



ITU Study on the Financial Aspects of Network Security: Malware and Spam

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

Final Report July 2008



**International
Telecommunication
Union**

Acknowledgements

This paper has been produced by Johannes M. Bauer, Quello Center for Telecommunication Management and Law Michigan State University, East Lansing, Michigan, USA, Michel J. G. van Eeten, School of Technology, Policy and Management Delft University of Technology, Delft, The Netherlands and Tithi Chattopadhyay, Yuehua Wu, Quello Center for Telecommunication Management and Law Michigan State University, East Lansing, Michigan, USA

The authors wish to thank Jennifer Defore for editorial support. Comments by Robert Shaw, Suresh Ramasubramanian, and participants at the ITU Cybersecurity Forum in Brisbane are gratefully acknowledged. Their feedback made this a much more coherent and readable report

This ITU Study on the Financial Aspects of Network Security: Malware and Spam is available online at:
www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

This document is formatted for printing recto-verso. This document has been issued without formal editing.

For further information and to make comments on this document, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Telecommunication Development Bureau
International Telecommunication Union
Place des Nations
1211 Geneva 20, Switzerland
Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

Disclaimer

The opinions expressed in this report are those of the author(s) and do not necessarily represent the views of the International Telecommunication Union (ITU) or its membership. The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

© ITU 2008



Please consider the environment before printing this report.

TABLE OF CONTENT

EXECUTIVE SUMMARY	I
1. INTRODUCTION	1
2. THE PROBLEM OF MALWARE	2
2.1. FUNCTIONING OF MALWARE.....	3
2.2. FRAUDULENT AND CRIMINAL USES.....	3
2.3. FACTORS AGGRAVATING THE DISSEMINATION OF MALWARE	5
3. BUSINESS MODELS RELATED TO MALWARE	7
3.1. DIVISION OF LABOR	8
3.2. THE ROLE OF BOTNETS	9
3.3. THE GEOGRAPHY OF MALWARE AND SPAM	10
4. A CONCEPTUAL FRAMEWORK FOR MODELING FINANCIAL ASPECTS OF MALWARE AND SPAM	12
5. FINANCIAL AND OPERATIONAL EFFECTS OF MALWARE.....	14
5.1. DIRECT AND INDIRECT COSTS OF MALWARE	14
<i>COSTS AT AN AGGREGATE LEVEL.....</i>	<i>14</i>
<i>COSTS FOR BUSINESSES</i>	<i>15</i>
<i>COSTS TO CONSUMERS.....</i>	<i>17</i>
5.2. ILLEGAL REVENUES ASSOCIATED WITH MALWARE	17
5.3. OPERATIONAL EFFECTS ON CYBER INFRASTRUCTURE	18
6. FINANCIAL AND OPERATIONAL EFFECTS OF SPAM	20
6.1. DIRECT AND INDIRECT COSTS OF SPAM	20
<i>EFFECTS ON BUSINESSES</i>	<i>20</i>
<i>EFFECTS ON INDIVIDUALS.....</i>	<i>23</i>
6.2. OPERATIONAL ASPECTS OF SPAM	26
<i>PROVIDING EMAIL SERVICES TO SEND SPAM.....</i>	<i>26</i>
<i>PROVIDING NETWORK BANDWIDTH TO CARRY SPAM AND MALWARE</i>	<i>28</i>
<i>FIGHTING SPAM.....</i>	<i>29</i>
7. WELFARE EFFECTS: A PRELIMINARY ASSESSMENT	31
7.1. CORRECTLY IDENTIFYING WELFARE EFFECTS	31
7.2. EXTERNALITIES AND WELFARE	32
7.3. CONCLUDING OBSERVATIONS: A PATCHWORK OF NUMBERS.....	33

Table of figures

FIGURE 1. VISIBILITY OF MALWARE VS. MALICIOUS INTENT	7
FIGURE 2 DIVISION OF LABOR IN THE MALWARE UNDERGROUND ECONOMY VISIBILITY OF MALWARE VS. MALICIOUS INTENT	8
FIGURE 3 LEGAL AND POTENTIALLY ILLEGAL FINANCIAL FLOWS RELATED TO MALWARE	12
FIGURE 4 AVERAGE REPORTED LOSSES IN CSI SURVEYS 1999-2007 (\$000)	15
FIGURE 5 THREATS TO CYBER INFRASTRUCTURE	19
FIGURE 6 PRIMARY ATTACK TARGETS.....	19
FIGURE 7 SPAM RATES 2005-2007.....	21
FIGURE 8 SPAM AND VIRUS INTERCEPTION BY BUSINESS SIZE	23

FIGURE 9 DISTRIBUTION OF ADS FOR GOODS IN LABELED DATA43	24
FIGURE 10 EXTRAPOLATED NUMBER OF ADS FOR COMPROMISED HOSTS	27
FIGURE 11 DISTRIBUTION OF ADS FOR GOODS IN LABELED DATA43	28
FIGURE 12 SUSTAINED ATTACK SIZE IN GBPS	29
FIGURE 13 ATTACK DETECTION TECHNIQUES	30

Tables

TABLE 1 SUMMARY OF FRAUD CASES FILED BY CIFAS	25
TABLE 2 FINANCIAL BENEFITS OR LOSSES AVOIDED BE PREVIOUS WARNINGS	25
TABLE 3 FINANCIAL EFFECTS OF MALWARE AND SPAM.....	35

EXECUTIVE SUMMARY

Measures to improve information security enhance trust in online activities and contribute directly and indirectly to the welfare gains associated with the use of information and communication technologies (ICTs). However, some expenditure on security is only necessary because of relentless attacks by fraudsters and cybercriminals that undermine and threaten trust in online transactions. Such costs are not welfare-enhancing but a burden on society. Two vectors through which such attacks are carried out are malware and spam.

Malware is a summary term for different forms of malevolent software designed to infiltrate and infect computers, typically without the knowledge of the owner. During the past two decades, the production and dissemination of malware has grown into a multibillion dollar business. Damages created by fraudulent and criminal activities using malware and the costs of preventative measures are likely to exceed that number significantly. Malware puts the private and the public sector at risk because both increasingly rely on the value net of information services.

Until a few years ago, the most common types of malware were viruses and worms. More recently, other kinds have appeared and are widely distributed, including trojan horses, backdoors, keystroke loggers, rootkits, and spyware. Whereas spam and malware were hitherto relatively separable problems they are presently converging with the emergence of botnets. These networks of remote-controlled malware-infected computers are the origin of the majority of spam messages but they are also sustained and extended through spam.

Spam and malware have multifaceted financial implications on the costs and the revenues of participants in the ICT value chain. Costs of all stakeholders across the value network of information services, such as software vendors, network operators, Internet Service Providers (ISPs), and users, are affected directly and indirectly. Cost impacts may include, but are not limited to, the costs of preventative measures, the costs of remediation, the costs of bandwidth and equipment, and the opportunity costs of congestion.

Activities associated with spam and malware also generate various revenue streams. Fraudulent and possibly criminal revenues include the renting out of botnets, bullet proof hosting services, commissions on spam-induced sales, and stock price manipulation schemes. At the same time, spam and malware provide legal business opportunities including anti-virus and anti-spam products, investment to improve the resilience of infrastructure, and bandwidth. Because of this broad range of financial implications, spam and malware create mixed and sometimes conflicting incentives for stakeholders. Consequently, coherent responses to the problem are complicated.

During the past few years, the generation, distribution, and use of malware have increasingly become organized as illegal business activities. Participants in the underground malware economy will pursue their activities as long as the benefits of semi-legal and illegal activities outweigh the costs of these activities, including the expected costs of sanctions. Due to the factors discussed in this report, the economic incentives to expand cybercriminal activity continue to be strong.

Malware and spam are associated with a web of financial flows between the main groups of stakeholders in the information and communication value net. The development of accurate measures of these flows is complicated by the large number of legal and illegal players and the elusive nature of some of the transactions. Most of the financial flows between the legal and illegal players in the underground cybercrime economy, for example, are not or only partially known.

This report develops a framework within which these financial impacts can be assessed and brings together the many disparate sources of financial data on malware and spam. The following points summarize key findings:

- Estimates of the financial effects of malware differ widely. Figures for overall effects range from US\$ 13.2 billion of direct damages for the global economy (in 2006) to US\$ 67.2 billion in direct and indirect effects on U.S. businesses alone (in 2005).
- In a survey of its members, the Computer Security Institute (CSI) estimated the loss caused by cybersecurity breaches per responding firm to US\$ 345,000 in 2006. This number is most likely not representative for businesses in general due to the unique membership of CSI. The 2006 number is considerably lower than its peak in 2001 but more than double the 2005 level.
- Consumer Reports estimated the direct costs to U.S. consumers of damages experienced due to malware and spam to US\$ 7.1 billion in 2007.
- One estimate put the global cost of spam in 2007 at US\$ 100 billion and the respective cost for the U.S. at US\$ 35 billion. Another study found that the cost of spam management in the U.S. alone amounted to US\$ 71 billion in 2007.
- In 2007, the costs of click fraud in the U.S. were estimated to be nearly US\$ 1 billion.
- Numbers documenting the magnitude of the underground Internet economy and transactions between it and the formal economy also vary widely. One source estimates the worldwide underground economy at US\$ 105 billion.
- No reliable numbers exist as to the potential opportunity costs to society at large due to reduced trust and the associated slower acceptance of productivity-enhancing IT applications. However, a considerable share of users expressed concern and indicated that it reduces their willingness to perform online transactions.

Although the financial aspects of malware and spam are increasingly documented, serious gaps and inconsistencies exist in the available information. This sketchy information base also complicates finding meaningful and effective responses. For this reason, more systematic efforts to gather more reliable information would be highly desirable.

1. INTRODUCTION

Measures to increase information security enhance trust in online activities, contributing directly and indirectly to the welfare gains associated with the more intense use of information and communication technologies (ICTs). As trust probably benefits society at large, efforts to increase information security may generate positive externalities, spill-overs that not only benefit the investor in security but a sector or even the economy as a whole. An optimal level of security is reached when the direct and indirect benefits of additional security approximate the additional costs of security. Because security is costly, it is rational to tolerate a certain level of insecurity. The cost of security is, however, greatly increased for all stakeholders because of relentless assault by fraudsters and cybercriminals. Two forms of attack that are gaining notoriety are malware and spam. Their financial effects are the focus of this report.

Malware is a summary term for different forms of malevolent software that are designed to infiltrate and infect computers, typically without the knowledge of the owner. During the past two decades, the production and dissemination of malware grew into a multibillion dollar business. As the discussion in sections 5 and 6 below illustrates, the direct and indirect costs of fraudulent and criminal activities using malware likely exceed that number significantly.

Malware puts both the private and the public sectors at risk because both increasingly rely on the value net of information services. All stakeholders across the value network of information services, such as software vendors, network operators, Internet Service Providers (ISPs), and users, are affected by malware and spam. A response to malware and spam is complicated by the fact that spam and malware not only cause costs but also generate new business opportunities and revenue streams. Cost impacts include, but are not limited to, the costs of preventative measures, direct and indirect damages, the costs of remediation, infrastructure costs, and the opportunity costs of congestion. Business opportunities associated with malware and spam include anti-virus and anti-spam products, new and enhanced security services, and additional infrastructure investment in equipment and bandwidth.

Malware has also spawned operations in a legally gray zone in which a legal and illegal economy overlap. Such semi-legal activities include spam-induced sales, bullet-proof Internet hosting, or pump and dump stock schemes. Moreover, malware is generated in and fuels a sizeable underground economy. Such illegal activities include the herding and renting out of botnets, different forms of fraud, and cybercrime. Some of the revenues generated in this underground economy are laundered and injected in the legal economy. This mesh of legal, semi-legal and illegal activities creates mixed and even conflicting incentives for individual stakeholders. Furthermore, it complicates coherent policy responses to the problem.

Until recently, spam and malware could be considered as two separate problems. However, due to the emergence and growth of botnets they are increasingly overlapping and converging. Botnets are networks of malware-infected computers. They are both the origin of the majority of spam messages but are also sustained and extended through spam.¹ Whereas it is fairly safe to claim that malware and spam have negative effects on the ICT value net in the aggregate individual stakeholders are not affected equally and not all are impeded by malware.

¹ See <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html> and FTC, *Spam Summit: The Next Generation of Threats*, Washington, D.C.: Federal Trade Commission, November 2007.

For example, security service providers create business activities from malware. Financial service providers have to weigh the benefits of enhanced security against the potential negative effects on online banking and the efficiency gains associated with it. As they experience costs and benefits differently, stakeholder will adopt a range of responses to the threats depending on their perceived individual costs and benefits but not necessarily based on social costs and benefits. As long as these different responses contribute to improvements overall, they are not problematic. However, if they are at cross purposes, they may aggravate the problems caused by malware. Recent studies of stakeholder incentives and the economics of security showed many instances in which the public interest and individual responses were aligned but also others where they were not.²

Reliable empirical information on the operational and financial aspects of malware and spam is difficult to come by. Many of the available estimates of attack trends and damages are provided by security service providers. While certainly useful, indeed these are often the only available figures, they need to be considered within this context as security service providers may have incentives to over- rather than underestimate security problems. Other information is considered proprietary or only reported if the damage exceeds a certain threshold. The purpose of this study is to sort through the available data and to document the state of knowledge on the financial effects of malware and spam. Where financial information is not available, we attempted to provide operational data if they allowed a provisional glance at the magnitude of a problem.

Given resource and time constraints, the study could not collect original data but had to focus on existing sources, pulling together scattered and scarce information resources. This report also develops an analytical framework, synthesizes, and where possible integrates, fragmented existing knowledge. We also point to gaps in the data that ideally would be filled in future efforts to support the design of better counter-measures against spam and malware.

The next section briefly discusses the problem of malware and the subsequent one gives a short overview of fraudulent and criminal business activities. Section four reviews the available empirical evidence on the financial effects of malware and section five the information base regarding spam. The concluding section is a first attempt at an overall assessment of the welfare effects of spam and malware.

