindler, G. (2007), *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären: Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen*, Bundesamt für Sicherheit in der Informationstechnik, *www.bsi.de/literat/studien/recht/Gutachten.pdf*.
6. In a dynamic context, reputation effects may mitigate some of the externalities, see the discussion below.

Glossary of Malware Terms

Authentication factors: Used to obtain access; something the user knows (such as a password); something the user has (such as a credit card or token); or something the user is (a photograph or thumbprint).

Authentication/Authenticity: Being able to prove or verify a person's or entity's identity with a certain level of assurance. Authentication mechanisms are used to provide access control to information systems.

Availability: Ensuring that digital data within an information system and the system itself are available to authorised users.

Backdoors[1]: A backdoor is malicious code that allows unauthorised access to a computer system or network by accepting remote commands from an attacker elsewhere on the Internet.

Bluejacking: Sending unsolicited messages to Bluetooth connected devices.

Bluesnarfing enables unauthorised access to information from a wireless device through a Bluetooth connection.

Bot programme: A type of 'backdoor' programme that allows attackers to remotely control many compromised information systems (often thousands) simultaneously (or individually).

Botnet(s): Group of malware infected computers that can be used to remotely carry out attacks against other computer systems.

Confidentiality: Being able to protect information and data from unauthorised access.

CERTs: Computer emergency response teams.

CSIRTs: Computer security incident response teams.

DDoS: Distributed denial of service attacks.

[1] NIST (2005), pp. 2-12.

Digital certificate: A means of authenticating an identity for an entity when doing business or other transactions on the web or on line. Digital certificates exist as part of public key infrastructures (PKI).

Domain name: The identifier or address of any entity on the Internet. Domain Name System (DNS): The way Internet domain names are located and translated into an Internet Protocol, or IP, address. For example, the domain name www.oecd.org is a more user friendly and memorable alternative to the IP address 193.51.65.71.

Honeynet: Two or more honeypots on a network form a honeynet.

Honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated, (un)protected and monitored, and which seems to contain information or a resource that would be of value to attackers.

Integrity: A primary security goal of information systems which seeks to ensure that the system as a whole (people, data, software) have not been compromised and can continue to be trusted. Internet Protocol The native language of programmatic communication on the Internet.

Keystroke loggers[2] *:* A hidden programme that records and "logs" each key that's pressed on the compromised system's keyboard, as the legitimate user of the system is typing.

Malware payload: The primary function of a piece of malware.

Non-repudiation: A security goal which seeks to prevent a person from denying they undertook an electronic transaction when they did.

Operating system: A computer program that manages the hardware and software on a computer.

Packet: The minimum autonomously-routable quantum of data which can be transmitted across a modern digital "packet switched" network.

Patch/Workaround: A small piece of software code designed to correct or rectify an existing bug or flaw in an operating system or application programme. A work-around is a set of actions that network security managers can take to reduce their exposure to a known software vulnerability.

[2] Ibid.

Payload: The essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination.

Rootkit: A set of programmes designed to conceal the compromise of a computer at the most privileged "root" level, by modifying operating system files or inserting code into the memory of running processes.

Social engineering: Techniques designed to fool human beings into providing information or taking an action that leads to a subsequent breach in information systems security.

Spam: Commonly understood to mean bulk, unsolicited, unwanted and potentially harmful electronic messages.[3]

Spoofing is a technique designed to deceive an uninformed person about the origin of, typically, an e-mail or a website.

Spyware: A form of malware that is capable of capturing a range of data from user input (keyboards, mice) and output (screens) and other storage (memory, hard drive etc.) and sending this information to the attacker without the user's permission or knowledge.

Transaction signing: The process of calculating a keyed hash function to generate a unique string that can be used to verify both the authenticity and integrity of an online transaction.

Trojan horses: A computer program that appears legitimate but actually has hidden functionality used to circumvent security measures and carry out attacks.

Virus: Directly analogous to its biological namesake, a virus is hidden code that spreads by infecting another program and inserting a copy of itself into that program.

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management of software that could be exploited.

Worm: A type of malware that self replicates without the need for a host programme or human interaction.

[3] OECD (2006).

Bibliography

A-i3 (2006), Zur Haftung von Phishing-Opfern. *Arbeitsgruppe Identitätsschutz im Internet e.V, www.a-i3.org/content/view/975/230/.*

Anderson, R. (2001), “Why Information Security is Hard: An Economic Perspective”, Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, IEEE Computer Society, *www.acsac.org/2001/papers/110.pdf*.

