OECD ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Directorate for Science, Technology and Industry
Committee for Information, Computer and
Communications Policy

Malicious Software (Malware): A Security Threat to the Internet Economy

Ministerial Background Report
DSTI/ICCP/REG(2007)5/FINAL

OECD Ministerial Meeting
on the Future of the Internet Economy

Seoul, Korea, 17-18 June 2008

Hosted by 방송통신위원회
KOREA COMMUNICATIONS COMMISSION

FOREWORD

Addressed primarily to policy makers, this report has been developed in the course of 2007, by the OECD Working Party on Information Security and Privacy (WPISP) in partnership with the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG).

The report was declassified by the Committee for Information, Computer and Communications Policy (ICCP) on 6 March 2008. The report is published under the responsibility of the Secretary-General of the OECD.

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

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

Note (9 June 2008): The following sentence p. 37 "Furthermore, it is estimated that 59 million users in the US have spyware or other types of malware on their computers" should read "After hearing descriptions of "spyware" and "adware," 43% of internet users, or about 59 million American adults, say they have had one of these programs on their home computer." The original source can be found in Pew/Internet, "Spyware", July 2005, p.3.

TABLE OF CONTENTS

Boxes

MAIN POINTS

A strategy for a global partnership against malware is needed to avoid it becoming a serious threat to the Internet economy and to national security in the coming years. Today, communities involved in fighting malware offer essentially a fragmented local response to a global threat.

Malicious software, commonly known as "malware", is software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners. Over the last 20 years, malware has evolved from occasional "exploits" to a global multi-million dollar criminal industry.

Malware affects all actors. It is increasingly a shared concern for governments, businesses and individuals in OECD countries and APEC economies. As governments rely ever more on the Internet to provide services for citizens, they face complex challenges in securing information systems and networks from attack or penetration by malicious actors. Governments are also being called on by the public to intervene and protect consumers from online threats such as ID theft. The past five years have indeed brought a surge in the use of malware to attack information systems for the purpose of gathering information, stealing money and identities or even denying users access to essential electronic resources. Significantly, the capability also exists to use malware to disrupt the functioning of large information systems, surreptitiously modify the integrity of data and to attack the information systems that monitor and/or operate major systems of the critical infrastructure.

This report, developed in collaboration with experts, aims to inform policy makers about malware impacts, growth and evolution, and countermeasures to combat malware. It seeks to analyse some of the main issues associated with malware and to explore how the international community can better work together to address the problem. Highlights include the following:

- Spam has evolved from a nuisance to a vehicle for fraud to a vector for distributing malware. Malware, in the form of botnets, has become a critical part of a self sustaining cyber attack system. The use of malware has become more sophisticated and targeted. Many attacks are smaller and attempt to stay "below the radar" of the security and law enforcement communities.
- The effectiveness of current security technologies and other protections in detecting and containing malware is challenged by the shrinking of the time between the discovery of vulnerabilities in software products and their exploitation.
- The behaviour of market players confronted with malware (whether Internet service providers, e-commerce companies, registrars, software vendors or end users) is influenced by mixed incentives, some working to enhance and some to reduce security. There are many instances in which the costs of malware are externalised by players at one stage of the value chain onto other players in the value chain.
- A wide range of communities and actors – from policy makers to Internet service providers to end users – has a role to play in combating malware. There is still limited knowledge, understanding, organisation and delineation of roles and responsibilities in this broad community of actors.

- Current response and mitigation are mainly reactive. There is a need for more structured and strategic co-ordination at national and international levels with involvement of all actors to more adequately assess and mitigate the risk of malware.
- No single entity has a global understanding of the scope, trends, development and consequences of malware and thus the overall malware problem is difficult to quantify. Data on malware are not consistent and terminology for cataloguing and measuring the occurrence of malware is not harmonised.
- Although its economic and social impacts may be hard to quantify, malware used directly or indirectly can harm critical information infrastructures, result in financial losses, and plays a role in the erosion of trust and confidence in the Internet economy.

Addressing limitations of ongoing action against malware and further exploring how to strengthen incentives for market players to fight this phenomenon is important for policy makers to help all concerned communities successfully work together across borders. This report outlines several areas in which improvements can be made, including raising awareness, improved legal frameworks, strengthened law enforcement, improved response, measuring of malware, measures to address vulnerabilities in software, technical measures, economic incentives, research and development, standards, guidelines and good practices.