2. THE PROBLEM OF MALWARE

Until a few years ago, the most common types of malware were viruses and worms. More recently other types appeared and are widely distributed, including trojan horses, backdoors, keystroke loggers, rootkits, and spyware. These terms correspond to the functionality and behavior of the malware. For instance, a virus is self-propagating and a worm is self-replicating. Malware is often categorized into “families” (referring to a particular type of malware with unique characteristics) and “variants” (usually a different version of code in a

² See M. J. G. van Eeten, J. M. Bauer with contributions by M. de Bruijne, J. P. Groenewegen, and W. Lemstra, *Economics of Malware: Security Decisions, Incentives, and Externalities*, , OECD STI Working Paper 2008/1 JT03246705, Paris, OECD, 2008, available online at <http://www.oecd.org/dataoecd/53/17/40722462.pdf>. See also R. Anderson, R. Böhme, R. Clayton, and T. Moore, *Security Economics and the Internal Market*, Study for the European Network and Security Information Agency (ENISA), March 2008, available at http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm.

particular family). Malware is put in an information system³ to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners.

2.1. Functioning of Malware

There are two principal ways by which malware can be inserted into information systems to carry out the malicious player's goal. One option is an automated installation and the other is manual installation. Malware compromises the system and may download additional payload code to expand or update its functionality. Once installed, new features and capabilities are therefore easily added.⁴

Malware can be used to distribute spam and to support criminal activities including those based on spam. It can be used to infect systems to gain remote access for the purpose of sending data from that system to a third party without the owner's permission or knowledge. Malware can be instructed to hide that the information system has been compromised, to disable security measures, to damage the information system, or to otherwise affect the data and system integrity. Sometimes it uses encryption to avoid detection or conceal its means of operation.

Acquiring malware is relatively easy and affordable, thus making it available to a wide variety of attackers. A flourishing underground economy exists for its sale and distribution. Furthermore, current generations of malware are easier to tailor to specific purposes and provide attackers with the capability to launch sophisticated attacks beyond their programming skill level. At the same time, the latest generation of malware is increasingly difficult to detect and remove. Variants of it are effective at defeating built-in information security counter-measures. For example, some forms of malware can circumvent strong forms of multi-factor authentication and others have been able to undermine the effectiveness of digital certificates.

Malware not only affects personal computers but also servers. In 2007, Google estimated that one in 10 web pages might serve malware to unsuspecting visitors.⁵ Furthermore, experts predict that malware will increasingly target mobile phones, personal digital assistants (PDAs) and a wide range of other intelligent devices.

2.2. Fraudulent and criminal uses

Early generations of viruses and malware were written and distributed by hackers who sought to enhance their "fame and glory." During the past few years, considerable evidence points to the fact that the generation, distribution and use of malware is driven predominantly by economic interests.⁶ Actors in the underground malware economy will continue to pursue

³ "Information systems" is a generic term referring to computers, communication facilities, computer and communication networks, and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specification and procedures for their operation, use and maintenance. See OECD, *Guidelines for the Security of Information Systems and Networks*, Paris 1992.

⁴ D. Danchev, "Malware—Future Trends," January 31, 2006, p. 3, online at <http://www.linuxsecurity.com/docs/malware-trends.pdf>.

⁵ See <http://news.bbc.co.uk/2/hi/technology/6645895.stm>.

⁶ See Symantec Internet Security Threat Report, September 2007 available at <http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport>; M. Schipka, "The Online Shadow Economy: A Billion Dollar Market for Malware Authors," White Paper, MessageLabs, 2007; ITU, *Botnet*

these activities, as long as benefits from semi-legal and illegal activities outweigh the costs of these activities, including the expected costs of sanctions. Due to the relatively low cost of launching fraudulent or criminal activities in cyberspace and the high potential gains, the economic incentives to expand cyber criminal activity continue to be strong.

Malware, together with other cyber tools and techniques, provides a low cost, reusable method of conducting cybercrime, much of it launched using unsolicited email messages. The majority of spam originates from botnets. According to net security firm Marshal 85 percent of botnet-originated spam comes from only six botnets, with two botnets (Srzibi and Rustock) accounting for more than 60 percent of all spam launched this way.⁷ Malware and spam can be categorized in various ways, for example, by target (business or private individuals), by method, and even by degree of legality (not all spam is per se illegal). A range of methods can be used to reach different objectives. Forms of attacks on businesses include denying access to critical information systems, conducting espionage, and extorting money (e.g., ransom). A main attack vector for individuals is the stealing information (e.g., identity theft) but forms of extortion are also in use. The tools with which these goals are pursued include Distributed Denial of Service (DDoS) attacks, click fraud, phishing, and many more.

Not all unsolicited email is necessarily illegal and/or unwanted by the recipient. Different people have diverging views as to which information constitutes advertising as opposed to unwanted information. Consequently, a precise definition of “spam” is impossible. Due to its low cost, e-marketers will use email to advertise their products and services as long as a sufficiently large share of recipients responds with purchases.⁸ Spam has thus been defined as “information pollution,” the “waste product of senders trying to reach those few recipients who actually want what they [the e-marketers] are offering.”⁹ The glut of information generated by mass e-mail campaigns could therefore be seen as the result of a lack of information about senders and recipients.¹⁰ In contrast, “malicious spam” (or just “spam”) is sent with explicit fraudulent or criminal intent. This differentiation is, for example, reflected in the U.S. CAN-SPAM Act of 2003, which defines the characteristics of illegal activities but continues to allow certain forms of electronic marketing.¹¹

Stealing financial and other personal information has been another prime goal of malware. Over the past five years, information theft (and in particular online ID theft) has been an increasing concern to business, governments, and individuals. Keyloggers and trojans are used to collect personal information directly from infected machines. Botnets are used to host phishing campaigns often using forms of social engineering to trick users into revealing personal information.

Malware has also been implicated in click fraud, a technique relying on infected machines to generate clicks on online advertisements. Online advertisers, such as Google AdSense,

Mitigation Tool Kit, November 2007; and R. Anderson, R. Böhme, R. Clayton and T. Moore, *Security Economics*, supra note 2.

⁷ See J. Leyden, “Most Spam Comes from Only Six Botnets”, available at http://www.theregister.co.uk/2008/02/29/botnet_spam_deluge/; see also Panda Security, *Annual Report 2007*, available at http://www.pandasecurity.com/resources/pro/02dw_Annual_Report_Pandalabs_2007.pdf.

⁸ M. Mangalindan, “Spam Queen: For Bulk E-mailer, Pestering Millions Offers Path to Profit”, *Wall Street Journal*, November 13, 2002, p. A1, argued that even response rates of 0.001 percent (that is, 1 in 100,000) could generate profits.

⁹ M. W. Van Alstyne, “Curing Spam: Rights, Signals & Screens,” *The Economists' Voice*: Vol. 4: Issue 2, Article 4. Available at <http://www.bepress.com/ev/vol4/iss2/art4>.

¹⁰ *Ibid.*

¹¹ See U.S. Congress, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003), Public Law 108–187.

sometimes pay the owners of websites that host their ads for every instance someone clicks on an ad.¹² Attackers can strike a deal with the hosting website to instruct the bots in the botnet to automatically click on the advertisements, generating false “hits.” This process can be further enhanced if the botnet hijacks the default web page of compromised end-user machines so that the “clicks” are executed each time the victim loads the browser.

Extortion, another form of abuse, is often based on the threat of launching a Distributed Denial of Service (DDoS) attack against a website. Popular targets include online gambling and e-commerce sites. A variant compromises the victim’s machine and then denies the victim access to his or her own digital data, resources or other services. To be able to unscramble his/her encrypted data, the user must pay a ransom. Businesses may run into substantial financial losses if their revenue-generating opportunities are affected or even come to a standstill, whether they give in to the extortion or not. Sometimes these attacks are employed by competing firms with the intent of sabotaging the other firm’s business operations.¹³ Several high profile cases in 2006 brought this kind of extortion to the limelight, even though it may be less frequently used as others forms of malware.¹⁴

A rising use for malware is espionage in which malicious code is used to intercept crucial information about a country’s citizens, business or critical infrastructures, threatening the security of individual organizations or even of a whole nation.¹⁵ The United Kingdom recently reported an attack on its public and private critical information infrastructure by trojans.¹⁶

2.3. Factors aggravating the dissemination of malware

The potential versatility and sophistication of malware render it a potent tool. This is further enhanced by several developments in the information and communication value net. Particularly important are the growing number of Internet users, the declining costs of storage and email access, widespread availability of malware tools, and a growing gap between the sophistication of systems and applications and end user awareness. The increased reliance on ICT, the advent of broadband, and technology vulnerability all magnify the problem.

As both the public and the private sector adopt increased use of ICT, the opportunities to attack information systems multiply. The OECD, in 2004, found that 100 percent of the large scale businesses in member countries were conducting transactions online.¹⁷ Medium sized firms are also following that strategy.¹⁸ Individuals as well are conducting an increasing range of activities online. People shop, bank, file taxes, and access information for work, and social networking online. The growth of online consumers and sellers provides cyber criminals with a larger victim base and, other things equal, reduces the probability of identification.

¹² Online advertisers use a range of compensation models. Clickfraud is only possible if a payment is dependent on the number of clicks. If the advertising website is only paid if an actual transaction takes place, clickfraud is less of a problem.

¹³ See D. Pappalardo and E. Messmer, “Extortion via DDoS on the Rise: Criminals are Using the Attacks to Extort Money from Victimized Companies”, *Network World*, May 15, 2005, available at <http://www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html>.

¹⁴ See SOPHOS, *2007 Security Threat Report*, page 8; available online at <http://www.sophos.com/security/>.

¹⁵ See D. Goodin, “Pentagon Attackers stole 'Amazing Amount' of Sensitive Data,” March 6, 2008, available at http://www.theregister.co.uk/2008/03/06/pentagon_breach_assessment/.

¹⁶ See “Targeted Trojan Email Attacks”; NISCC Briefing Issued 16 June 2005 (Centre for the Protection of the National Infrastructure); <http://www.cpni.gov.uk/docs/ttea.pdf>.

¹⁷ OECD Science, *Technology and Industry Scoreboard 2005: Toward a Knowledge-based Economy*, available at <http://lysander.sourceoecd.org/vl=880974/cl=12/nw=1/rpsv/scoreboard/d09.htm>.

¹⁸ *Ibid.*

The availability of increasingly sophisticated applications and a global migration to broadband connectivity contribute to problems generated by malware. With the expansion of broadband access, more customers are taking advantage of always-on connectivity, use wireless hotspots at home or while traveling, and use more and more diverse devices to connect to the Internet. The multiplicity of devices, network configurations, and applications offers new attack vectors for malware to reach a target. In 2007, the ITU quantified the global number of internet users as nearly 1.5 billion. Of this total, nearly 340 million, slightly less than a quarter, used broadband connections.¹⁹ The large number of users helps attackers carry out assaults as they can compromise more computers to, for example, send massive amounts of spam and conduct DDoS attacks. More widespread availability of wireless broadband access allows attackers to use connectivity in public places, further complicating finding these criminals.

A last point that deserves mentioning is technological vulnerabilities. Different and newer types of software and hardware also bring along complexity and associated vulnerabilities that can be exploited by attackers. These effects are sometimes exacerbated by user ignorance as well as a lack of incentives to reveal these vulnerabilities and update software. Microsoft, for example, reported an increase of nearly 2,000 disclosed vulnerabilities from 2005 to 2006.²⁰ At the same time, the firm reported an increase in the number of disinfected machines from less than 4 million at the beginning of 2005 to more than 10 million at the end of 2006 (aided by a malware removal tool introduced by the firm).²¹ Similarly, the security service provider Symantec²² reported a 12 percent rise in the number of known vulnerabilities from the first half of 2006 (January–June) to the second half (June–December) which the firm suspects is primarily caused by the increase in broadband connectivity.

¹⁹ See International Telecommunication Union (ITU), ITU ICT EYE, <http://www.itu.int/ITU-D/ict/statistics/>.

²⁰ See *Microsoft Security Intelligence Report*, July–December 2006; pg. 8; available online at <http://www.microsoft.com/downloads/details.aspx?familyid=af816e28-533f-4970-9a49-e35dc3f26cfe&displaylang=en> (last accessed December 3, 2007).

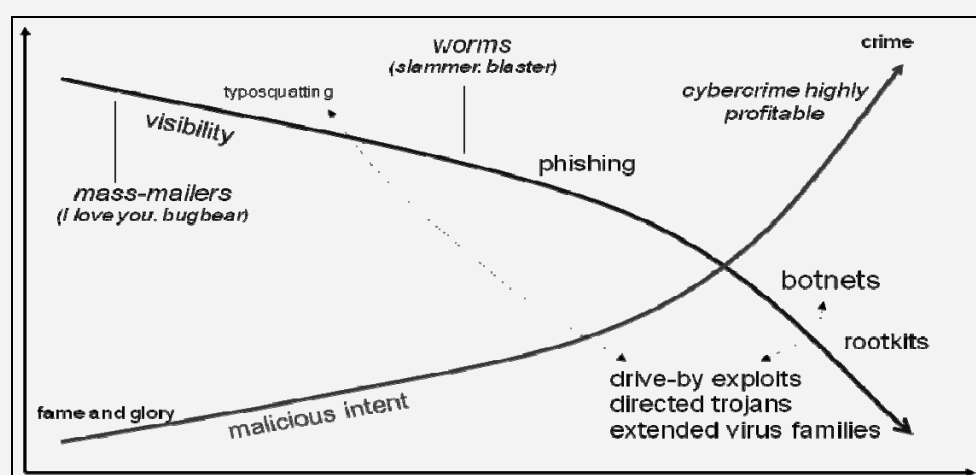
²¹ *Ibid.*, p. 20-21.

²² Symantec Corporation has over 40,000 sensors monitoring network activity in over 180 countries around the world. See *Symantec Internet Security Threat Report*, Volume XI at 38; available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

3. BUSINESS MODELS RELATED TO MALWARE

A diverse cast of actors with widely differing motives populate the malware economy. Main groups are (1) innovators seeking to find security problems to improve the working of information systems; (2) amateurs seeking fame and notoriety without malicious intent; (3) copy catters who usually only replicate simple attacks but often with malicious goals, (4) insiders, usually employees with experience at a particular work place that breach security, and (5) a range of actors in the realm of organized crime.²³ Figure 1 illustrates the evolution of malware in terms of motives from fame seeking but relatively harmless “techies” to criminals motivated by financial gain.