Anderson, R. (2002), “Unsettling Parallels between Security and the Environment”, First Annual Workshop on Economics and Information Security, *www.cl.cam.ac.uk/~rja14/econws/37.txt*.

Anderson, R. (2007), “Closing the Phishing Hole – Fraud, Risk and Nonbanks”, *www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf*.

Anderson, R. and T. Moore (2006), “The Economics of Information Security”, *Science*, 314: 610-613.

Anderson, R. and T. Moore (2007), “Information Security Economics – and Beyond”, Computer Laboratory, University of Cambridge, *www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf*.

Anderson, R., *et al.* (2008), “Security Economics and the Internal Market”, European Network and Information Security Agency, *www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf*.

APACS (2008), “Fraud abroad pushes up losses on UK cards following two-year fall”, press release, *www.apacs.org.uk/2007Fraudfiguresrelease.html*.

APWG (Anti-Phishing Working Group) (2006a), *Phishing Activity Trends Report*, *www.antiphishing.org/reports/apwg_report_april_2007.pdf*, last accessed 14 December 2007.

APWG (2006b), *Phishing Activity Trends Report, www.websense.com/securitylabs/resource/PDF/apwg_report_december_2006.pdf*, last accessed 14 December 2007.

Arbor Networks (2007), *Worldwide Infrastructure Security Report, Volume III*, *www.arbornetworks.com/report*.

August, T. and T. I. Tunca (2006), “Network Software Security and User Incentives, *Management Science*, 52(11): 1703–1720.

AusCERT (2005), “Windows Rootkit, Prevention, Detection and Response”, *www.auscert.org.au/*, last accessed 11 December 2007.

AusCERT (2006), “Haxdoor – An anatomy of an online ID theft Trojan”, *www.auscert.org.au/render.html?cid=1920*, last accessed 10 December, 2007.

Australian Government, Office of the Privacy Commissioner (2004), *Community Attitudes towards Privacy 2004, www.privacy.gov.au/publications/rcommunity/chap10.html*, last accessed 11 December 2007.

Bangeman, E. (2006), “Court likely to order ICANN to suspend Spamhaus’ domain”, *Ars Technica*, *http://arstechnica.com/news.ars/post/20061009-7938.html.*

Banktip (2006). “Phishing: Kunden haften für Trojaner”, Banktip.de, *www.banktip.de/News/20648/Phishing-Kunden-haften-fuer-Trojaner.html.*

Barnum, S. and M. Gegick (2005), *Economy of Mechanism*, Build Security In, *https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/348.html?branch=1&language=1.*

Bauer, J. M., *et al.* (2008), “Financial Aspects of Network Security: Malware and Spam”, International Telecommunication Union, July, *www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.*

BBC News (2004), “MyDoom virus biggest in months”, BBC News website, *http://news.bbc.co.uk/1/hi/technology/3432639.stm*, last accessed 14 December 2007.

BBC News (2007a), “Google searches web’s dark side”, BBC News website, *http://news.bbc.co.uk/2/hi/technology/6645895.stm.*

BBC News (2007b), “Burgers paid for by mobile phone”, BBC News website, *http://news.bbc.co.uk/2/hi/technology/6400217.stm*, last accessed 7 December, 2007.

Becker, G. S. (1968), “Crime and Punishment: An Economic Approach”, *The Journal of Political Economy*, 76(2): 169-217.

Becsi, Z. (1999), “Economics and Crime in the States,” *Economic Review - Federal Reserve Bank of Atlanta*, 84(1): 38-56, *http://ezproxy.msu.edu:2047/login?url=http://proquest.umi.com/pqdweb?did=40779835&Fmt=7&clientId=3552&RQT=309&VName=PQD.*

Berner, R. and A. Carter (2005), "The truth about credit-card fraud", *Business Week Online*, *www.businessweek.com/technology/content/jun2005/tc20050621_3238_tc024.htm.*

Bernstein, D. J. (2007), "Some thoughts on security after ten years of qmail 1.0", 1st Computer Security Architecture Workshop in conjunction with 14th ACM Conference on Computers and Communication Security, Fairfax, Virginia, *http://cr.yp.to/qmail/qmailsec-20071101.pdf.*

Böhme, R. (2005), "Cyber-Insurance Revisited", Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/15.pdf.*

Brendler, B. (2007), "Spyware/Malware Impact on Consumers"; APEC-OECD Malware Workshop, StopBadware Project, April, *www.oecd.org/dataoecd/33/55/38652920.pdf*, last accessed 13 December 2007.