In light of the need for a holistic and comprehensive approach to malware to effectively reduce malicious activity on the Internet, this report suggests to organising a global “Anti-Malware Partnership” involving governments, the private sector, the technical community and civil society to produce joined-up policy guidance to fight malware on all fronts from educational to technical to legal and economical.

BACKGROUND

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

In 2002, the OECD adopted the *Guidelines for the Security of Information Systems and Networks* ("the *Security Guidelines*") which provide a clear framework of principles at the policy and operational levels to foster consistent domestic approaches to addressing information security risks in a globally interconnected society. More broadly, the *Security Guidelines* reflect a shared ambition to develop a culture of security across society, so that security becomes an integral part of the daily routine of individuals, businesses and governments in their use of Information and Communication Technologies (ICTs) and in conducting online activities.[1]In 2003 and 2005, the OECD monitored efforts by governments to implement national policy frameworks consistent with the *Security Guidelines*, including measures to combat cybercrime, develop Computer Security Incident Response Teams (CSIRTs), raise awareness, and foster education as well as other topics.[2] In 2006 and 2007, the OECD focused on the development of policies to protect critical information infrastructures.[3]

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

Shared OECD and APEC objectives

In 2005, the APEC and OECD co-organised a workshop to share information on evolving information security risks and to explore areas for further co-operation between the organisations to better tackle the international dimension of information security risks. In 2006, both organisations agreed that the need to encourage a safer and more secure online environment was more pressing than ever due to the continued growth of economic and social activities conducted over the Internet and the increased severity and sophistication of online malicious activity. Subsequently, they decided to organise a workshop[4] and

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

[2] See DSTI/ICCP/REG(2005)1/FINAL.

[3] See DSTI/ICCP.REG(2006)15/FINAL and DSTI/ICCP/REG(2007)16/FINAL.

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

develop an analytical report to examine the issues of malicious software, commonly known as “malware”, with a view to:

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

Prepared by the OECD Secretariat in close collaboration with volunteer government experts from OECD and APEC as well as the private sector, this report does not discuss every aspect of malware, all types of malware, or all propagation vectors. Rather, it focuses on issues of significant concern and areas which may pose problems in the future. Similarly, the report does not examine all possible strategies associated with preventing, detecting and responding to malware but rather focuses on elements of relevance to OECD member countries, APEC economies, and other governments and organisations more broadly. Finally, the report refers to forms of cybercrime, such as spam and phishing[5] that may not *directly* involve the use of malware but nevertheless demonstrate how malware can also be used *indirectly* to facilitate cybercrime.

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

MALWARE IN BRIEF

What is malware?

Malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners.[6]

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

Different types of malware are commonly described as viruses, worms, trojan horses, backdoors, keystroke loggers, rootkits or spyware. These terms correspond to the functionality and behaviour of the malware (*e.g.* a virus is self propagating, a worm is self replicating).[7] Experts usually group malware into two categories: family and variant. "Family" refers to the distinct or original piece of malware; "variant" refers to a different version of the original malicious code, or family, with minor changes.[8]

Box 1. Malware: A brief history

Viruses and worms date back to the early days of computers when most viruses were created for fun and worms were created to perform maintenance on computer systems.[9] Malicious viruses did not surface until the 1980s when the first personal computer (PC) virus, Brain (1986), appeared and propagated when the user "booted up" his/her computer from a floppy disc.[10] Two years later, in 1988, the Morris worm received significant media attention and affected over 6 000 computers. Although other types of malicious software appeared in the mid 80's, the landscape of the late 80s and early 90s predominantly consisted of viruses. Until about 1999, most people related viruses to the example of a teenager hacking into the Pentagon's systems as seen in the 1983 movie *Wargames.*

In the mid to late 1990s, the landscape began to change with the growth of the Internet and personal computer use, the rise of networking, and the adoption of electronic mail systems. The so-called "big impact worms" began to reach the public in novel ways. The increased use of e-mail brought high-profile mass-mailer worms such as Melissa (1999), "I Love You" (2000), Anna Kournikova (2001), SoBig (2003) and Mydoom (2004) that made the headlines and entered the public consciousness.[11] These types of worms doubled their number of victims every one-to-two hours, rapidly reaching peak activity within 12-to-18 hours of being released. This marked the parallel rise in organised, sometimes co-ordinated attacks. The explosive growth of online financial transactions resulted in increased security incidents and in the appearance of new types of malicious software and attacks. Today, mass worms and virus outbreaks are becoming ever scarcer while stealthy malware such as trojans and backdoors are on the rise. Many attacks are smaller to stay "below the radar" of the security and law enforcement communities. The goals of the attackers tend to be focused on financial gain. These new trends help explain why malware is now a global multi-million dollar criminal industry.