Figure 1. Visibility of malware vs. malicious intent



Source: www.govcert.nl

Malware-based crimes are steadily becoming cross-national or even global in nature, making it very difficult to find the perpetrators. Even if a criminal can be identified, differences in national laws and weaknesses in cross-border cooperation can make prosecution daunting. This has obfuscated our understanding of the underlying motives and demographic profiles of the individuals and groups involved. Consequently, the design of effective countermeasures is greatly complicated.

The malware market and associated activities have expanded and differentiated beyond smaller groups so that apparently mechanisms to increase trust among the many actors are emerging. For example, some malware variants carry a guarantee by the seller to remain undetectable by anti-malware software. Certain versions may include “service level agreements” by which a seller promises to provide a newer undetectable version in case of detection.²⁴

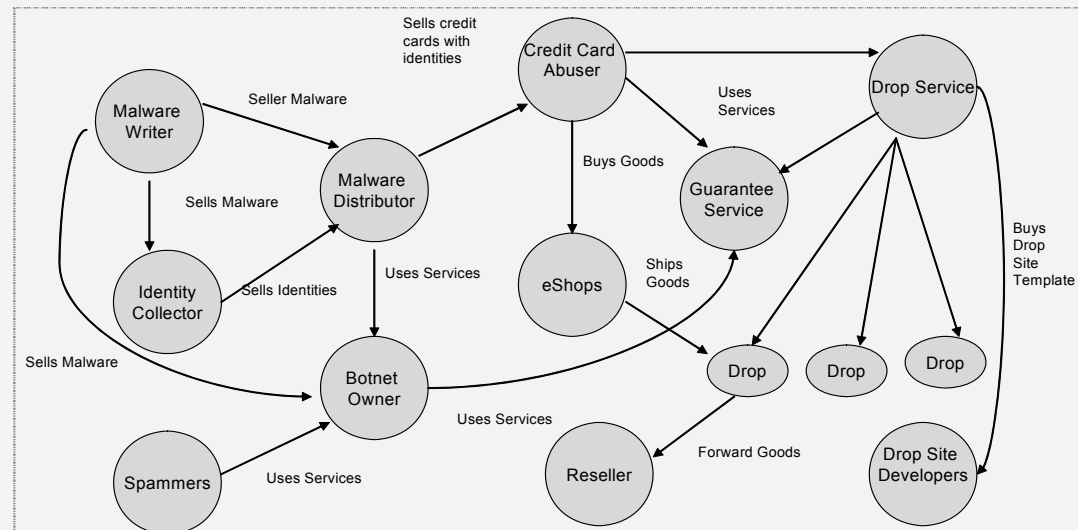
²³ Adapted from McAfee *Virtual Criminology Report 2007*, page 8; available online at http://www.mcafee.com/us/threat_center/white_paper.html.

²⁴ See MessageLabs *Intelligence: 2007 Annual Security Report*, available at <http://www.messagelabs.com/resources/mlireports>

3.1. Division of labor

The cyber criminal market is surprisingly specialized. Division of labor and competition among actors has contributed to a considerable drop in the price of malware. Figure 2 illustrates key players in the malware economy. Given the dynamic nature of this realm, however, the degrees of specialization, and the differentiation of roles are in continuous flux.

Figure 2. Division of labor in the malware underground economy Visibility of malware vs. malicious intent



Source: Source: MessageLabs, 2007

Certain groups of malicious actors seem to be involved in the entire malware ecosystem from the development of malware, acquisition of targets and distribution of spam and/or malware, all the way to laundering the money into a “clean” bank account. Much of the criminal market, however, is divided into segments that have a certain expertise. This expands the opportunity to source partners globally, primarily through Internet Relay Chat (IRC) channels, underground bulletin boards, and online forums.

For example, a malware distributor may buy malware from an author and use services offered by a botnet owner to spread it (see below section 3.2 for a discussion of botnets). Botnets are assembled from thousands to millions of infected computers located around the world. The person running a bot on his or her system is typically completely unaware of it. Performance degradation is at best noticeable during the short periods during which the botnet is active. The system of computers constituting the botnet enables the attacker to efficiently target a large number of individual users and organizations.

Other participants specialize in turning illegally acquired information into money, be it from stolen credit cards or identity theft. Stolen credit card information, for example, may be used to make purchases for parties known as “drops.” These drops, in turn, post the acquired merchandise on eBay or sell it immediately for cash. This way balances in credit card accounts are extracted to the criminals and the funds eventually laundered.

3.2. The role of botnets

Three principal types of actors are involved in the illegal activities associated with botnets and their uses: (1) malware authors write and release malicious code; (2) bot-herders assemble and run the botnets, operating them through “command-and-control” channels; (3) and clients commission new malware development or botnet activity in order to accomplish fraudulent and criminal objectives such as spam distribution, identity theft, DDoS attacks, etc.²⁵ There is plenty of evidence that organized crime gangs are as involved in all stages of the botnet economy as are individual users. These criminals use a variety of tactics such as “mules” and “drops,” as well as electronic fund transfer and offshore banking services to orchestrate the flow of money between different countries.²⁶

High speed Internet connections and increased bandwidth also allow for self-sustaining attacks through compromised information systems. In this model, malware is initially inserted into a few vulnerable computers. The compromised Internet-connected bots are in turn used to scan and compromise more computers by installing malware through spam or from hosted Trojan sites. Gradually, the number of infected machines recruited into the botnet is increased. The compromised computers can then be rented to initiate other forms of cyber fraud or crime. These actions could thus be considered as attacks that are indirectly caused by malware. The whole system is self-sustaining and perpetuating a vicious circle.

Criminals have advanced technologically to the point where they are able to recognize if their activities are being detected. This makes it more challenging to identify them as they switch services or evade detection by shifting their activities to another compromised system. According to Panda Security, as of March 10, 2008, 30 percent of computers on the Internet were infected and posed latent threats. About half of these machines were active.²⁷

Despite evidence of co-operation between botnets²⁸ there is also competition within the botnet economy, sometimes resulting in fierce attacks against one another as each botnet tries to protect its compromised node.²⁹ The highly illegal and competitive nature of the botnet underground economy has led to the development of a well-developed system of self-regulation and policing to identify and launch counter attacks on “bad actors” (a catch-all term for fraudsters who try to cheat other fraudsters, undercover law enforcement or security employees, etc.)³⁰.

The year 2007 brought with it new tactics used by cyber criminals. Not only have they come up with newer ways to distribute spam but they have also found newer methods to spread malware. Increasingly, rather than attaching the malware to an email, spam contains links that connect to infected websites. Malware is downloaded just by visiting the webpage (so-called “drive-by” downloads). The proportion of emails with links to malicious websites increased from 3 percent in the beginning of the year to 25 percent in December. Postini, a wholly owned subsidiary of Google, estimated that approximately 10 percent of websites are infected with malware.³¹

²⁵ J. Franklin, V. Paxson, A. Perrig, S. Savage, “An Inquiry into the Nature and Cause of the Wealth of Internet Miscreants”, paper presented at CCS’07, October 29-November 2, 2007.

²⁶ ITU, *Botnet Mitigation Toolkit*, Geneva, November 2007.

²⁷ See <http://www.infectedornot.com/usa/>.

²⁸ For example, the sending of spam from multiple botnets simultaneously, see Panda Security, *Annual Report 2007*, supra, note 9.

²⁹ See J. Leyden, “Malware Removes Rival Rootkits,” February 28, 2008, available at http://www.channelregister.co.uk/2008/02/28/rootkit_wars/.

³⁰ ITU, *Botnet Mitigation Tool Kit*, Geneva, November 2007.

³¹ See <http://www.postini.com/>.

3.3. The geography of malware and spam

The global reach of information and communication networks allows different actors to pursue their fraudulent and criminal activities in a geographically dispersed and distributed fashion. Although other motives are often at play, criminal activities predominantly follow an economic logic. In selecting an optimal location to launch malicious activities or a location to target with attacks, different trade-offs are taken into account. It may be economically rational to locate criminal activities in places where law enforcement is weak and/or where it is comparatively easy to find the required hosting services as this reduces the costs of committing the crime.

Regarding the location of bots, several tradeoffs will be considered. On the one hand, it may be more efficient to place bots in countries with good Internet connectivity. However, these will typically also be nations with better law enforcement, laws attempting to keep malware at bay, and ISPs that pursue suspicious activity more vigorously. Therefore, for certain types of activities, it may be advantageous to launch attacks from nations with poorer connectivity but without relevant cybercrime legislation or weak law enforcement.

While these tradeoffs are relevant, actual attack trends suggest that malicious actors do not weigh these pros and cons in a static way. Rather than opting for specific regions or countries, they frequently move their operations from one location to the next in response to changing opportunities. One reason could be that ISPs in their current location may have become more proactive in combating spam or botnet activity. Another reason is that the location has become less attractive as it is increasingly blacklisted. In short, the geographical origin of malware is highly dynamic and distributed.

MessageLabs reports disaggregated data from the subset of messages intercepted by its software that originated from new and unknown sources and hence was subjected to more detailed analysis. This data indicates that in 2007 the top five countries targeted³² with email viruses were India with a 2.92 percent virus interception, Germany with 1.95 percent, Switzerland with 1.66 percent, France with 1.59 percent and United Arab Emirates with 1.55 percent. MessageLabs also detected differences by sector. The top 5 industries targeted by viruses were education with 1.76 percent, chemical/pharmaceutical with 1.33 percent, wholesale with 1.17 percent, retail with 1.09 percent and accommodation/catering with 1.05 percent.³³

Spammers can change apparent source addresses fairly dynamically, for example, using what is known as fast flux techniques. Nonetheless, data from Spamhaus, which measures the number of IP addresses from which spam is sent, indicate that the emergent aggregate geographic pattern of spam origination is fairly stable. The top 10 countries continue to be the United States, China, Russian Federation, United Kingdom, South Korea, Germany, Japan, France, Canada, and Taiwan. During the period February through March 2008, the ranking of the top 10 countries identified as sources of spam remained the same.³⁴ The list of the 10 worst ISPs was less stable. Nonetheless, eight of 10 ISPs remained in the top, although

³² MessageLabs collects billions of messages processed through the MessageLabs network to provide real-time data and analysis. Some experts argue that the data collection method is insufficient to generate a representative picture as MessageLab filters can be bypassed.

³³ See MessageLabs, *2007 Annual Security Report*, available at <http://www.messagelabs.com/resources/mlireports>.

³⁴ See <http://www.spamhaus.org/statistics/countries.lasso>.

marginal changes in ranks occurred.³⁵ Similarly, Spamhaus data suggests that a relatively small and stable group of spammers is responsible for much of the traffic.³⁶

In terms of volume of spam SOPHOS estimated that during the fourth quarter of 2007 the U.S. was the leading source of spam, followed by Russia, China, and Brazil.³⁷ Data collected by Team Cymru also indicates a similar geographic distribution of botnet and malware activity.³⁸ Symantec expects the U.S. to remain the top country until another nation will surpass it in the total number of broadband connections.

Another source of data, MessageLabs, uses its spam filtering technology Skeptic™ to create more detailed data on messages that needed further analysis. This way, spam directed to specific countries in local languages can be identified. The firm found that in 2007 the top five countries targeted by email spam were Israel with a 68.9 percent of spam interception, Hong Kong with 64.5 percent, Germany with 55.2 percent, the United States with 54.2 percent, and France with 53.8 percent. Using the same method, the firm found that the top 5 industries targeted by spam were manufacturing with 61.0 percent, agriculture with 60.4 percent, education with 57.8 percent, IT services with 54.3 percent and marketing/ media with 5.7 percent.³⁹

Overall, there seems to be a shift in the origination of spam. In its State of Spam Report in February 2008, Symantec found that the percentage of spam messages originating from Europe was greater than the percentage of spam messages originating from North America. During the preceding three months, approximately 44 percent of all spam email originated from Europe versus 35.1 percent from North America. This new picture has emerged and remained constant since the beginning of November 2007. When Symantec first started recording this data in August of 2007, 30.6 percent of spam originated in Europe while 46 percent originated in North America⁴⁰

³⁵ See <http://www.spamhaus.org/statistics/countries.lasso>.

³⁶ See <http://www.spamhaus.org>.

³⁷ See "Russia Emerges as Spam Superpower, as Asia and Europe Overtake North America", available at <http://www.sophos.com/pressoffice/news/articles/2008/02/dirtydozfeb08.html>.

³⁸ See <http://www.team-cymru.org/>.

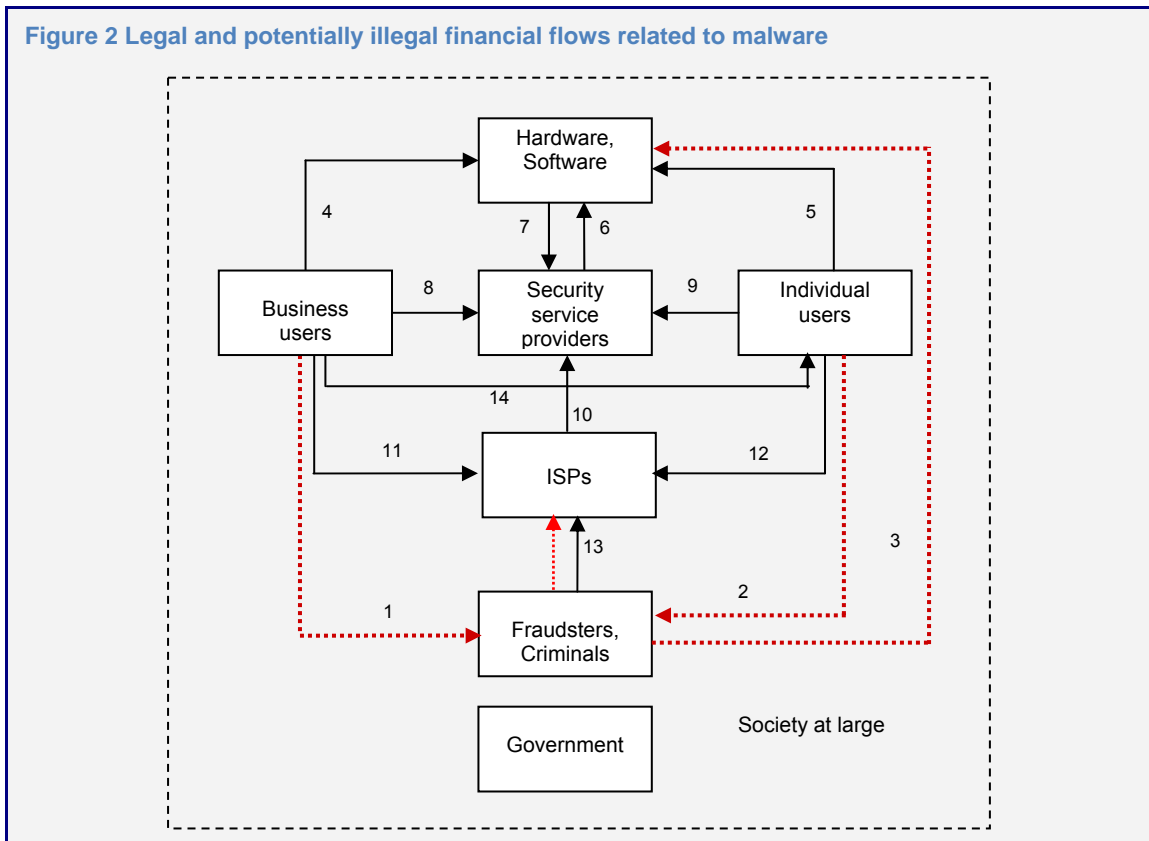
³⁹ See MessageLabs, *2007 Annual Security Report*, available at <http://www.messagelabs.com/resources/mlireports>.