Camp, L. J. (2006), *Mental Models of Privacy and Security*, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=922735.*

Camp, L. J. and C. Wolfram (2004), *Pricing Security: Vulnerability as Externalities*, *http://ssrn.com/abstract=894966.*

Campbell, K., *et al.* (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", *Journal of Computer Security* 11(3): 431-448, *http://brief.weburb.dk/archive/00000130/01/2003-costs-security-on-stockvalue-9972866.pdf.*

Cavusoglu, H., B. Mishra and S. Raghunathan (2004), "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *International Journal of Electronic Commerce*, 9(1): 69, *www.gvsu.edu/business/ijec/v9n1/p069.html.*

Cavusoglu, H., H. Cavusoglu and S. Raghunathan (2005), *Emerging issues in responsible vulnerability disclosure*, Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/cavusoglu.pdf.*

CERT (United States Computer Emergency Response Team), Federal Incident Reporting Guidelines, *www.us-cert.gov/federal/reportingRequirements.html.*

CERT Coordination Center (2006), List of CSIRTs with national responsibility, www.cert.org/csirts/national/contact.html, last accessed 10 December 2007.

CERT Coordination Center (2007), The Use of Malware Analysis in Support of Law Enforcement, *www.securitynewsportal.com/securitynews/article.php?title=The_Use_of_Malware_Analysis_in_Support_of_Law_Enforcement*, last accessed 11 December 2007.

Charney, S. (2005), “Combating Cybercrime: A Public-Private Strategy in the Digital Environment”, Microsoft Corporation, www.nwacc.org/programs/conf05/UNCrimeCongressPaper.doc, last accessed 11 December 2007.

Chen, P.-Y., G. Kataria and R. Krishnan (2005) “Software Diversity for Information Security”, Fourth Workshop on the Economics of Information Security, Harvard University, http://infosecon.net/workshop/pdf/47.pdf.

Choi, J. P., C. Fershtman and N. Gandal (2005), “Internet Security, Vulnerability Disclosure, and Software Provision”, Fourth Workshop on the Economics of Information Security, Harvard University, http://infosecon.net/workshop/pdf/9.pdf.

Clayton, R. (2007), “Phishing and the gaining of ‘clue’”, Light Blue Touchpaper, www.lightbluetouchpaper.org/2007/08/16/phishing-and-the-gaining-of-clue/.

Computer Economics (2007), 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code, *www.computereconomics.com/page.cfm?name=Malware%20Report.*

Congressional Budget Office Cost Estimate (2007), “H.R. 1525 Internet Spyware (I-SPY) Prevention Act of 2007”, as ordered reported by the House Committee on the Judiciary, 7 May, *www.cbo.gov/ftpdocs/80xx/doc8076/hr1525.pdf.*

Consumer Reports WebWatch (2005), “Leap of Faith: Using the Internet Despite the Dangers”, results of a National Survey of Internet Users for Consumer Reports WebWatch, www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm ;

Consumers Union (2007), “State of the ‘Net’ Survey ‘07”, *Consumer Reports*, 2007(9): 28-34.

Consumentenbond (2006), “PC beveiliging & veilig Internet: Een enquête onder computergebruikers”, *Consumentengids*, 2006(11).

Council of Europe (2001), *Convention on Cybercrime*, Budapest, 23 November, *http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.*

Council of Europe (2007), “Status of Signatories and Parties to the Convention on Cybercrime”, CETS No. 185, *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/04&CL=ENG*, last accessed 11 December 2007.

Counterpane & MessageLabs (2006), *2005 Attack Trends & Analysis*, *www.counterpane.com/dl/attack-trends-2005-messagelabs.pdf*.

CSI (Computer Security Institute) (2007), *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey*, *www.gocsi.com/forms/csi_survey.jhtml*.

CSI/FBI Computer Crime and Security Survey (2006), *www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=4SCJQ3Y0PCPTOQSNDLPCKHSCJUNN2JVN*.

Dancho D. (2006), "Malware – future trends", *www.linuxsecurity.com/docs/malware-trends.pdf*, last accessed 7 December 2007.

Dearne, K. (2007), "Online security begins at home", *Australian IT News*, *http://australianit.news.com.au/articles/0,7204,21675098%5E24169%5E%5Enbv%5E,00.html*, last accessed 11 December 2007.