Overall characteristics of malware

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

[6] The 1992 OECD *Guidelines for the Security of Information Systems and Networks* defined an information system as computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specification and procedures for their operation, use and maintenance.

[7] See Annex E – Glossary of Terms.

[8] For example, W32.Sober@mm (also known as Sober) was the primary source code of the "Sober" family. Sober.X is a variant of Sober. (See Symantec 2006 p.67).

[9] NIST p. 2-10 .

[10] SOPHOS (2006a) p.1.

[11] Tippett (2006), and BBC News online (2004).

Malware is multi-functional and modular: there are many kinds of malware that can be used together or separately to achieve a malicious actor's goal. New features and additional capabilities are easily added to malware to alter and "improve" its functionality and impact.[12] Malware can insert itself into a system, compromise the system, and then download additional malware from the Internet that provides increased functionality. Malware can be used to control an entire host[13] or network, it can bypass security measures such as firewalls and anti-virus software, and it can use encryption to avoid detection or conceal its means of operation.

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

Malware is persistent and efficient: malware is increasingly difficult to detect and remove and is effective at defeating built-in information security counter-measures. Some forms of malware can defeat strong forms of multi-factor authentication and others have been able to undermine the effectiveness of digital certificates.[14]

Malware can affect a range of devices: because malware is nothing more than a piece of software, it can affect a range of devices, from personal devices such as personal computers (PCs) or Personal Digital Assistants (PDAs) to servers[15] across different types of networks. All these devices, including the routers that allow traffic to move across the Internet to other end points, are potentially vulnerable to malware attacks.

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

Malware is profitable: malware is no longer just a fun game for script kiddies[16] or a field of study for researchers. Today, it is a serious business and source of revenue for malicious actors and criminals all over the world. Malware, together with other cyber tools and techniques, provides a low cost, reusable method of conducting highly lucrative forms of cybercrime.

How does malware work?

Malware is able to compromise information systems due to a combination of factors that include insecure operating system design and related software vulnerabilities. Malware works by running or installing itself on an information system manually or automatically.[17] Software may contain

[12] Danchev, Dancho (2006) p.3.

[13] Host refers to a computer at a specific location on a network.

[14] See Annex B for a discussion of digital certificates.

[15] Servers are generally more powerful computers which provide services to (and accept connections from) many clients however home PCs and corporate workstations can also act as servers, particularly when they become compromised. Common types of servers include web, e-mail and database servers.

[16] Script Kiddie refers to an inexperienced malicious actor who uses programs developed by others to attack computer systems, and deface websites. It is generally assumed that script kiddies are kids who lack the ability to write sophisticated hacking programs on their own and that their objective is to try to impress their friends or gain credit in underground cracker communities.

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

vulnerabilities, or "holes" in its fabric caused by faulty coding. Software may also be improperly configured, have functionality turned off, be used in a manner not compatible with suggested uses or improperly configured with other software. All of these are potential vulnerabilities and vectors for attack. Once these vulnerabilities are discovered, malware can be developed to exploit them for malicious purposes before the security community has developed a “fix”, known as a patch. Malware can also compromise information systems due to non-technological factors such as poor user practices and inadequate security policies and procedures.

Many types of malware such as viruses or trojans require some level of user interaction to initiate the infection process such as clicking on a web link in an e-mail, opening an executable file attached to an e-mail or visiting a website where malware is hosted. Once security has been breached by the initial infection, some forms of malware automatically install additional functionality such as spyware (*e.g.* keylogger), backdoor, rootkit or any other type of malware, known as the payload.[18]

Social engineering,[19] in the form of e-mail messages that are intriguing or appear to be from legitimate organisations, is often used to convince users to click on a malicious link or download malware. For example, users may think they have received a notice from their bank, or a virus warning from the system administrator, when they have actually received a mass-mailing worm. Other examples include e-mail messages claiming to be an e-card from an unspecified friend to persuade users to open the attached “card” and download the malware. Malware can also be downloaded from web pages unintentionally by users. A recent study by Google that examined several billion URLs and included an in-depth analysis of 4.5 million found that, of that sample, 700 000 seemed malicious and that 450 000 were capable of launching malicious downloads.[20] Another report found that only about one in five websites analysed were malicious by design. This has led to the conclusion that about 80% of all web-based malware is being hosted on innocent but compromised websites unbeknownst to their owners.[21]

A different report found that 53.9% of all malicious websites observed are hosted in China.[22] The United States ranks second in the same study with 27.2% of malicious websites observed located in there. Furthermore, data provided in Annex A of this report demonstrates that malware on web pages accounts for 52.8% of incident reports by mid-2007 received by the United States Computer Emergency Readiness Team (US-CERT).