⁴⁰ See "The State of Spam, A Monthly Report—February 2008", available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_February_2008.pdf.

4. A CONCEPTUAL FRAMEWORK FOR MODELING FINANCIAL ASPECTS OF MALWARE AND SPAM

Numerous financial flows take place in the malware and spam ecosystem. This section develops a conceptual framework for the subsequent discussion of the empirical data.

Figure 2 Legal and potentially illegal financial flows related to malware



Legend (solid lines: legal; dotted lines: potentially illegal financial flows)

- 1 Extortion payments, click fraud, compensated costs of ID theft and phishing
- 2 Uncompensated costs of ID theft and phishing, click through, pump and dump schemes, Nigerian 419 scams, and other forms of consumer fraud
- 3, 4, 5, 6 Hardware purchases by criminals, corporate and individual users
- 7, 8, 9, 10 Security service purchases by hardware manufacturers, corporate and individual users, ISPs
- 11, 12, 13 ISP services purchased by corporate and individual users, criminals
- 14 Payments to compensate consumers for damages from ID theft (if provided)

Figure 3 depicts aggregate flows between main groups of actors. Within each category, complex financial transactions take place. Some of the transactions are legal whereas others are clearly illegal. Moreover, there are interactions between the legal and illegal realm, as some legal transactions are caused or at least affected by illegal transactions. For example, the revenues of security service providers are positively influenced by the extent of criminal activity. In that sense, a positive externality exists between cyber criminals and security service providers.

Development of accurate measures of these flows is complicated by the large number of legal and illegal players and the elusive nature of some of the transactions. Most of the financial flows between players in the underground cybercrime economy are not or only partially known. Due to the sensitive nature of some information, many of the financial flows even in the legal segment of the economy, such as the extent of damages related to malware, are not systematically tracked. Even if such attempts existed, it would be difficult to estimate the exact amount of financial losses associated with such activities because of the complicated nature and effects of attacks. Moreover, in cases where a company, organization or the government has data regarding financial losses, management may be reluctant to make it public because it might affect the firm's reputation. No systematic and aggregate figures exist as to investment in preventative measures. In as far as the information exists, it is typically considered proprietary and not released to the public.

To describe Figure 3 in more detail, it depicts aggregate financial flows corresponding to transactions between main players. Solid lines represent legal forms of business transactions whereas dotted lines indicate transactions of a potentially illegal nature. All users purchase security services (lines 7-10). Although the exact magnitude of the flows from each group of players is not exactly known, the total revenue generated by security service providers can serve as a proxy for them. Both legitimate and illegitimate users purchase services from hardware manufacturers and software vendors (lines 3-6). Likewise, both legitimate and illegitimate users buy from ISPs (lines 11-13). For example, cyber criminals may buy bullet-proof hosting services at premium prices.⁴¹

Sources of revenues of cyber criminals include extortion payments from companies for click fraud (line 1) as well as funds appropriated from individual users through identity theft but also voluntary if fraudulent payments in the context of click through, pump and dump schemes, or phishing attacks. In addition to these transactions between players, financial flows may happen within a sector. For instance, as discussed above, considerable division of labor exists within the criminal segment, contributing to financial flows internal to that segment.

Whereas Figure 3 represents the financial flows between these aggregates, it does not necessarily depict the incidence of costs. In many countries, for instance, financial institutions (part of the corporate user aggregate) hold their customers harmless for losses incurred in the context of phishing attacks. This practice constitutes, on the one hand, a financial flow from consumers to criminals. At least initially, however, it is the banks who bear the financial burden. Only in the medium and long run will financial institutions attempt to pass the costs of fraud on to consumers.

The whole system represented in Figure 3 is embedded in societal institutions. Some cost of malware and spam are imposed on government and society at large, be it in the form of law

⁴¹“Bullet-proof hosting” also “bulk-friendly hosting” refers to hosting services that give their customers great freedom as to the type of content they may upload. Some of these services are not in compliance with national laws and have been used by spammers. Many but not all of the bullet-proof hosting services are outside of the country of the content provider.

enforcement costs or in the form of opportunity costs due to the malware-induced slower adoption of productivity-enhancing applications of ICT.

As mentioned, malware and spam are intricately related phenomena. For the sake of expositional clarity, we will, in the following two sections, discuss empirical evidence as to their operational and financial effects separately. Operational impacts are identified even if no reliable cost figure can be associated with that effect. In addition, we review the evidence as to the known financial effects of malware and spam.

5. FINANCIAL AND OPERATIONAL EFFECTS OF MALWARE

Estimates of the costs of malware vary widely and the empirical knowledge base is sketchy and incomplete. Each empirical data source and method of measurement typically has its own advantages and disadvantages. Many statistics are provided by stakeholders who might have an incentive to underreport or overreport threats.⁴² More accurate data is typically available for narrowly defined segments of the global or national economy. It is usually not straightforward to derive estimates for the whole economy from these more specific surveys. In most cases, very strong assumptions would have to be made to arrive at such scaled-up numbers. This section summarizes the most important data related to malware and the next section elaborates on the related problem of spam.

5.1. Direct and indirect costs of malware

Several public and private sector organizations have tried to quantify the direct and indirect costs of malware. The following sub-sections differentiate between findings at an aggregate level, for businesses, and individual users.

Costs at an aggregate level

Computer Economics attempted to quantify the worldwide damage caused by malware. The survey of 52 information technology professionals and managers estimated the direct worldwide damage due to malware to be US\$ 13.2 billion in 2006. This was a decline from the figures of US\$ 14.2 billion in 2005, and US\$ 17.5 billion in 2004.⁴³ A large proportion of companies in the survey kept a record of the frequency of malware incidents but was unable to put a specific number on financial losses incurred.⁴⁴ Although the survey is the only one applying a global perspective, one has to keep in mind that it is based only on a small number of respondents.

According to Computer Economics, the decline probably reflects two main developments. First, anti-malware technology is becoming more widely employed and more effective against certain types of threats. Second, Computer Economics observed that whereas the direct costs may be declining the indirect or secondary costs may be increasing. These include preventative costs (e.g., hardware, software, IT security staff), secondary costs of secondary attacks, insurance costs, as well as intangible costs such as brand damage and loss of market share. Many of these cost components are difficult to measure and were not included in the estimates of direct damages above.

⁴² See R. Anderson et al., *Security Economics*, supra, note 2.

⁴³ Computer Economics, *2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other Malicious Code*, p. 5, available at

<http://www.computereconomics.com/page.cfm?name=Malware%20Report>

⁴⁴ *Ibid*, page 9.

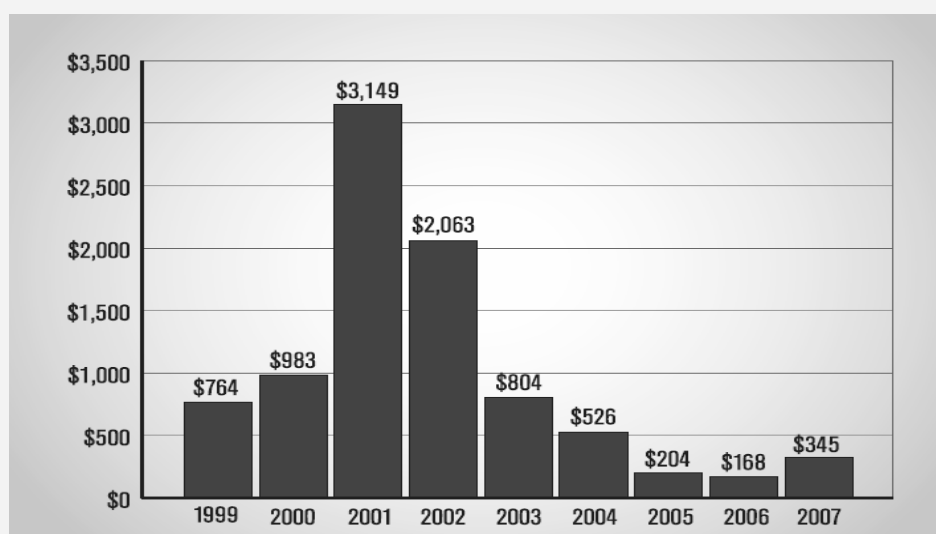
An alternative number provided by the U.S. Federal Bureau of Investigation (FBI) estimates that in 2005 computer crime cost the U.S. economy US\$ 67.2 billion, approximately 0.5 percent of GDP.⁴⁵ The considerable gap between these two sources can be explained by the focus of the Computer Economics survey on direct costs of malware whereas the FBI report is more inclusive.

Costs for businesses

Probably the most-quoted data source is the CSI (formerly CSI/FBI) Annual Computer Crime and Security Surveys.⁴⁶ This anonymous survey, in 2007 its 12th consecutive year, reflects the experience of the U.S. community associated with the Computer Security Institute and its conferences. While not fully representative of this community (the survey response rate is about 10 percent) it reflects major trends within it. The 494 respondents to the 2007 survey represented a broad range of sectors, including finance (20 percent), state, local and federal government (13 percent), education (11 percent), information technology (11 percent), and manufacturing (95 percent).

In 2007, practitioners from 494 organizations responded, of which 194 were able to provide numerical estimates of the losses that they had experienced during the year. The total loss due to cybercrime for the reporting organizations was estimated to US\$ 66.9 million. By far the highest damage was caused in the category of financial fraud (US \$21.1 million), followed by damage from viruses/worms/spyware (US \$8.9 million) and damage from system penetration by outsiders (US \$ 6.9 million). In 2007, these aggregate numbers translate into average losses per reporting firm of approximately US\$ 345,000.

Figure 3 Average reported losses in CSI surveys 1999-2007 (\$000)



Source: CSI (2007), p. 16.

⁴⁵ See Federal Bureau of Investigation, *2005 FBI Computer Crime Survey*. See also Government Accountability Office, "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats"; June 2007, available online at <http://www.gao.gov/new.items/d07705.pdf>.

⁴⁶ CSI, *2007 CSI Computer Crime and Security Survey*, San Francisco, CA: Computer Security Institute, available at http://www.qocsi.com/forms/csi_survey.jhtml.

Figure 4 shows the average losses reported in the CSI surveys since 1999. Although the composition of the respondents changed slightly from year to year, according to CSI, it remains generally representative of the community. The peak loss was experienced in 2001 with more than US\$ 3.1 million per reporting organization. Ever since, most likely due to increased awareness and more systematic investment in computer security, the damages declined to a low of US\$ 168,000 per reporting organization in 2006. In 2007, the downward trend reversed as damages per reporting organization doubled to US\$ 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. First, these estimates do not include the cost of preventative measures. The amount spent by companies on information security falls in a broad range. Gartner estimates that the total global revenue of security service providers in 2006 was US\$ 7.5 billion. On the user side, 61 percent of the respondents in the CSI survey reported security costs of 0-5 percent of the total IT budget, 23 percent reported a share of 5 percent or higher of the IT budget.⁴⁷ A recent study by the TU Delft and the Quello Center at Michigan State University revealed similar numbers.⁴⁸

Second, these direct costs do not include the costs of other indirect preventative measures such as expenses of training personnel to adopt security-conscious work procedures or labor expenses for researching malware in order to disinfect infected machines. Respondents to the CSI survey indicated that a small share of the IT security budget is spent on awareness training (48 percent responded that 1 percent or less of the IT security budget was spent for that purpose).⁴⁹ However, it is probably safe to assume that this represents only a fraction of the total cost of personnel-related preventative measures.

Third, these direct costs do not include opportunity costs to society at large. In as far as the perception of security threats slows down the adoption of efficiency-enhancing ICTs throughout society we may also suffer from unrealized efficiency gains. The existence of such opportunity costs is, however, difficult to establish and nearly impossible to quantify. The empirical evidence is somewhat contradictory. Surveys by the Pew Internet & American Life Project in 2003 and subsequent years indicated considerable concerns of individual users about spam. In contrast, panelists at the 2007 FTC Spam Summit, while reporting negative effects on consumer trust, presented evidence of declining concerns by individuals.⁵⁰

A recent report by the U.S. Federal Deposit Insurance Corporation (FDIC) contained data on the damages caused by malware to the financial services industry during the second quarter of 2007. Although the report was not made public, some aggregate numbers are available. The report focuses on suspicious activity reports (SARs), which need to be filed in cases of suspicious or fraudulent transactions exceeding US\$ 5,000. The number of computer intrusion related SARs in the second quarter of 2007 was 536 with an average loss per

⁴⁷ *Ibid*, p. 7.

⁴⁸ See M. J. G. van Eeten, J. M. Bauer with contributions by M. de Bruijne, J. P. Groenewegen, and W. Lemstra, *Economics of Malware: Security Decisions, Incentives, and Externalities*, OECD STI Working Paper 2008/1 JT03246705, Paris, OECD, 2008, available online at <http://www.oecd.org/dataoecd/53/17/40722462.pdf>.