Denning, D. (2000), "Statement by Dorothy E. Denning", Georgetown University, *http://ftp.fas.org/irp/congress/2000_hr/00-05-23denning.htm*.

Devillard, A. (2006), *Le « phishing » en France, peu de victimes mais une menace grandissante*, 01net, *www.01net.com/editorial/311785/cybercriminalite/le-phishing-en-france-peu-de-victimes-mais-une-menace-grandissante/*, last accessed 11 December 2007.

Dhamija, Rachna, *et al.* (2007), "The Emperor's New Security Indicators, An evaluation of website authentication and the effect of role playing on usability", *http://usablesecurity.org/emperor*.

Dot-TK (2007), "Dot Tk Free Domain Names – A New Approach To Make A Whole Top Level Country Domain Free Of Illicit Content", *www.dot.tk/en/press_jul16-07.pdf*.

Du, Y. (2007), "Introduction of malware Issues", presentation by CNCERT/CC at the APEC-OECD Malware Workshop, *www.oecd.org/dataoecd/33/59/38653107.pdf*, last accessed 10 December, 2007.

Dynes, S., E. Andrijicic and M. E. Johnson (2006), "Costs to the U.E. Economy of Information Infrastructure Failure from Field Studies and Economic Data", Fifth Workshop on the Economics of Information Security 2006, *http://weis2006.econinfosec.org/docs/4.pdf*.

Dynes, S., H. Brechbühl and M. E. Johnson (2005), *Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm*, Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/51.pdf*.

The Economist (2007), “A cyber riot”, 10 May, *www.economist.com/world/europe/displaystory.cfm?story_id=9163598*, accessed 4 December, 2007.

Edwards, L., (2004), “Reconstruction Consumer Privacy Protection Online”, *International Review of Law – Computers & Technology*, Vol. 18, No. 3, p. 315.

Eeten, M. J. van and J. M. Bauer (2008), “Economics of Malware: Security Decisions, Incentives and Externalities”, *OECD Science, Technology and Industry Working Papers*, 2008/1, OECD Publishing, doi:10.1787/241440230621.

Ehrlich, I. (1996), “Crime, Punishment, and the Market for Offenses”, *The Journal of Economic Perspectives*, 10(1): 43-67, *http://links.jstor.org/sici?sici=0895-3309%28199624%2910%3A1%3C43%3ACPATMF%3E2.0.CO%3B2-U*.

ENISA (European Network and Information Security Agency) (2006), *Provider Security Measures Part 1: Security and Anti-Spam Measures of Electronic Communication Service Providers - Survey*, *www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf.*

Ernst & Young (2007), *Global Information Security Survey 2006*, *www.ey.nl/download/publicatie/2006_GISS_EYG_AU0022.pdf.*

European Union (1995), “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, *Official Journal of the European Communities*, L 281/31, *http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf*, accessed 11 December 2007.

European Union (2002), “Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector”, *Official Journal of the European Communities*, L 201/37, *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf*, accessed 11 December 2007.

European Union (2005), “Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems”, *Official Journal of the European Communities,* L 69/67 *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.*

European Commission (2007), “E-Communication Household Survey”, Special Eurobarometer 274, Wave 66.3, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_274_en.pdf*, last accessed 10 December 2007.

Fox, J. (2007), *Consumer Reports: Putting Consumers Back in Control*, Federal Trade Commission, *www.ftc.gov/bcp/workshops/spamsummit/presentations/Consumers.pdf*.

Franklin, J., *et al*. (2007), "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants", CCS'07, *www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf.*

Friedman, L. S. (2002), *The Microeconomics of Public Policy Analysis*, Princeton University Press, Princeton.

F-Secure (2007), "IT Security Threat Summary for H1 2007", F-Security Data Security Wrapup 1/2007, *www.f-secure.com/2007/1/.*

Gal-Or, E. and A. Ghose (2003), "The Economic Consequences of Sharing Security Information", 2nd Annual Workshop on Economics and Information Security, *www.cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf.*

Gal-Or, E. and A. Ghose (2005), "The Economic Incentives for Sharing Security Information", *Information Systems Research*, 16(2): 186-208, *www.andrew.cmu.edu/user/aghose/Infosec.pdf.*

Gartner (2005), "Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce", press release, *www.gartner.com/press_releases/asset_129754_11.html.*

Gaudin, S. (2007), "T.J. Maxx Security Breach Costs Soar To 10 Times Earlier Estimate", *Information Week*, *http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201800259.*

GetSafeOnline (2006), *The Get Safe Online Report*, October, *www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf.*

Google, Inc. (2007), "The Ghost In The Browser Analysis of Web-based Malware", *www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf*, accessed 12 December 2007.