Malware propagation vectors

Malware propagation vectors refer to the electronic methods by which malware is transmitted to the information systems, platforms or devices it seeks to infect. Email and instant messaging applications are some of the most common vectors used for spreading malware through social engineering techniques. Any medium that enables software to be distributed or shared, however, can be a vector for malware. Examples of malware propagation or distribution vectors include the World Wide Web (WWW), removable media (such as USB storage keys), network-shared file systems, P2P file sharing networks, Internet relay chat (IRC), Bluetooth or wireless local area networks (WLAN).[23]

[18] See Annex E – Glossary of Terms.

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

[20] Google Inc. p.2.

[21] Sophos (2007) p.4.

[22] Sophos (2007) p.6.

[23] See Annex D for additional detail of propagation vectors.

Bluetooth is one prominent vector for malware propagation on mobile devices. Bluetooth is a wireless personal area network (PAN) that allows devices such as mobile phones, printers, digital cameras, video game consoles, laptops and PCs to connect through unlicensed radio frequency over short distances. Bluetooth can be compromised by techniques such as bluejacking and bluesnarfing[24] and is most vulnerable when a user’s connection is set to "discoverable" which allows it to be found by other nearby bluetooth devices.[25]

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

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

Box 2. Malware on mobile devices

There is some debate around the current seriousness of threats to mobile devices such as cell phones, PDAs, and smartphones.[26] For example, some factors seem to indicate that threats to mobile devices are still limited. These factors include the following: *i*) some of the current forms of mobile attacks can only be launched within the 10 metres personal area network (PAN)[27] range - which limits the scope of the danger compared to traditional malware threats which have a global reach; *ii*) mobile devices are restricted by bandwidth because there is a limited amount of spectrum allocated for their use; *iii*) the very small user interface is still an impediment to conducting Internet banking and other value transactions – until mobile devices become a popular means to conduct such transactions there are fewer incentives for attackers to develop malware for the mobile telephone platform;[28] *iv*) the cost associated with using general packet radio service (GPRS) to connect to Internet Protocol (IP) data networks may also make the mobile device less popular compared to Internet-connected PC which use technologies such as asymmetric digital subscriber line (ADSL), cable or broadband wireless.

However, there is also recognition that such threats, while emerging, are quite real.[29] Some data shows that although still relatively small in comparison to the amount of PC malware, mobile malware, which first appeared in 2004, increased from only a few instances to over 300 in total in a two year period.[30] Further, concerns about security increase as mobile devices become more prevalent and are used to access more critical or 'valuable' services.[31] For example, the use of smartphones is on the rise with projections as high as 350 million in use by 2009.[32] In 2006, Apple announced that a number of video iPods had been shipped to customers with the RavMonE virus.[33] Many experts are concerned that mobile malware will soon become far more dangerous to the mobile devices themselves, the wireless networks over which those devices communicate and the corporate networks, servers and/or personal computers with which those devices exchange information. Undetected malware on a smartphone could get transferred to a corporate network and used to perform further malicious functions.[34]

What is malware used for?

The numerous types of malware can be used separately or in combination to subvert the confidentiality, integrity and availability of information systems and networks. Likewise, a range of different attacks can be conducted to reach different goals, such as denying access to critical information systems, conducting espionage, extorting money (*e.g.* ransom), or stealing information (*e.g.* ID theft).

[26] A Smartphone is a cellular phone coupled with personal computer like functionality.

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

[28] These transactions are possible as is demonstrated by the Japanese market (see BBC).

[29] Hypponen, Mikko (2006) p.73 (4 of 8).

[30] Hypponen, Mikko (2006) p. 72 (2 of 8).

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

[32] Hypponen, Mikko (2006) p. 73 (3 of 8).

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

[34] iGillottResearch Inc (2006) p.8.