⁴⁹ CSI, *2007 CSI Computer Crime and Security Survey*, San Francisco, CA: Computer Security Institute, available at http://www.gocsi.com/forms/csi_survey.jhtml, p. 8.

⁵⁰ See FTC, *Spam Summit*, supra, note 1, p. 9-10.

intrusion of US\$ 29,630.⁵¹ Prior to 2007, the number of SARs during the second quarter had been 503 in 2004, declined to 293 in 2005 and increased again to 370 in 2006. In 2006, the average loss had been US\$ 10,536. The number of credit card fraud cases increased from 6,301 during the second quarter of 2005 to 7,962 during the same period in 2007. Likewise, the number of debit card fraud cases increased from 777 in the second quarter of 2005 to 1,142 in the second quarter of 2007.⁵² It is important to keep in mind that the actual number of fraud incidents will be substantially higher, as many cases – or most cases, as some argue – do not cross the reporting threshold of US\$5,000.

Costs to consumers

It is even more difficult to assess the financial losses inflicted by malware to individual consumers although there is scattered evidence that damages can be very large. Such costs have different components. They may result in direct damages to hardware and software as well as financial and other damages due to identity theft or other fraudulent schemes (discussed in section 6 below). The range of estimates differs, although the emerging overall picture is quite coherent.

Based on information collected from 2,000 participants in its 2006 State of the Net survey, *Consumer Reports* projected total losses for U.S. consumers of US\$ 7.1 billion. 1 in 5 consumers reported problems with viruses, causing costs of US\$ 3.3 billion. Fixing problems caused by spyware cost consumers US\$ 1.7 billion and losses from phishing attacks amounted to US\$ 3.1 billion.⁵³ The total damage in 2006 was down from the estimated US\$ 8.4 billion in 2005.

Another estimate for the U.S. aimed at quantifying the direct damages to repair or replace information systems infected with viruses and spyware. According to the report, consumers paid nearly US\$ 7.5 billion over two years to repair or replace hardware.⁵⁴

5.2. Illegal revenues associated with malware

It is increasingly easy to set up and even create one's own bot. Specific skills or technological knowledge is not a criterion anymore as there is a wide selection of readily available tools online including access to the malware source code.⁵⁵ There are several "off-the-shelf" kits with ready-made Trojans that can be easily downloaded. The costs of such services are reportedly low and estimated to be as little as US\$ 2,000.⁵⁶ Botnets can be leased at an estimated price of about US\$ 50–60 per 1,000–2,000 bots.⁵⁷ Another source quotes prices of 2.5 to 6 cents per bot per week depending on the configuration.⁵⁸

Some actors offer a complete range of services. They develop, maintain and sell malware, botnets, spam transmission software, CDs full of addresses harvested from web pages, lists of

⁵¹ See B. Krebs, "Banks: Losses from Computer Intrusion up in 2007", http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html?nav=rss_blog.

⁵² *Ibid.*

⁵³ See *Consumer Reports*, September 2007, pp. 30-31, available at <http://www.ConsumerReports.org>.

⁵⁴ See *Consumer Reports*, national survey 2006.

⁵⁵ See McAfee *Virtual Criminology Report 2007*, page 6; available online at http://www.mcafee.com/us/threat_center/white_paper.html.

⁵⁶ See MessageLabs, *Intelligence: 2007 Annual Security Report*, available at <http://www.messagelabs.com/resources/mlireports>

⁵⁷ *Ibid.*

⁵⁸ See M Handley, "DoS-resistant Internet Subgroup Report", presentation at University College, London.

open proxy servers, and lists of open simple mail transfer protocol (SMTP) relays. Lists of email addresses are now fairly cheap and usually cost about US\$ 100 for 10 million addresses. Some provide servers and bandwidth, charging around US\$ 300 per million messages sent.⁵⁹ This allows for the whole process to be carried out in an inexpensive manner.

Some malicious actors also rent component services such as bullet-proof hosting, email lists, or services offered by botnet herders. However, other actors in the underground economy act as free-riders, taking advantage of the existing information and communications infrastructure without compensation. Thus, the cost of bandwidth, Internet connectivity, email addresses and web hosting used to operate a botnet are typically absorbed and borne unwittingly by end users, ISPs, and other participants in the value net.

As described above, middlemen are typically involved in selling and marketing the stolen information (e.g., identities) for monetary benefits. An identity can sell for as low as \$5. It can include the person's name and address, a passport or driver's license scan, credit card numbers and bank account details. Credit card numbers often sell for 2-5 percent of the remaining credit balance on the cards in question⁶⁰. Identity thieves also offer specialized services to their customers. Identities may be sold sorted by country, industry, role, and credit cards sorted by remaining balance.

5.3. Operational effects on cyber infrastructure

Although no financial data is available, activities in the underground internet economy also affect the operations of the entire cyber infrastructure. Therefore, it seems justified to present, in conclusion, available evidence as to the operational interruptions of that infrastructure. These attacks cause costs that will show up in the operational data of the organizations attacked but may not be identified as costs of security.

The *Worldwide Security Infrastructure Report* of September 2007 identified the most urgent threats in the cyber world (Figure 5 above). The various threats were studied according to the effect they had and if the system was the primary target of an attack or only a secondary target.

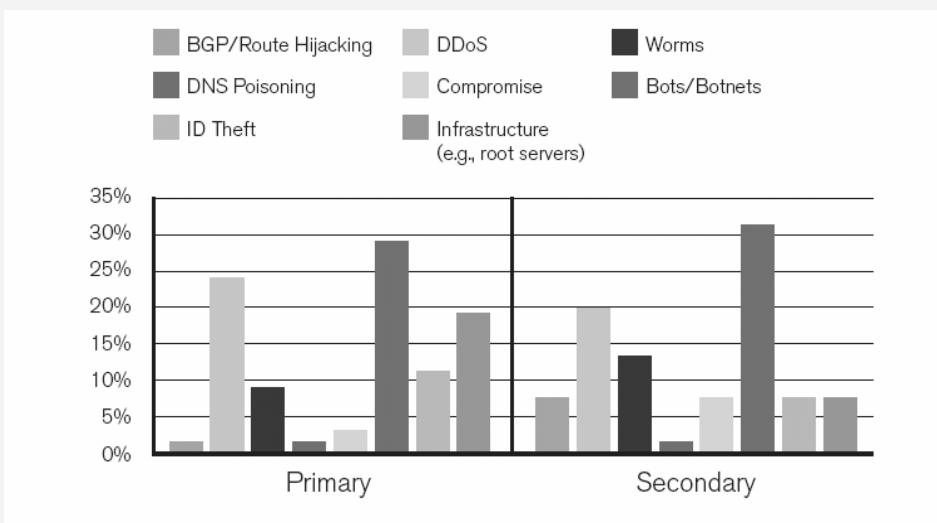
The primary attack targets are depicted in Figure 6. The data was collected by asking respondents of their perception of the primary target of an action or actionable attack.⁶¹ As these categories are not mutually exclusive respondents were allowed multiple answers.

⁵⁹ See S. Vaknin, "The Economics of Spam," available at <http://www.webprnews.com/topnews/2005/06/13/the-economics-of-spam>

⁶⁰ See M. Schipka, "The Online Shadow Economy: A Billion Dollar Market for Malware Authors," White Paper, MessageLabs, 2007.

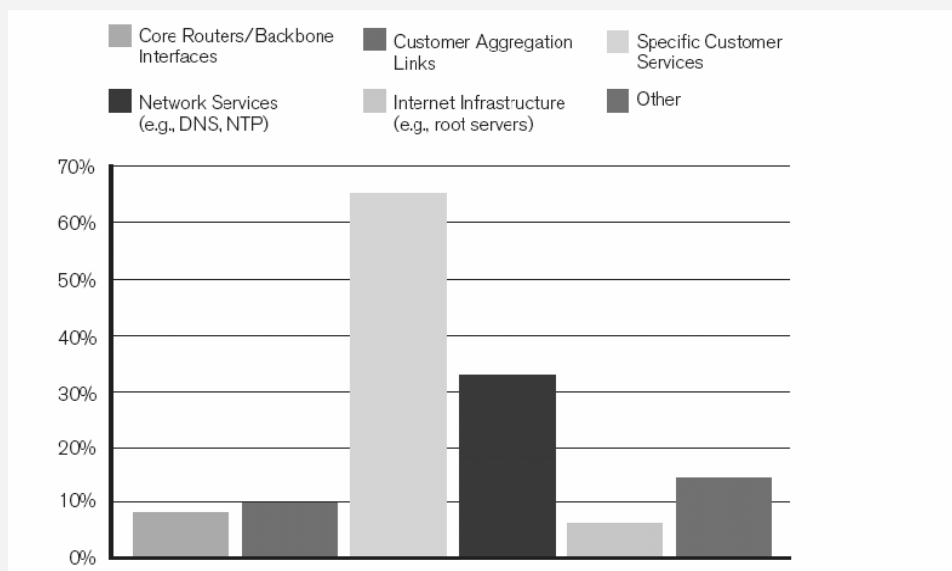
⁶¹ Survey conducted by Arbor Networks, Inc., covering the 12-month period between July 2006 and June 2007.

Figure 4 Threats to cyber infrastructure



Source: Arbor Networks, Inc., 2007.

Figure 5 Primary attack targets



Source: Arbor Networks, Inc., 2007.

6. FINANCIAL AND OPERATIONAL EFFECTS OF SPAM

As discussed, malware and spam are increasingly overlapping. Nonetheless, there are aspects of spam that justify a separate treatment. Most importantly, whereas most of recent sophisticated malware, with the exception of DDoS attacks, do not consume significant computing and communication capacity, much of spam is still based on the economics of large numbers and generates non-negligible traffic volume. In 2007, Web, e-mail and file transfer represented 21.3 percent of consumer IP traffic, making it the second largest category after P2P, which generated 54.4 percent of total traffic.⁶² Cisco estimates that this share will remain stable, making up 22.4 percent of consumer IP traffic by 2011.⁶³ Nonetheless, e-mail is likely only a small fraction of this broader category of traffic.

This may further change in the future as recent forms of malware and spam are becoming more targeted, perhaps reducing the overall traffic volume associated with spam. As in the case of malware, empirical data on spam is incomplete and specific numbers vary widely. This section reviews the available evidence as to the financial and operational burden of spam on the information and communications value net and the indirect effects of spam due to the associated fraudulent and criminal activities.

Traditionally, spamming has been defined as the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. More recently, some spam has become more targeted and in the case of “whaling” sent to individuals with almost surgical precision. The most widely used form of spam is email spam, which targets individual users with direct mail messages. Email spam lists are often created by scanning Internet mailing lists, searching the Web for addresses, or by harvesting Usenet postings. However, the term is also applied to similar abuses on other media platforms. Among the many other forms of spam are messaging spam (“SPIM”, using instant messaging services), mobile phone spam (m-spam, directed at the text messaging service of a mobile phone), VoIP spam (sometimes dubbed “SPIT” for spam over Internet telephony), and the oldest form, newsgroup spam (targeting usenet groups).

6.1. Direct and indirect costs of spam

Spam entails a multitude of costs for the recipient, players in the ICT value net used to deliver spam, and for society at large. Whether a business or private account is targeted, the recipient typically will spend some time sorting through email and deleting unwanted messages, even when protected by spam filters, and thus incurs opportunity cost of time. Spam also increases the cost of ISPs and other players in the ICT value net. Finally, as spam is used to achieve other fraudulent or criminal goals, potentially significant indirect costs are associated with it.

Effects on businesses

In a business environment, spam causes several forms of cost, including the cost of security services, hardware and software; the costs of awareness raising and re-training; the cost of lost productivity due to time spent deleting unwanted emails (and searching for accidentally deleted ones), and the cost of additional storage capacity. In addition, businesses also suffer from indirect effects of spam, for example, by having to pay higher prices for ISP services, who will try to recover their own elevated costs due spam through higher prices.

⁶² Cisco, “Global IP Traffic Forecast and Methodology, 2006-2011”, White Paper, San Jose, CA: 2006, p. 4.

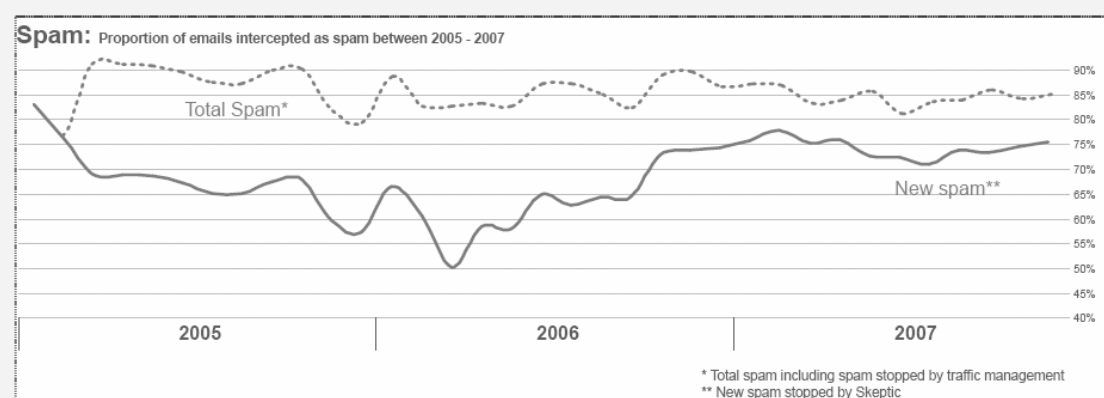
⁶³ *Ibid.*

The opportunity cost of time spent sorting through and eliminating spam from email inboxes is dependent on the cost of time of an employee, the skills of the organization and the individual user to deal with spam, the sophistication of filtering technology, and the audacity of attacks. Likewise, other spam-related costs will be dynamic numbers that will fluctuate in response to these and other factors. In 2005, Ferris Research estimated the global cost of spam to be US\$ 50 billion.⁶⁴ At the national level, the cost was estimated to be highest for the U.S. with US\$ 17 billion, followed by Japan with US\$ 5.2 billion and Germany with US\$ 4.5 billion. Two years later, Ferris estimated the global cost of spam at US\$ 100 billion and the U.S. burden at US\$ 37 billion. Also in 2007, Nucleus Research Inc. reported that the costs of spam management to U.S. businesses alone were US\$ 71 billion.⁶⁵

At the ISP level, the costs of spam are part and parcel of the IT security budget discussed in the previous section. No specific numbers that separate the cost of spam are available. Until a few years ago, ISPs considered spam an individual user problem. However, with a massive increase in spam, ISPs faced potentially costly investments in email infrastructure. The share of unwanted mail in overall mail helps shed some light on these potential costs.