Gordon, L. A. and M. P. Loeb (2002), "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, Vol. 5, Issue 4, pp. 438-457, *http://portal.acm.org/citation.cfm?id=581274*.

Govcert.nl (2006), *Annual Review, www.govcert.nl/render.html?it=147*, last accessed 13 December 2007.

Govcert.nl (2007), "Botnets", presentation given by Douwe Leguit at the APEC-OECD Malware Workshop, *www.oecd.org/dataoecd/34/36/38653287.pdf*, accessed 10 December 2007.

Greene, T. (2007), “Kapersky seeks help from international police to fight cybercrime”, *Network World*, *www.networkworld.com/news/2007/013107-kaspersky-cybercrime.html*, accessed 14 December 2007.

Heidrich, J. (2007), “IP-Blacklisting zur Spam-Abwehr kann rechtswidrig sein”, *Heise Online, www.heise.de/newsticker/meldung/97568*.

Higgins, K. J. (2007a), “Battling Bots, Doing No Harm”, *Dark Reading*, *www.darkreading.com/document.asp?doc_id=118739*.

Higgins, K. J. (2007b), “Untying the Bot Knot”, *Dark Reading*, *www.darkreading.com/document.asp?doc_id=114081&WT.svl=news1_6*

Honeynet Project and Research Alliance (2007), *Know your enemy: Fast-Flux Service Networks*, *www.honeynet.org/papers/ff/*, accessed 13 December, 2007.

House of Lords (2007a), *Science and Technology Committee, 5th Report of Session 2006–07, Personal Internet Security, Volume I: Report*, Authority of the House of Lords, *www.publications.parliament.uk/pa/ld/ldsctech.htm*.

House of Lords (2007b), *Science and Technology Committee, 5th Report of Session 2006–07, Personal Internet Security, Volume II: Evidence*, Authority of the House of Lords, *www.publications.parliament.uk/pa/ld/ldsctech.htm*.

Hypponen, M. (2006); “Malware goes mobile”; *Scientific American,* pp.70-77, *www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf*, accessed 13 December 2007.

iGillottResearch, Inc. (2006), “The Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks”, White Paper, September, *www.trustedcomputinggroup.org/groups/mobile/Final_iGR_mobile_security_white_paper_sept_2006.pdf*, accessed 7 December 2007.

ITU (International Telecommunications Union) (2007), “Executive Summary”, *World Information Society Report 2007: Beyond WSIS*, *www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07-summary.pdf*.

Javelin Strategy & Research (2007), *2007 Identity Fraud Survey Report – Consumer Version How Consumers Can Protect Themselves*, *www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf*, accessed 14 December 2007.

Just, R. E., D. L. Hueth and A. Schmitz (2004), *The Welfare Economics of Public Policy: A Practical Approach to Project and Policy Evaluation*, Edward Elgar, Cheltenham, UK and Northampton, MA.

Kaspersky Labs (2006), *Malware Evolution 2006: Executive Summary, www.kaspersky.com/malware_evolution_2006_summary*.

Krebs, B. (2006), “The New Face of Phishing”, Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html.*

Krebs, B. (2007), “Study: $3.2 Billion Lost to Phishing in 2007”, Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2007/12/study_32_billion_lost_to_phish_1.html*.

Krebs, B. (2008), “Banks: Losses from Computer Intrusions Up in 2007”, Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html*.

Kunreuther, H. and G. Heal (2003), “Interdependent security”, *Journal of Risk and Uncertainty*, 26(2): 231.

Lacohée, H., S. Crane and A. Phippen (2006), “Trustguide: Final Report”, BT Group Chief Technology Office, Research & Venturing / HP Labs / University of Plymouth, Network Research Group, *www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf*.

LaRose, R., N. Rifon, S. Liu and D. Lee (2005), “Understanding Online Safety Behavior: A Multivariate Model”, International Communication Association, New York, *www.msu.edu/~isafety/papers/ICApanelmult21.htm*.

Lemos, R. (2006), “Attackers pass on OS, aim for drivers and apps”, Security Focus website, *www.securityfocus.com/news/11404*.

Lemos, R. (2007), “Estonia gets respite from web attacks”, Security Focus website, *www.securityfocus.com/brief/504*.