Malware can also be used to compromise authenticity and non-repudiation or conduct attacks on the Domain Name System (DNS).[35]

Denying access

Denying access to digital data, network resources, bandwidth, or other network services (denial of service - DoS) is a common goal of attacks using malware. Popular targets include companies that conduct business online and risk losing significant revenue for every minute their website or network is unavailable, and governments who rely on websites to provide essential services to their citizens. These attacks are usually used for sabotage (for example, to hurt a competitor or an organisation against whom the attacker holds a grudge or grievance), extortion,[36] or for politically and ideologically motivated purposes.

Distributed Denial of Service (DDoS) attacks

The most well known and perhaps most common method to deny access is distributed denial of service attacks (DDoS). DDoS attacks seek to render an organisation's website or other network services inaccessible by overwhelming them with an unusually large volume of traffic.[37] Malware indirectly contributes to DDoS attacks by creating a renewable supply of compromised computers (bots[38]) through which the flood attacks are launched. DDoS traffic may consist of relatively easily identified bogus packets, or properly-formed and seemingly legitimate "requests for service." This flood of traffic is intended to exceed the capacity of either the network bandwidth or the computer resources of the targeted server, or both, thereby making the service unavailable to most or all of its legitimate users, or at least degrading performance for everyone.

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

DDoS attacks have been launched against governments for various purposes including political or ideological ones. For example, Swedish government websites were attacked in the summer of 2006 as a

[35] See Annex B for further information on types of attacks.

[36] Messmer, Ellen and Pappalardo, Denise (2005).

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

[38] See "The Malware Internet: Botnets" chapter of this report for a comprehensive discussion of bots and botnets.

protest against the country's anti-piracy measures. More recent events in Estonia have raised an interesting discussion on what a cyber attack of this nature means for countries.[39]

Box 3. The Estonian case[40]

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

Estonia's computer emergency response team (EE-CERT) acted swiftly and, in collaboration with partners from the international community, was able to weather a very serious attack with little damage. The attack was primarily defended through filtering – blocking connections from outside Estonia. For example, Estonia's second largest bank, SEB Eesti Uhispank, blocked access from abroad to its online banking service while remaining open to local users.[41] One major contributor to the stability of their services domestically during the attack was the fact that Estonia has two domestic Internet exchange points (IXPs).[42]

Three weeks after the attacks ended, one researcher identified at least 128 separate attacks on nine different websites in Estonia. Of these 128 attacks, 35 were reportedly against the website of the Estonian Police, another 35 were reportedly against the website of the Ministry of Finance, and 36 attacks were against the Estonian parliament's, prime minister's, and general government websites.[43] It has further been estimated that some of the attacks lasted more than 10 hours, exceeded 95Mbps, and peaked at about million packets per second. While this may seem like a lot, other attacks considered "big" by security experts usually peak at about 20 million packets per second, 5 times more than the attack against Estonia. This has led experts to conclude that the attack was not optimised for maximum impact on and damage to the network, but rather to make a statement and prove a point.

Extorting money: Ransom

Some malware is designed to encrypt or scramble users' data so that the owner cannot retrieve it. Often the owner will be asked to pay a ransom for the "key" used to encrypt their data, and which is often required to reverse that process and restore the data.[44] Although this type of malware is not as prevalent as other types of malware, there were several high profile cases in 2006 that raised attention around the issue.[45] Such attacks, not only deny the user/owner access to their own data, but harm the confidentiality and integrity of that data by the attacker's unauthorised access to it and encryption of it.

[39] For example, a senior official was quoted by *The Economist* saying "If a member State's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?"; See *The Economist* (2007).

[40] *The Economist* (2007)

[41] *The Sydney Morning Herald* (2007)

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

[43] Lemos, Robert (2007).

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

[45] Sophos (2007a) p.8.

Box 4. A ransom example: The Arhiveus[46]

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

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

INSTRUCTIONS HOW TO GET YOUR FILES BACK READ CAREFULLY. IF YOU DO NOT UNDERSTAND - READ AGAIN.

This is the automated report generated by auto archiving software.

Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder My Documents was archived with long password.

You cannot guess the password for your archived files - password length is more than 30 symbols that makes all password recovery programmes fail to brute force it (guess password by trying all possible combinations).

Do not try to search for a programme that encrypted your information - it simply does not exist in your hard disk anymore. Reporting to police about a case will not help you, they do not know the password. Reporting somewhere about our email account will not help you to restore files. Moreover, you and other people will lose contact with us, and consequently, all the encrypted information.