During the past few years, depending on the source of information and the specific metric used, about 85-95 percent of emails have been considered spam. One source of data is the Messaging-Anti-Abuse Working Group (MAAWG) which collects data from ISPs collectively serving more than 240 million mailboxes. MAAWG reports “abusive” messages, which is the sum of dropped connections and blocked/tagged emails. In the case of dropped and prohibited (“null-routed”) connections, no email actually reaches a mailbox. As such connections are only counted as one abusive mail MAAWG numbers likely represent a lower bound of the actual share of abusive emails in overall email traffic. Nonetheless, MAAWG statistics indicate a steadily increasing share of dropped connection and blocked/tagged inbound emails per delivered unaltered email. During the second quarter of 2007, MAAWG reported 86.7 percent abusive mail.⁶⁶

Figure 6 Spam rates 2005-2007



Source: MessageLabs, 2007.

⁶⁴ Ferris Research, The Global Economic Impact of Spam, research report, San Francisco, CA: 2005.

⁶⁵ See J. Edwards, “The Real Cost of Spam,” *IT Security*, December 10, 2007, available at <http://www.itsecurity.com/features/real-cost-of-spam-121007/>.

⁶⁶ See MAAWG, E-mail Metrics Program: The Network Operator’s Perspective, report #6, second quarter 2007, available at <http://www.MAAWG.org/>.

According to data Message Labs, a security service provider, the overall proportion of spam intercepted in 2007 was around 84.6 percent of the total number of emails, compared to 86.2 percent in 2006. Of this volume, 73.9 percent was from new and previously unknown sources as compared to 63.4 percent for 2006 (see Figure 7).⁶⁷

Given the relative costs of filtering, rather than expand network infrastructure, ISPs started to reconfigure their networks and to filter incoming traffic to reduce the amount of received spam. Some ISPs have also started blocking port 25 to reduce outgoing spam messages. Finally, many ISPs began offering their customers additional spam filtering tools. Industry data suggest that these measures could reduce spam at the level of an ISP by 85-90 percent.

Spam and its effects also increases the number of customer service calls. ISPs have adopted widely different approaches for their back offices and their complaint and abuse desks in particular. Data collected in the context of a study for the OECD indicate a wide range of practices.⁶⁸ ISPs face a trade-off between investment in capital equipment that facilitates automated responses to spam, staffing a larger abuse and help desk or being less responsive to abuse notifications. The number of full-time abuse desk employees per 100,000 customers varies by an order of magnitude and ranges from 0.24 to 2.5 for the residential market. It is typically much higher in the business market. Consequently, the costs of ISPs for spam-related customer support also vary considerably.

Message Labs, in November 2006 tried to study the demographics of the businesses targeted with spam. Their survey revealed that small-to-medium sized businesses (1–500 employees) are targeted with three times more spam per user per month than the larger enterprise clients (2,500+), and almost twice as much as medium-sized (501–2,500) corporate clients (see Figure 8).

Businesses are also affected by fraudulent activities related to spam. Some attacks, such as click fraud schemes, directly target businesses whereas others affect businesses indirectly via their customers. Systematic click fraud data are difficult to come by. A detailed analysis of a low-noise click fraud attack against syndicated search engines carried out by the Clickfraud.A botnet was provided by Google. According to the paper, the botnet comprised 100,000 bots controlled by a HTTP-based botmaster. The clickbot remained undetected by a majority of anti-virus scanners but overall caused only US\$ 50,000 in damages.⁶⁹

For the past three years, Click Forensics publishes the Click Fraud Index, based on data from more than 4,000 online advertisers and agencies. According to the data, the click fraud rate is steadily increasing. During the 4th quarter of 2007, the average click fraud rate across industries was 16.6 percent up from 14.2 percent during the same quarter in 2006.⁷⁰ In content industries, an even higher click fraud rate of 28.3 percent was detected during the 4th quarter of 2007. Given the amount spent for online advertising, these rates translate into potential damages in 2006 of US\$ 750 million⁷¹ and nearly US\$ 1 billion in 2007.

⁶⁷ MessageLabs Intelligence: *2007 Annual Security Report*, at <http://www.messagelabs.com/resources/mlireports>.

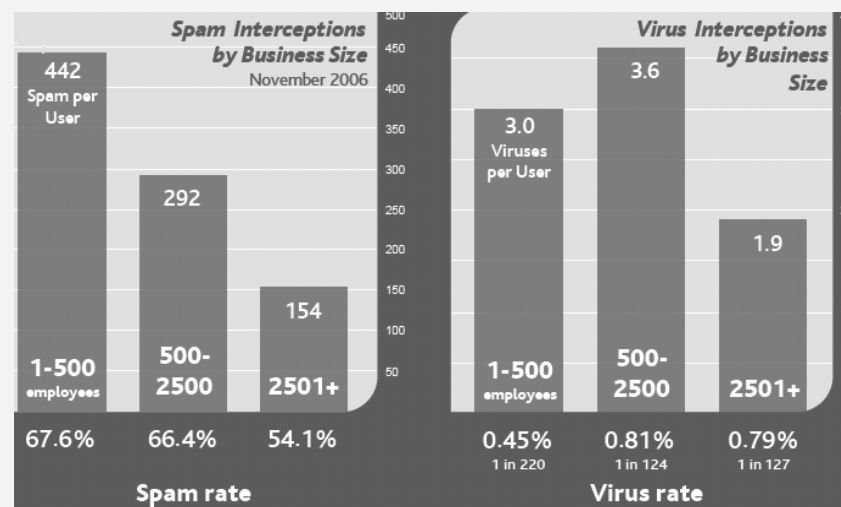
⁶⁸ See M. J. G. van Eeten, J. M. Bauer with contributions by M. de Bruijne, J. P. Groenewegen, and W. Lemstra, *Economics of Malware: Security Decisions, Incentives, and Externalities*, OECD STI Working Paper 2008/1 JT03246705, Paris, OECD, 2008, available online at <http://www.oecd.org/dataoecd/53/17/40722462.pdf>.

⁶⁹ See N. Daswani, M. Stoppelman and the Google Click Quality and Security Teams, "The Anatomy of Clickbot.A", without year.

⁷⁰ See <http://www.clickforensics.com/Pages/ClickFraudIndex.aspx>, last visited 16 February 2008.

⁷¹ See T. Claburn, "The Cost of Click Fraud," *Information Week*, April 18, 2006, available online at http://www.informationweek.com/blog/main/archives/2006/04/the_cost_of_cli.html.

Figure 7 Spam and Virus interception by business size



Source: MessageLabs Intelligence, November 2006.

Effects on individuals

A considerable number of unsolicited emails are not sent with fraudulent or criminal intent and a fair share of recipients responds to such offers. Many are based on earlier business relations or sent with benign intent. According to Consumer Reports, 650,000 Americans ordered a product or a service advertised in spam the month before the survey (this would translate into 7.8 million people per year, or 3.6 percent of the U.S. online population). Whereas such emails theoretically also could be considered spam, the more problematic forms remain those that are sent with fraudulent or criminal intent.

In the Internet economy, fraud refers to any deceitful scheme that uses one or more online services such as chat rooms, e-mail, message boards, or web sites to (1) present dishonest solicitations to prospective victims, (2) conduct fraudulent transactions, or (3) transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Types of online fraudulent activities targeted to individuals include phishing, email spoofing, and pharming (redirecting traffic from a legitimate to a bogus website). Spam is widely used to carry out such activities, in particular in phishing campaigns.

Team Cymru, citing research by the Cyber Security Alliance, states that Americans lost more than US\$ 336 million in 2005 due to online fraud.⁷² In its 2007 State of the Net survey which was already referred to earlier, Consumer Reports quantified the annual damage to consumers, some but not all of which is spam-related, to US\$ 7.1 billion.

Similar numbers can be found in a recent document by the Internet Crime Complaint Center (IC3). In 2007, according to the document, U.S. consumers lost more than \$239 million due to online fraud an increase of 20.7 percent from \$198 million in 2006.⁷³ In almost 74 percent of the cases the perpetrators contacted the victims via email. The actual numbers may be higher, as many instances of fraud are misclassified.

⁷² Team Cymru, "The Underground Economy: Priceless", *Login*, Vol. 31, No. 6, 2006.

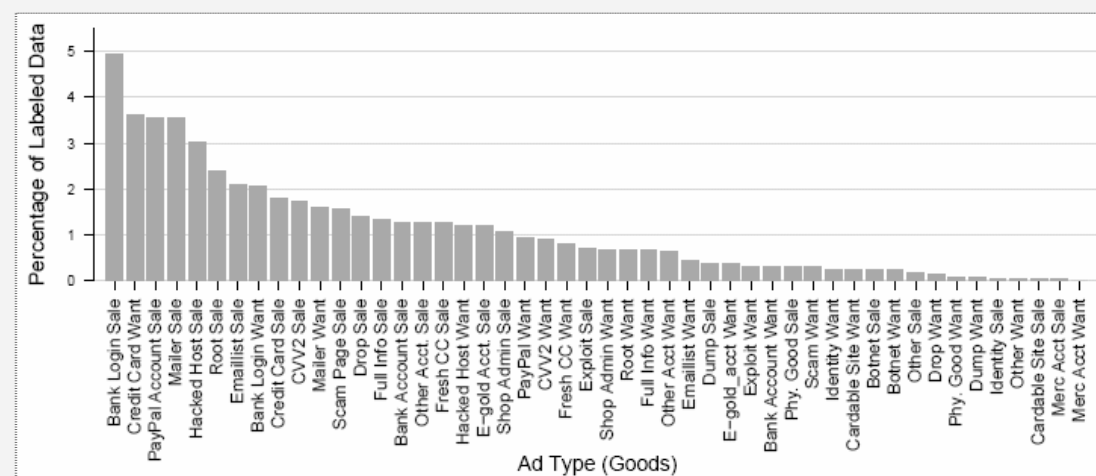
⁷³ Internet Crime Complaint Center, *2007 Internet Crime Report*, prepared by the The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation, 2008.

In 2007, according to data by MessageLabs, the level of phishing attacks rose to 1 in 156.0 (0.64 percent) from 1 in 274.2 (0.36 percent) in 2006, an increase of 0.28 percentage points. When measured as a proportion of all malware attacks, phishing attacks accounted for 66 percent of all attacks, a steep increase when compared with the average of 34.9 percent in 2006. Phishing attacks have widened their targets from defrauding major international banks and financial organizations to also targeting smaller national and state banks, including credit unions.⁷⁴

According to the UK Association of Payment Clearing Services (APACS), the number of phishing attacks in the UK has also risen dramatically over the past couple of years. Bank losses from online fraud in the UK rose to £23 million (US\$ 45 million) during the first half of 2006.⁷⁵ Phishing continued to be an increasing threat during 2006, accounting for an annual average of 0.36 percent or 1 in every 274.2 of all email traffic. In 2005, the annual average of phishing emails had been 0.3 percent or 1 in every 304. In 2006, phishing accounted for 24.8 percent of malicious email traffic intercepted, rising from 10.6 percent in January to 68.6 percent toward the end of the year. When compared with the annual average in 2005 of 13.1 percent, the 2006 figure highlights a marked shift in cyber criminal activity towards phishing between these two years.⁷⁶

It is interesting to see the different kinds of ads that were used to inject phishing attacks. Figure 9 below, gives the distribution of ads for goods in labeled data as found in a recent study:⁷⁷

Figure 8 Distribution of ads for goods in labeled data⁴³



Source: MessageLabs Intelligence, November 2006.

⁷⁴ MessageLabs Intelligence: 2007 Annual Security Report, <http://www.messagelabs.com/resources/mlireports>.

⁷⁵ See http://www.apacs.org.uk/media_centre/press/07_14_03.html.

⁷⁶ MessageLabs Intelligence: 2006 Annual Security Report, <http://www.messagelabs.com/resources/mlireports>.

⁷⁷ See J. Franklin, V. Paxson, A. Perrig, S. Savage, "An Inquiry into the Nature and Cause of the Wealth of Internet Miscreants", paper presented at CCS'07, October 29-November 2, 2007.

Several studies have attempted to monitor and investigate the monetary damage from fraudulent fund transfers as a result of phishing and ID theft trojan related attacks. These studies usually involve identification of individuals that are recruited by criminals to facilitate illegal funds transfers from bank accounts. A recent example of such activity is the exploitation of the launch of the iPhone to re-direct people to a spoof website to collect their bank information.⁷⁸

Empirical data is available for the U.S. and the U.K. For the latter, CIFAS reports growth in different types of fraud in 2007.⁷⁹ However, identity fraud had stabilized when compared to 2006. The number of cases of identity fraud identified in 2007 was 39,261, and it was observed that the number of victims had increased from 32,039 in 2006 to 33,411 in 2007.

Table 1 Summary of fraud cases filed by CIFAS

	Jan to June 2006	Jan to June 2007	% Change
Subjects Identified	122,633	132,631	8%
Fraud Cases Identified	85,128	91,509	8%
Financial Benefit/Losses Avoided	£360m	£473m	32%

According to CIFAS the amount of money its members have saved through being alerted to previous frauds by CIFAS warnings are shown in the table 2.

Table 2 Financial benefits or losses avoided by previous warnings

CIFAS Case Type	Jan to June 2006	Jan to June 2007	% Change
Identity fraud	39,647	39,621	0%
Application Fraud	31,488	37,357	19%
Facility Takeover Fraud	2,142	3,101	45%
Asset Conversion	168	220	31%
Misuse of Facility	11,504	11,012	-8%
False Insurance Claim	179	198	11%

Another perspective is provided by the CIS Report. The total damage due to financial fraud in the reporting companies in 2007 was US\$ 21,124,750. Financial fraud was identified to cause the largest financial damage among all kinds of cybercrime. Phishing caused a damage

⁷⁸ See <http://www.techcentral.ie/article.aspx?id=11580>.