Liu, P.-W. (2007), “Panel Discussion: Gaps and Challenges”, presentation at the OECD-APEC Tel Malware Workshop by the Director of the Information and Communication Security Technology Center, Chinese Taipei, *www.oecd.org/dataoecd/34/19/38653499.pdf*, accessed 10 December 2007.

McAfee, Inc. (2006), “Virtual Criminology Report 2007 Organized Crime and the Internet”, *McAfee Avert® Labs Technical White Papers,* December, *www.mcafee.com/us/threat_center/white_paper.html*.

McAfee Inc. (2007), “Identity Theft”, *McAfee Avert® Labs Technical White Papers*, January, *www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf*.

McCarthy, C. (2007), “Study: Identity theft keeps climbing”, *Cnet News*, *http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html*.

McNamara, P. (2007), “Survey: Identity theft on the decline”*, Network World*, *www.networkworld.com/community/?q=node/11009*, accessed 11 December 2007.

Marshall, A. (1920), *Principles of Economics: An Introductory Volume*, Macmillan, London.

Mashevsky, Y. (2007), “The Virtual Conflict – Who Will Triumph?”, *The Virtualist*, *www.viruslist.com/en/analysis?pubid=204791915*.

Mell, P., K. Kent and J. Nusbaum (2005), *Guide to Malware Incident Prevention and Handling*, National Institute of Standards and Technology, *http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf*.

Messaging Anti-Abuse Working Group (2007), “Email Metrics Program: The Network Operators’ Perspective; Report #5 - First Quarter 2007, June 2007”, *www.maawg.org/about/MAAWG20071Q_Metrics_Report.pdf*, accessed 10 December 2007.

NISCC (UK National Infrastructure Security Information Centre) (2005), “Targeted TrojanEmail Attacks”, *NISCC Briefing*, 08/2005, *www.cpni.gov.uk/docs/ttea.pdf*, accessed 7 December 2007.

MessageLabs (2006), *MessageLabs Intelligence: 2006 Annual Security Report - A Year of Spamming Dangerously: The Personal Approach to Attacking, www.messagelabs.com/mlireport/2006_annual_security_report_5.pdf*, accessed 10 December 2007.

Messagelabs (2007), *MessageLabs Intelligence: 2007 Annual Security Report - A year of storms, spam and socializing, www.messagelabs.com/resources/mlireports*, accessed 10 December 2007.

Messmer, E. and D. Pappalardo (2005), “Extortion via DDoS on the rise: Criminals are using the attacks to extort money from victimized companies”, *Computerworld*, *www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html*, accessed 7 December 2007.

Microsoft (2005), *The Trustworthy Computing Security Development Lifecycle*, *http://msdn2.microsoft.com/en-us/library/ms995349.aspx*.

Microsoft (2006a), *Security Intelligence Report (January – June 2006)*, *www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en*.

Microsoft (2006b), *Security Intelligence Report (July - December 2006), www.microsoft.com/downloads/details.aspx?familyid=af816e28-533f-4970-9a49-e35dc3f26cfe&displaylang=en*, accessed 3 December 2007.

Microsoft (2007), "Storm Drain", Anti-Malware Engineering Team Weblog, *http://blogs.technet.com/antimalware/archive/2007/09/20/storm-drain.aspx*.

Netcraft Toolbar Community (2007), "Phishing By The Numbers: 609,000 Blocked Sites in 2006", Netcraft website, *http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html*, accessed 11 December 2007.

NIST (National Institute of Standards and Technology) (2005), *Guide to Malware and Incident Handling: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-83, November, *http://csrc.nist.gov/publications/nistpubs/800-83/SP800 83.pdf*.

NIST (2008), *Computer Security Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-61 Revision 1, March, *http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf*.

Nowotny, E. (1987), *Der öffentliche Sektor: Einführung in die Finanzwissenschaft*, Springer, Berlin.

Oberoi, S. (2007), "Addressing the Malware Problem", presentation given at the APEC-OECD Malware Workshop, *http://www.oecd.org/dataoecd/33/57/38653049.pdf*.

OECD (2002a), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, www.oecd.org/dataoecd/16/22/15582260.pdf.*

OECD (2002b). "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security – Questions and Answers", *www.oecd.org/dataoecd/27/6/2494779.pdf*.

OECD (2005a), "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2005)1/FINAL, 16 December, *www.oecd.org/dataoecd/16/27/35884541.pdf*.