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

Espionage

Malware can be and has been used to gain access to or spy on business and government operations and gather information that could be critical to business operations or national security. Recently, the United Kingdom reported that a number of targeted trojan attacks had been directed against parts of the UK's public and private critical information infrastructure. These trojans were assessed to be seeking covert gathering and transmitting of privileged information.[47] Malware of this sort can also be used by companies and other organisations to gather information about their competitors as demonstrated by the below example.

Box 5. The case of Michael and Ruth Haephrati

In March of 2006, Michael and Ruth Haephrati were extradited to Israel from Britain where they were charged with creating and distributing a trojan used to conduct industrial espionage against some of the biggest companies in Israel.[48] Michael Haephrati is said to have developed and refined the programme while his wife, Ruth, managed business dealings with several private investigation companies which bought it and installed it on the computers of their clients' competitors. Specifically, the trojan horse is believed to have been used to spy on the Rani Rahav public relations agency (whose clients include Israel's second biggest mobile phone operator, Partner Communications), and the HOT cable television group. Another alleged victim was Champion Motors, who import Audi and Volkswagen motor vehicles.

Ruth Brier-Haephrati was formally charged with aggravated fraud, unlawful computer access, virus insertion, installing tapping equipment, invasion of privacy, managing an unlawful database, and conspiracy to commit a crime. Michael Haephrati was charged with lesser offenses as the prosecution regarded him as Ruth's assistant because his job was only to perfect the programme and tailor it to the needs of specific clients.[49]

[46] Sophos (2007b).

[47] United Kingdom Centre for the Protection of the National Infrastructure (2005).

[48] Messagelabs (2006) p.11.

[49] Sophos (2006c).

Stealing information

Over the past five years, information theft, and in particular online identity (ID) theft,[50] has been an increasing concern to business, governments, and individuals. Although malware does not always play a *direct* role,[51] ID theft *directly* using malware has become increasingly common with the rise of backdoor trojans and other stealthy programmes that hide on a computer system and capture information covertly.

As illustrated in Figure 1, online ID theft attacks using malware can be complex and can use multiple Internet servers to distribute spam and malware, compromise users' information systems, and then log the stolen data to another website controlled by the attacker or send it to the attacker's e–mail account. Generally, the attacker operates under multiple domain names and multiple IP addresses for each domain name and rapidly rotates them over the life of the attack (for example see botnet hosted malware sites #1 and #2 in Figure 1).[52] The use of multiple domain names and multiple hosts or bots (and their associated IP addresses) is designed to increase the time available for capturing the sensitive information and reduce the effectiveness of efforts by affected organisations (such as banks), CSIRTs and ISPs to shut down fraudulent sites. Under the domain name system (DNS) attackers are able to quickly and easily change their DNS tables[53] to reassign a new IP addresses to fraudulent web and logging sites operating under a particular domain.[54] The effect is that as one IP address is closed down, it is trivial for the site to remain active under another IP address in the attacker's DNS table. For example, in a recent case IP addresses operating under a single domain name changed on an automated basis every 30 minutes and newer DNS services have made it possible to reduce this time to five minutes or less. Attackers may use legitimate existing domains to host their attacks, or register specially created fraudulent domains. The only viable mitigation response to the latter situation is to seek deregistration of the domain.[55]

[50] See DSTI/CP(2007)3/FINAL where Identity Theft is defined as the unlawful transfer, possession, or misuse of personal information with the intent to commit, or in connection with, a fraud or other crime.