⁷⁹ See CIFAS, "Worrying Fraud Trends–The Rise Continues," available at http://www.cifas.org.uk/default.asp?edit_id=715-57.

of US\$ 2,752,000 in 2007. Telecom fraud was relatively smaller and was US\$ 651,000. There could be several other kinds of attacks that could eventually lead to a case of fraud.⁸⁰

In the US, according to Javelin Strategy & Research, identity theft cost consumers and businesses US\$ 49.3 billion in 2006. In 2008 the firm reported that identity fraud had fallen for a second year in a row and that thieves had fallen back to old methods using predominantly mail and telephone fraud. Online attacks only constituted 19 percent of the cases. For 2005, a study prepared for the Federal Trade Commission by Synovate estimated that 8.3 million Americans had fallen victim to ID theft, although this included all forms, including online ID theft.⁸¹

6.2. Operational aspects of spam

Providing email services to send spam

Through 2007, new spam techniques used innovative means, such as PDF spam, image spam, or MP3 spam, as new ways to bypass traditional countermeasures adopted to prevent them from reaching their targets. Although PDF spam briefly exploded during mid-2007, it has since declined to virtually zero. Similarly, image spam has largely declined in 2007, giving way to more text-based and HTML-based spam, which is highly obfuscated. There had also been an increase in the number of bounce-back spam in 2007 in which spammers spoof the “from:” and “reply-to:” addresses in the original spam message.⁸²

A spam spike is a technique whereby individual domains are targeted in a particularly aggressive attack. The purpose of which is to defeat appliance-based anti-spam systems that rely heavily on signatures (rather like desktop anti-virus software). For businesses without the infrastructure in place to handle such attention, these attacks can cause severe problems for the company’s email servers. In just the same way that traditional anti-virus countermeasures can be targeted during an outbreak, by the time an anti-spam vendor has obtained a sample and produced a signature, the attack is already over. With spammers attempting to cash in on the potential rewards available through the virus writers’ targeted approach, targeted spam has increased in visibility over the last 12 months.

Most notably, advance-fee fraudsters (including Nigerian 419 scams) have targeted particular organizations within the Accommodation, Catering and Hotel sectors, mainly in North America. These scams – while in themselves not particularly new – are often customized. In some recent examples, the emails were sent to named individuals within the target organization that had purchasing authority, such as the owner, a manager, or the CEO. The use of image spam has increased during 2007 and peaked in September at around 20 percent of all spam targeting businesses. With spam levels rising, Instant Messaging (IM) was expected to be on the spammers list of targets for 2007. However, this did not happen but the predicted increase in IM attention might still happen in 2008. The average virus level for 2007 was 1 in 117.7 emails (0.8 percent) which reflects a fall of 0.6 percent since 2006 where levels averaged 1 in 67.9 emails.

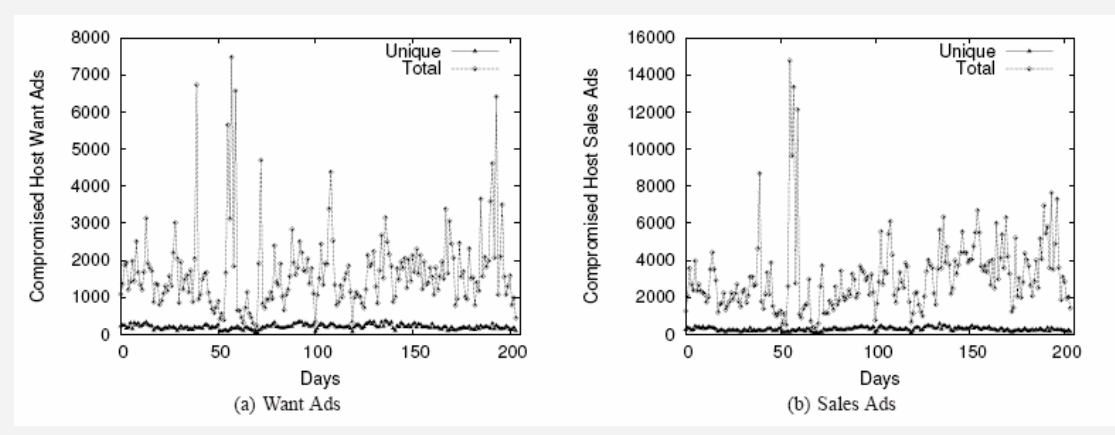
⁸⁰ CSI, Computer Crime and Security Survey, 2007, p. 15. These numbers were based on a survey of 194 respondents.

⁸¹ See Synovate, *2006 Identity Theft Survey Report*, Washington, D.C., Federal Trade Commission, November 2007.

⁸² MessageLabs Intelligence: *2007 Annual Security Report*, <http://www.messagelabs.com/resources/mlireports>.

More than 80 percent of all spam in circulation is known to be distributed from botnets, expressly created for this purpose by specially crafted strains of viruses. The first well-known example was Sobig in 2003. Since then, almost all major virus outbreaks have been for the purpose of creating a botnet that will subsequently be used to send out spam. The distribution of spyware and adware is reportedly a multi-billion dollar industry, fuelling a boom in the number of botnets that are now being created. As mentioned above, renting a botnet is reported to cost as little as \$50-\$60 per 1,000 to 2,000 bots approximately, but it depends on how the bots are to be used. In some cases, prices may be higher or lower or payment may be in exchange for a list of stolen credit card numbers. For example, a fraudster who has developed a “bank stealing trojan” (a trojan that becomes active once a user logs on to his or her bank), but no distribution network, may expect to pay a bot herder to install the trojan on some of the machines in his network. Sometimes the bot herders expect “extras” i.e. they will monitor what their bots are doing when they are hired out and log any credit card numbers, personal data, etc. that may be collected or relayed through them.⁸³

Figure 9 Extrapolated number of ads for compromised hosts

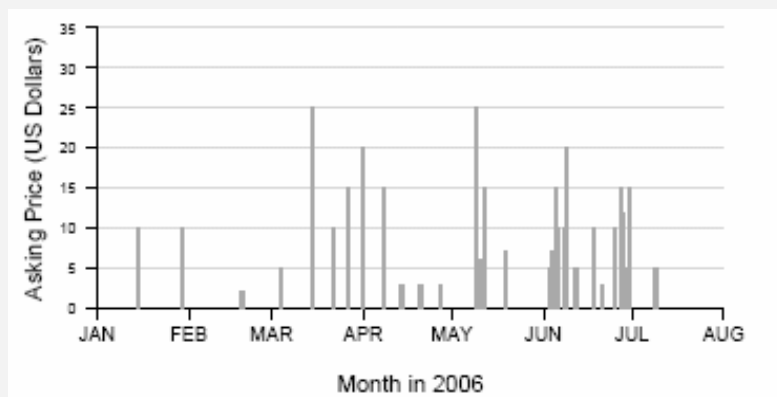


In their study of the underground internet economy, Franklin et. al. found that the majority of spam and phishing-related ads in the labeled dataset were sales ads offering bulk email lists and sales offers for URLs of web email forms vulnerable to “email injection attacks.”⁸⁴ An email injection attack exploits the input validation of web email forms such as the ubiquitous *contact us* form to include additional recipient email addresses. Rather than simply being sent to the individual responsible for the contact form, the web server sends the message to a list of injected addresses. The ease with which vulnerable email forms can be found has produced a bustling trade of such mailers. Vulnerable mailers ease the job of spammers who might otherwise have to locate open mail relays or employ bots to send spam. Email lists created by crawling web pages with email spiders or extracted from customer databases of compromised e-merchants further ease the job of spammers by enabling targeted spam campaigns.

⁸³ *Ibid.*

⁸⁴ See J. Franklin, V. Paxson, A. Perrig, S. Savage, “An Inquiry into the Nature and Cause of the Wealth of Internet Miscreants”, paper presented at CCS’07, October 29-November 2, 2007.

Figure 10 Distribution of ads for goods in labeled data43



The paper also explores the asking price for compromised hosts. These prices enable defenders to quantify the *cost to buy* sufficient resources to overcome a defense system. For example, a DDoS defense that is effective for up to 1,000 hosts could be overwhelmed by US\$10,000 in January or as little as US\$2,000 in February. The *cost to buy* can be used to assess the strength of an adversary with resources r at time t . For example, a US\$10,000 adversary could purchase 1,000 compromised hosts in January. In Figure 11 the asking prices of compromised hosts in 2006 is shown.

Providing network bandwidth to carry spam and malware

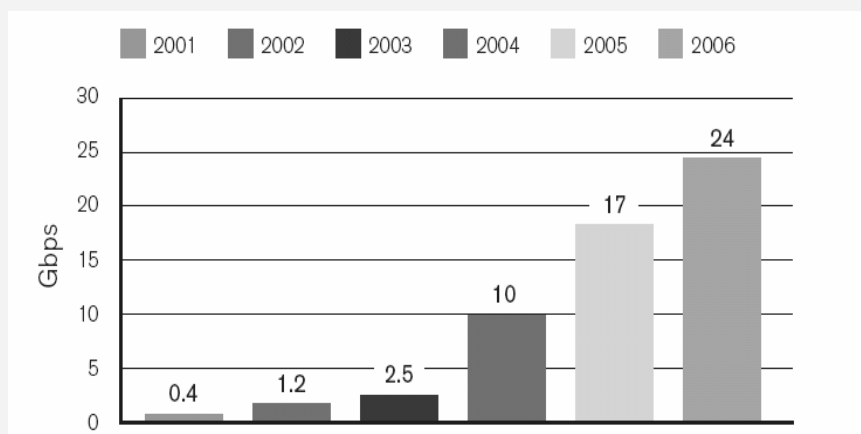
The Worldwide Security Infrastructure report, September 2007, found the growth in DDoS sustained attack size illustrated in Figure 12 below. These attack sizes refer to DDoS attacks – in other words, they do not indicate the bandwidth usage for the distribution of spam and malware, but the bandwidth effects of the use of malware and spam for criminal purposes. A recent report mentioned that attack sizes are growing more rapidly than the ISPs can expand their infrastructure.⁸⁵

When investigating the source of much of the malware, spam and phishing attacks, the U.S. remains the majority of the world's compromised computers. In the first quarter of 2006, 18.1 percent of the world's zombie computers were found in the U.S. ⁸⁶ However, these estimates vary, both over time and per security service provider.

⁸⁵See the report "Attacks on ISP Nets Intensifying," http://www.darkreading.com/document.asp?doc_id=133973.

⁸⁶Message Labs Intelligence Report, April 2006.

Figure 11 Sustained attack size in Gbps



Source: Arbor Networks, Inc.

Modern ISP networks no longer consist of a collection of broadband, dial-up, and corporate-leased lines, but utilize additional platforms and access points. The growth of easy-to-use public Wi-Fi services has increased potential entry points for the delivery of hard-to-trace spam. Suddenly, coffee shops, airports, and other locales are all potential launch pads for spam. It is easy to anonymously purchase 30 minutes of network access over the counter and use it for illegal activities. And very little can be done to combat unsolicited email delivered in this way unless providers of these networks take action.⁸⁷

Steadily, more text and voice spam are invading handsets of mobile phones. Wireless users in the U.S. will receive about 1.1 million spam text messages this year, up 38 percent from 2006, estimates messaging specialist Ferris Research. By 2008, mobile spam messages are expected to hit 1.5 million. That is far from an epidemic—it pales next to the 250 million Americans who use wireless services—but security experts and wireless consultants warn that phone spam will grow in coming years. Viruses and surreptitious code that monitors phone use may be next.⁸⁸

E-mail spam is bothersome. But mobile spam can also be expensive. Consumers, especially in the U.S., are charged for receiving their text messages and sometimes as much as 20 cents per message. Spammers, using automated dialers, can shoot millions of texts to random cell-phone numbers. Phone companies intercept many of them; in May, Verizon Wireless sued telemarketers that it said had “inundated” the company with more than 12 million unsolicited commercial text messages. Verizon said it blocked all but 4,618 from reaching customers, but the torrent still hit them with unwanted charges and clogged networks.

Fighting spam

Experts claim that no single method of detection will block spam.⁸⁹ The only solution is to use a collection of tools. Such hybrid detection needs to include at least these four elements:

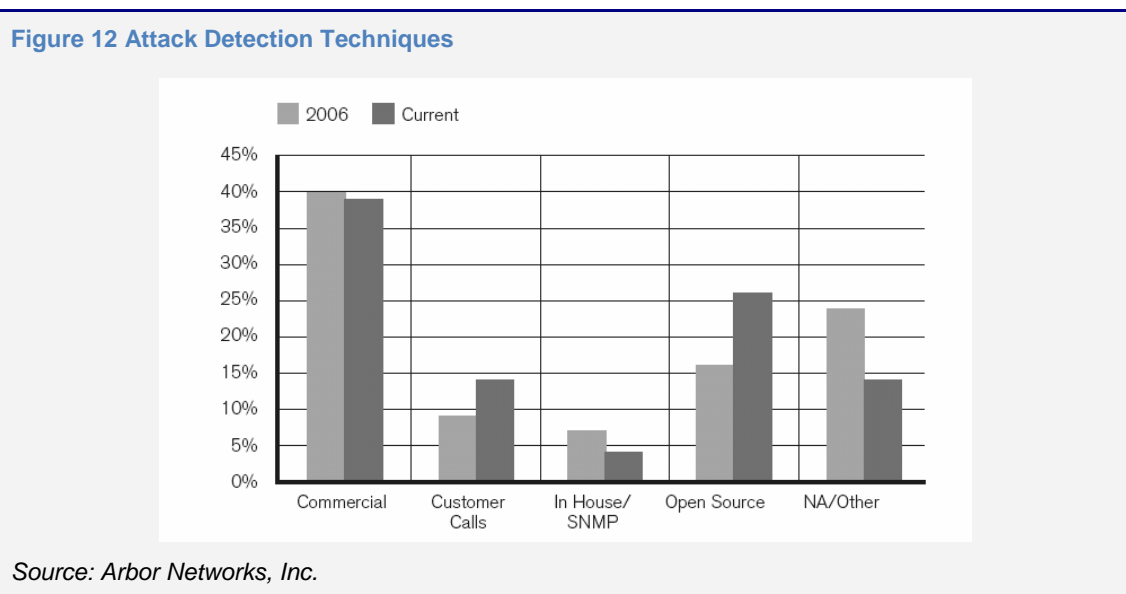
⁸⁷ S. Cronje “E-mail’s spam plague persists,” in: *Sage*, April 2007.