OECD (2005b), *Science, Technology, and Industry Scoreboard*, 2005 edition*,* OECD Publishing, Paris.

OECD (2006), "OECD Anti-Spam Toolkit of Recommended Policies and Measures", report of the OECD Task Force on Spam, DSTI/CP/ICCP/SPAM(2005)3/FINAL, www.oecd-antispam.org/, accessed 13 December 2007.

OECD (2007a), *OECD Communications Outlook 2007*, Information and Communications Technologies, OECD Publishing, Paris.

OECD (2007b), "APEC-OECD Malware Workshop: Summary Record", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)15, 15 June, *www.oecd.org/dataoecd/37/60/38738890.pdf*.

OECD (2007c), "The Development of Policies for the protection of Critical Information (CII): A comparative analysis in four OECD countries: Canada, Korea, the United Kingdom and the United States", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2006)15/FINAL, 6 February, *www.olis.oecd.org/olis/2006doc.nsf/ENGREFCORPLOOK/NT00007766/$FILE/JT03221273.PDF*.

OECD (2008a), "The Development of Policies for the protection of Critical Information (CII): A comparative analysis in three OECD countries: Australia, Japan, and the Netherlands", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)16/FINAL, 9 January, *www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005A5E/$FILE/JT03238526.PDF*.

OECD (2008b), "Scoping Paper on Online Identity Theft", unclassified document, DSTI/CP(2007)3/FINAL, 15 May, *www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005CAE/$FILE/JT03240674.PDF*.

OECD (2008c), "The Development of Policies for the Protection of Critical Information Infrastructures (CII): A Comparative Analysis in Seven OECD Countries: Australia, Canada, Korea, Japan, The Netherlands, The United Kingdom and the United States", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)20/FINAL, 8 April, *http://www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005A8A/$FILE/JT03243745.PDF*.

ORF (2007), *Spamhaus antwortet auf nic.at*. futurezone, *http://futurezone.orf.at/it/stories/201738/*, accessed 25 November 2007.

Outlaw.com (2007), "Phishing attack evades ABN Amro's two-factor authentication", OUT-LAW News, 18 April, *www.out-law.com/page-7967*, accessed 11 December 2007.

PayPal (2007), "Key Financial Facts", Paypal website, *www.pppress.co.uk/* .

Pigou, A. C. (1932), *The Economics of Welfare*, Macmillan, London.

Poindexter, J. C., J. B. Earp and D. L. Baumer (2006), "An experimental economics approach toward quantifying online privacy choices", *Information Systems Frontiers*, 8(5): 363-374.

Poulsen, Kevin (2003), *Slammer worm crashed Ohio nuke plant network,* Security Focus, *www.securityfocus.com/news/6767*, accessed 11 December 2007.

Register (2007), "Phishing attack evades bank's two-factor authentication", *www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/.*

Rescorla, E. (2004), "Is finding security holes a good idea?", Workshop on Economics and Information Security 2004, *www.rtfm.com/bugrate.pdf.*

Rifon, N., E. T. Quilliam and R. LaRose (2005), "Consumer Perceptions of Online Safety", paper presented at the International Communication Association, Communication and Technology Division, New York, 27 May, *www.msu.edu/~isafety/papers/ICApanelfg.htm.*

Rowe, B. R. and M. P. Gallaher (2006), "Private Sector Cyber Security Investment: An Empirical Analysis", Fifth Workshop on the Economics of Information Security, Cambridge, March, *www.weis2006.econinfosec.org/docs/18.pdf.*

RSA Security (2006), "Internet Confidence Index Shows that – for Businesses and Consumers – Transactions are Outpacing Trust", *www.rsa.com/press_release.aspx?id=6502,* accessed 14 December 2007.

Schechter, S. E. (2004), *Computer Security Strength & Risk: A Quantitative Approach*, thesis presented to the Division of Engineering and Applied Sciences, Harvard University, May, *www.eecs.harvard.edu/~stuart/papers/thesis.pdf.*

Schneier, B. (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley, New York.