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

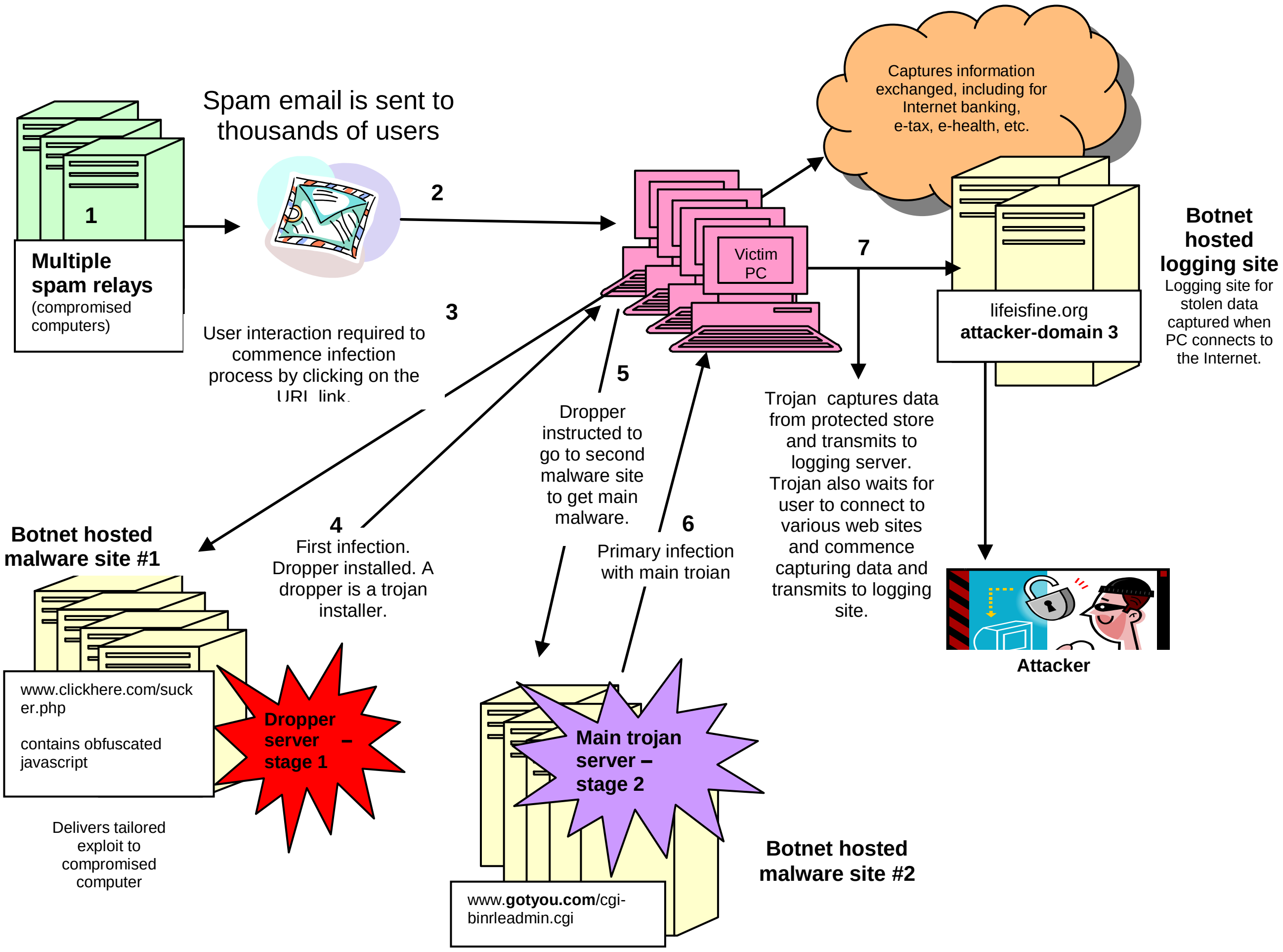
[52] This is a technique known as "fast flux".

[53] A DNS table provides a record of domain names and matching IP addresses.

[54] See Annex B for a discussion on attacks using the DNS and attacks against the DNS.

[55] AusCERT (2006) p.19-20.

Figure 1. Online ID theft attack system involving malware[56]