⁸⁸ R. O. Crockett , “E-mail’s Scourge is Coming to Your Cell Phone, Where it Will be More than Annoying—It’ll Cost You,” in: *Business Week*, November 26, 2007.

⁸⁹ S. Cronje “E-mail’s spam plague persists,” in: *Sage*, April 2007.

(1) highly dynamic IP-based sender reputation; (2) content analysis; (3) bulk pattern detection; and (4) botnet detection.

The Worldwide Security Infrastructure Report, September 2007, gave the primary attack detection techniques as depicted in Figure 13.



The direct costs of fighting spam are embedded in the total costs businesses and individuals incur in the form of protective and remedial measures. The OECD suggested the following proxy costs and operational data associated with spam filtering in developing countries: Bandwidth costs were estimated to US\$ 600/MB/month, bandwidth consumption for mail was found to be 70 MB/day, the incoming mail rejected as spam was 80 percent, the percentage of accepted mail that is spam that gets past by filters was 15 percent, the monthly bandwidth cost of spam is US\$ 6,300, the monthly storage cost of spam is US\$ 5,400, the monthly salary expenses for mail/abuse administrators is close to US\$ 75,000 and finally one needs to add all the costs incurred because of erosion in trust by users due to spam.⁹⁰

⁹⁰ OECD, *Spam Issues in Developing Countries*, Paris, 2005.

7. WELFARE EFFECTS: A PRELIMINARY ASSESSMENT

7.1. Correctly identifying welfare effects

Our review of the available research has demonstrated a wide range of estimates as to the potential financial impacts of malware and spam on participants in the information and communication value network. It has also revealed many serious shortcomings and gaps in the existing information base. Data is often unavailable or the methodology used to collect the available data may be wanting.

From a welfare perspective one needs to ask whether the costs and revenues streams associated with preventative and remedial measures related to malware and spam are welfare-enhancing or not. It seems relatively straightforward that the cost associated with damages from malware and spam is welfare-reducing, as they do not add any net value to the economy.

However, the analysis is more complicated when it comes to revenues associated with preventative measures such as those of software vendors specializing in security software, security service providers, ISPs providing special hosting services or DDoS protection, and hardware manufacturers that offer sophisticated devices to fight malware and spam. These are principally legitimate revenues albeit associated with malware and spam. Some of these activities may add value to the information and communication industries and users of these services. For example, if security services enhance trust in the whole e-commerce system, they facilitate a migration to more efficient forms of transacting with the associated welfare gains.

This conclusion does not hold for all legal revenues, however. Many activities are caused by the need to fix problems created by fraudulent and criminal activities and by attacks on the information and communication value network. Costs are also incurred because the players in the value net externalize costs onto other players because of flawed incentives to invest in security. Such costs are an outcome of a violation of efficiency conditions in the first place. As in the case of environmental cleanups, the economy “benefits from its ills.” Should such revenues be counted as welfare-enhancing activities? Or should parts (or possibly all) of them be considered as activities that do not add net welfare? One option is to look at them as a class of “neutral” activities that do not enhance welfare (but also not reduce it). A more radical approach would be to treat them as “economic bads,” lawful economic activities that actually reduce welfare.⁹¹

Furthermore, there is a booming illegal underground economy related to fraud and cybercrime. Some stakeholders, such as Internet hosting and access service providers, ISPs and hardware manufacturers, may even earn legitimate business revenues from clients that are criminals (both sometimes known and sometimes unbeknownst to them). Significant revenues are generated by transactions within the illegal underground economy of malware-based fraud and cybercrime. Some if not all of this money is laundered and flows back into the economy as “legal” economic transactions. Nonetheless, underground economy revenues are, from a welfare point of view, to be considered as “bads” that reduce economic welfare. In other words, the financial streams related to these activities constitute a burden to society even if they eventually lead to legitimate transactions.

Finally, individual stakeholders and societies face an increasing cost of restoration of damages as well as law enforcement. These costs, while they generate legitimate incomes

⁹¹ See N.O. Keohane and R.J. Zeckhauser, “The Ecology of Terror Defense,” *Journal of Risk and Uncertainty*, 203, 26(3), pp. 201-229, for a similar argument with regard to terrorism and defences against it.

and revenues, also cannot be regarded as welfare-enhancing. Rather they constitute costs to society. Money is spent to prevent something unwanted from happening.

7.2. Externalities and welfare

The players in the information and communication value net are highly interrelated. Security decisions by one player have consequences on many other players. Externalities prevail whenever the private costs and benefits taken into account by decision-makers deviate from the social costs and benefits of a decision. For example, individual users may face financial expenses to protect their machines against malware but not experience the costs of failing to do so as these costs are incurred by other users who are the targets of malware and/or spam sent from the infected machine. In this case, under-protection will probably result as end-users will invest insufficiently in security.

Van Eeten, Bauer et.al. distinguished three main scenarios.⁹² In rare cases, decision-makers, first, consider all the relevant social costs and benefits in their decisions and no externalities exist. However, more likely are two other scenarios. In a second situation the private costs and benefits of decision-makers deviate from the social ones, but another actor in the value chain is in a position to correct the effect because its benefits exceed the costs of internalizing the damage. For example, a bank may internalize damages experienced by customers from phishing and set certain levels of security for its services. In so doing, the bank trades off the direct and indirect damages from malware against other costs and benefits of its business activities, most notably usability of their services and the growth of overall transaction volumes.

In the third scenario, the private costs and benefits of decision-makers deviate from the social ones but no other actor in the value chain is in a position to correct the effect. For example, the costs for an ISP of isolating all the machines that participate in dynamically configured botnets are presently prohibitively high. The ISPs have incentives to isolate machines that they are notified about or that might lead to disruptive levels of blacklisting. But this only concerns a small fraction of the overall number of infected machines on their network. Another example is the need for e-commerce companies to buy DDoS mitigation or protection services from ISPs. In these cases, costs are increased for the respective actors and typically costs are also shifted to society at large in the form of law enforcement costs or costs of remediation in case of damages.

In both the second and third cases, the costs associated with malware should be considered an economic bad. In the second scenario, costs are shifted between players (a distributional effect) and the conditions for an efficient economic allocation are violated. Even if a player that does not originate a violation can achieve security cheaper, such an efficiency violation occurs as long as the originating player is not assessed an appropriate share of the costs. Nevertheless, as some players in the value net take corrective action, the whole system is brought closer to an efficient outcome than would otherwise be the case. In the third scenario, costs will be borne by market players who cannot influence the risky decisions from which these costs originate – e.g., e-commerce companies having to buy DDoS mitigation services from their ISP to protect them from botnets of infected end user machines. In such cases, an exogenous intervention by law enforcement may be necessary. It is not straightforward to

⁹² See M. J. G. van Eeten, J. M. Bauer with contributions by M. de Bruijne, J. P. Groenewegen, and W. Lemstra, *Economics of Malware: Security Decisions, Incentives, and Externalities*, OECD STI Working Paper 2008/1 JT03246705, Paris, OECD, 2008, available online at <http://www.oecd.org/dataoecd/53/17/40722462.pdf>.

assess whether such an intervention will bring the system closer to an efficient state or which form of an intervention will do so.

The information and communication value net is not only afflicted with negative externalities. The openness of the system, which also increases its vulnerability, is at the same time at the heart of positive externalities that have contributed to and possibly accelerated the rate of technological and economic advances as different players can also create a virtuous circle of innovation.

7.3. Concluding observations: a patchwork of numbers

Table 3 summarizes the main findings of this report. It indicates that the empirical understanding of the effects of malware is far from complete. The magnitude of many financial aspects is unknown or cannot be disentangled from larger aggregates. Estimates as to the magnitude of damages and other financial effects differ widely. Many numbers are only available for a small subset of the relevant population and do not easily allow estimates as to the overall size of the effects.

Given the incomplete availability of numbers and their variability, it would be premature to claim that the overall financial effects of malware can be determined with satisfactory reliability. All figures indicate that the effects are non-negligible. The continuous attacks on the information and communication value net have raised the costs of preventative measures and of remediation for all stakeholders. These effects taken together are probably higher than the direct costs of damages.

Estimates of damages from fraudulent and criminal activities vary widely. For the U.S., estimates of direct damages to consumers range from \$336 million to \$7.1 billion (or 0.04 to 0.1 percent of U.S. total consumer spending). Estimates by Javelin Research put the costs of identity theft and related forms of fraud, not all of which is malware-related, as high as \$49.3 billion (or 0.4 percent of GDP). The FBI estimated the cost of computer crime to \$67.2 billion (or 0.54 percent of GDP) in the U.S. Although some of these sources produce relatively reliable numbers, minimum reporting thresholds generate systematic underrepresentation of the actual size of damages.

Many statistics are only available for specific nations and strong assumptions will have to be made to scale the information to estimate global effects (for example, that the effects of cybercrime are of similar magnitude compared to GDP). It is probably reasonable to assume that, due to lower Internet use, these figures are somewhat lower in other industrialized nations and much lower in developing nations. Other costs, such as the costs of preventative measures and security services cannot be fully seen as economic bads, as discussed. However, some of the costs should be attributed to malware and spam.

An alternative to such bottom up aggregation is to try to directly come up with a global estimate. Such an approach is fraught with potential pitfalls and often only a very rough approximation or even a back-of-the envelope calculation is possible. However, some figures are available for the global economy. The size of the global underground malware economy, that is, the total of legal and illegal transactions has been estimated at \$105 billion by MessageLabs.⁹³ Ferris Research quantified the global cost of spam at \$100 billion. Both effects, despite the fact that some legal revenues are associated with them, can be treated as an “economic bad” (just as revenues generated from fixing cars that were damaged in accidents are contributions to GDP but do not necessarily add to the well-being of society).

⁹³ See M. Schipka, “The Online Shadow Economy: A Billion Dollar Market for Malware Authors,” White Paper, MessageLabs, 2007.

On direct rough estimate is to take the size of the malware underground economy and the global cost of spam together. This approach avoids double-counting effects. As it does not include certain costs of preventative measures, it will most likely be a lower boundary of the global costs. The combined effect is about 0.3 percent of the global economy, measured at \$66,000 billion. Taking margins of error into consideration, a conservative estimate of the financial impact of malware and spam would be in the 0.2-0.4 percent range of global GDP. If other direct and indirect effects—in particular the costs of slower migration to productivity-enhancing ICT applications—are added, the total impact could be as high as 0.5-1 percent of global GDP.

Table 3 Financial effects of malware and spam

Player	Available data		Remarks
	Type and source	Impact	
<i>Cost/revenues of preventative measures</i>			
Security services	Combined global revenues	US\$ 7.5 bn	2007
ISPs	Cost of filtering, Eeten et.al. (2007), selected interviews	6-10% of IT budget	Costs, incremental revenue opportunities unknown
Hardware, software	Cost of equipment protection	N/A	
Business users	CSI (2007), 494 U.S. organizations	0-10% of IT budget	Costs, some included in security service revenues
Individual users	Cost of anti-virus programs, firewalls, etc.	N/A	Part included in security service, ISP, hardware, and software revenues
<i>Costs of damages and remedial measures</i>			
ISPs	Eeten et. al. (2007), cost of abuse desk and customer service	0.25-2.5 FTE per 100,000 customers	Higher for business services
Hardware, software	Security-related incremental revenues	N/A	
Costs to business users	Global direct costs of malware	\$13.2 bn	Computer Economics
	FBI estimate of costs of cybercrime for U.S.	US\$ 67.2 bn	2005, approximately 0.5% of GDP
	CSI Survey (194 respondents)	US\$ 345,000 per firm	2007
	Click fraud	US\$ 1 bn	2007
	Global cost of spam	US\$ 100 bn	2007, Ferris Research
	U.S. cost of spam	US\$ 35 bn	2007, Ferris Research
	Cost of spam management	US\$ 712 per employee	2007, Nucleus Research Inc.
Individual users	Cost to consumers	US\$ 7.1 bn	2007, <i>Consumer Reports</i>
	Cost of computer repairs, U.S.	US\$ 3.25 bn per year	US\$ 15 per Internet user and year
	Costs of financial fraud to US consumers	US\$ 336 mill	2005, estimated by Team Cymru
	Losses from online fraud to US consumers processed by IC3	US\$ 239 mill	2007, Internet Crime Complaint Center

	Identity theft and other forms of fraud	US\$49.3 bn including online fraud	Javelin Strategy & Research
	UK online banking fraud	£ 33.5 mill	2006, APACS
Government, law enforcement, self-regulation	Cost of law enforcement and self-regulation	N/A	Numbers not available on disaggregated level
Society at large	Opportunity costs of slower adoption of productivity-enhancing technology	N/A	Mixed evidence pro and con such effects
<i>Size of global underground malware economy</i>			
Malware economy	Global total of illegal transactions	\$105 bn	Estimated by MessageLabs 2007

Given the positive effect of ICTs on economic growth—the Commission of the European Communities, for example, estimates that 40 percent of European productivity growth and 25 percent of GDP growth are due to ICTs—malware and spam constitute a non-negligible drag.⁹⁴ The negative effects of malware and spam diminish other efficiency gains from ICT.

Although no detailed research as to this relation is available, it is likely that the potential contribution of ICTs to economic growth differs across nations. First, the impact of ICT on economic growth and its specific form are probably dependent on the stage of economic development. At an earlier stage of economic development, the availability of basic means of communication, such as fixed or mobile phones or dial-up Internet access, may have visible productivity effects. At subsequent stages, more advanced ICT will be necessary to achieve such a positive contribution. In either case, the presence of malware and spam may diminish these potential positive effects significantly.

Although the financial aspects of malware and spam are increasingly documented, serious gaps and inconsistencies exist in the available information. This sketchy information base also complicates finding meaningful and effective responses. For this reason, systematic efforts to gather more reliable information would be highly desirable. This would require agreement as to a set of metrics and collaboration in data collection between public sector and private sector organizations. In particular, a single nation cannot design its best policy approach based on global numbers alone. It will be necessary to gather specific data for the country. A first step in this direction is the establishment of better reporting requirements. International collaboration in the creation of metrics that provide better measures for the costs of spam and malware are, therefore, highly recommendable.

⁹⁴ Commission of the European Communities, *i2010 - A European Information Society for Growth and Employment*. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2005) 229 final, Brussels: 2005.