Schneier, B. (2005), "A Real Remedy for Phishers", *Wired News*, *www.wired.com/news/politics/0,1283,69076,00.html.*

Schneier, B. (2007), "Information Security and Externalities", NSF/OECD Workshop on Social & Economic Factors Shaping The Future of the Internet, Washington, DC, *www.oecd.org/dataoecd/60/8/37985707.pdf.*

Shifrin, T. (2007), "Lose an unencrypted laptop and 'face criminal action'", *Computerworld UK*, 15 November, *www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=6241.*

Shin, A. (2007a); “Is Identity Theft Decreasing?”, The Checkout Washington Post Blog, 6 February, *http://blog.washingtonpost.com/thecheckout/2007/02/is_identity_theft_decreasing.html.*

Shin, A. (2007b), “Looking for a Job? Phishers Are Looking for You.”, The Checkout Washington Post Blog, 12 February, *http://blog.washingtonpost.com/thecheckout/2007/02/looking_for_a_job_phishers_are.html.*

Shostack, A. (2005), “Avoiding Liability: An Alternative Route to More Secure Products”, Fourth Workshop on the Economics of Information Security, Harvard University, *infosecon.net/workshop/pdf/44.pdf.*

Snyder, W. (2007), “Time to Deploy improvement of 25 %”, Mozilla Security Blog, *http://blog.mozilla.com/security/2007/06/18/time-to-deploy-improvement-of-25-percent/.*

Sokolov, D. A. (2007), “Spamhaus.org setzt Österreichs Domainverwaltung unter Druck”, Heise online, *www.heise.de/newsticker/meldung/91417*; last accessed 25 November 2007.

Sophos (2006a), “The Growing Scale of the Threat Problem”, *www.sophos.com/sophos/docs/eng/papers/Growing-threat-wpus.pdf*, accessed 7 December, 2007.

Sophos (2006b), “Devious Arhiveus ransomware kidnaps data from victims' computers”, *www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html*, accessed December 7, 2007.

Sophos (2006c), “Married couple formally charged over spyware Trojan horse”, *www.sophos.com/pressoffice/news/articles/2006/03/israeliesp2.html*, accessed 13 December 2007.

Sophos (2007a), “Security Threat Report”, Sophos Security white paper, *www.sophos.com/security/whitepapers/*, last accessed 12 December 2007.

Sophos (2007b), “Security Threat Report Update July 2007”, Sophos Security white paper, *www.sophos.com/security/whitepapers/*, accessed 12 December 2007.

South, G. (2007), “Web issues over banking code”, *The New Zealand Herald*, *www.nzherald.co.nz/topic/story.cfm?c_id=126&objectid=10458545.*

Spamhaus (2007), “Report on the criminal 'Rock Phish' domains registered at Nic.at”, Spamhaus statements, 21 June, *www.spamhaus.org/organization/statement.lasso?ref=7*, accessed 25 November 2007.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(93 2009 01 1 P) ISBN 978-92-64-05650-3 – No. 56607 2009

Computer Viruses and Other Malicious Software

A THREAT TO THE INTERNET ECONOMY

The Internet has become a powerful tool for enhancing innovation and productivity. Nevertheless, the increasing dependence on the Internet and other communication networks means the Internet has also become a popular and efficient way to spread computer viruses and other types of malicious software (malware).

Malware attacks are increasing in both frequency and sophistication, thus posing a serious threat to the Internet economy and to national security. Concurrently, efforts to fight malware are not up to the task of addressing this growing global threat; malware response and mitigation efforts are essentially fragmented, local and mainly reactive.

A wide range of communities and actors – from policy makers to Internet Service Providers to end users – all play a role in combating malware. But there is still limited knowledge, understanding, organisation and delineation of the roles and responsibilities of each of these actors. Improvements can be made in many areas, and international co-operation would benefit greatly in areas such as: proactive prevention (education, guidelines and standards, research and development); improved legal frameworks; stronger law enforcement; improved tech industry practices; and better alignment of economic incentives with societal benefits.

This book is a first step toward addressing the threat of malware in a comprehensive, global manner. It has three major aims: 1) to inform policy makers about malware – its growth, evolution and countermeasures to combat it; 2) to present new research into the economic incentives driving cyber-security decisions; and 3) to make specific suggestions on how the international community can better work together to address the problem.

The full text of this book is available on line via these links:
www.sourceoecd.org/governance/9789264056503
www.sourceoecd.org/scienceIT/9789264056503

Those with access to all OECD books on line should use this link:
www.sourceoecd.org/9789264056503

SourceOECD is the OECD online library of books, periodicals and statistical databases.
For more information about this award-winning service and free trials, ask your librarian, or write to us at **SourceOECD@oecd.org**.

OECD*publishing*
www.oecd.org/publishing

ISBN 978-92-64-05650-3
93 2009 01 1 P

9 789264 056503