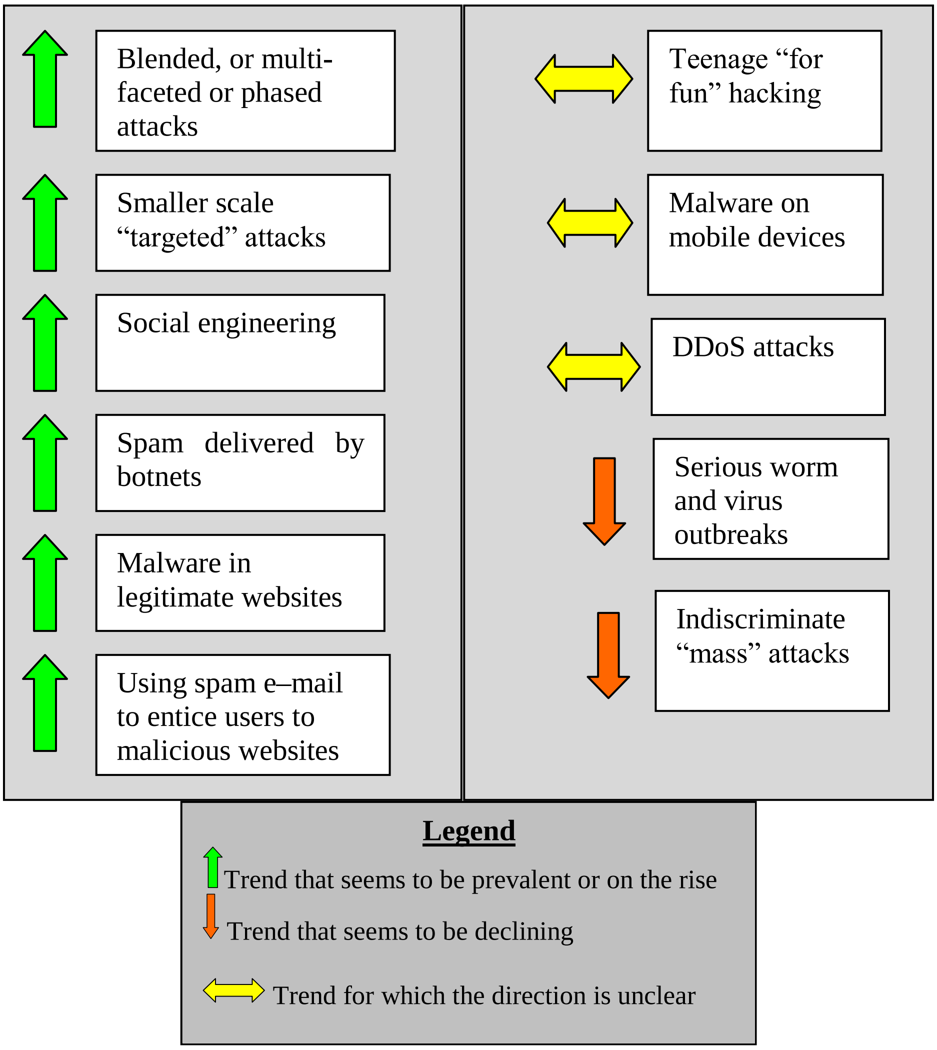

Spam email is sent to thousands of users
1
Multiple spam relays
(compromised computers)
2
3
User interaction required to commence infection process by clicking on the URL link.
Captures information exchanged, including for Internet banking, e-tax, e-health, etc.
Victim PC
7
Botnet hosted logging site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

Malware attack trends

The dynamic nature of malware keeps most security experts constantly on the lookout for new types of malware and new vectors for attack. Due to the complex technical nature of malware, it is helpful to examine overall attack trends to better understand how attacks using malware are evolving. As mentioned previously, the use of malware is becoming more sophisticated and targeted. Attackers are using increasingly deceptive social engineering techniques to entice users to seemingly legitimate web pages that are actually infected and/or compromised with malware. Figure 2 illustrates the types of attack that seem to be on the increase, those that are falling out of favour, and those for which the trend remains unclear or not changed.

[56] AusCERT (2006) at 7.

Figure 2. General attack trends


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

Origin of malware attacks

Origin refers to both where the attackers who launch the attack are based and where the computer systems that actually attack the targeted system are located. In most cases, it is easy to see where the attacking computer systems are hosted based on their Internet protocol or "IP" addresses, but this is not usually sufficient to identify the person responsible for launching the attack. For example, "spoofing" is a technique designed to deceive an uninformed person about the origin of, typically, an e–mail or a website.[57]

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

Moreover, rarely is the attacker located in the same geographic region as the attacking hosts. It is common practice among cybercriminals[58] to use compromised computers (and to a lesser extent anonymous proxies[59]) hosted in a foreign legal jurisdiction to launch their attacks. This protects their identity and provides additional computing resources beyond what they could otherwise afford. Criminals are acutely aware of the significant jurisdictional impediments that hinder or even prevent cybercrime investigations from being conducted if the crimes are sourced internationally.

Malware is now spread around the world and rankings[60] tend to show that a whole host of countries across the developed and the developing world are home to online criminals using malware. Although attacks originating from one country may have local targets, the predominant trend is attacks that originate internationally relative to their targets. In addition, geography may play a role depending on the end goal of the attacker. For example, broadband Internet speeds differ from country to country. If an attacker wishes to maximise network damage, he/she may use compromised computers located in countries where broadband is prevalent. If the goal is to degrade service or steal information over time, the attacker may use compromised computers from a variety of geographical locations. Geographical distribution allows for increased anonymity of attacks and impedes identification, investigation and prosecution of attackers.

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

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

[60] For example, see Symantec (2007) p. 9.

THE MALWARE INTERNET: BOTNETS

What is a botnet?

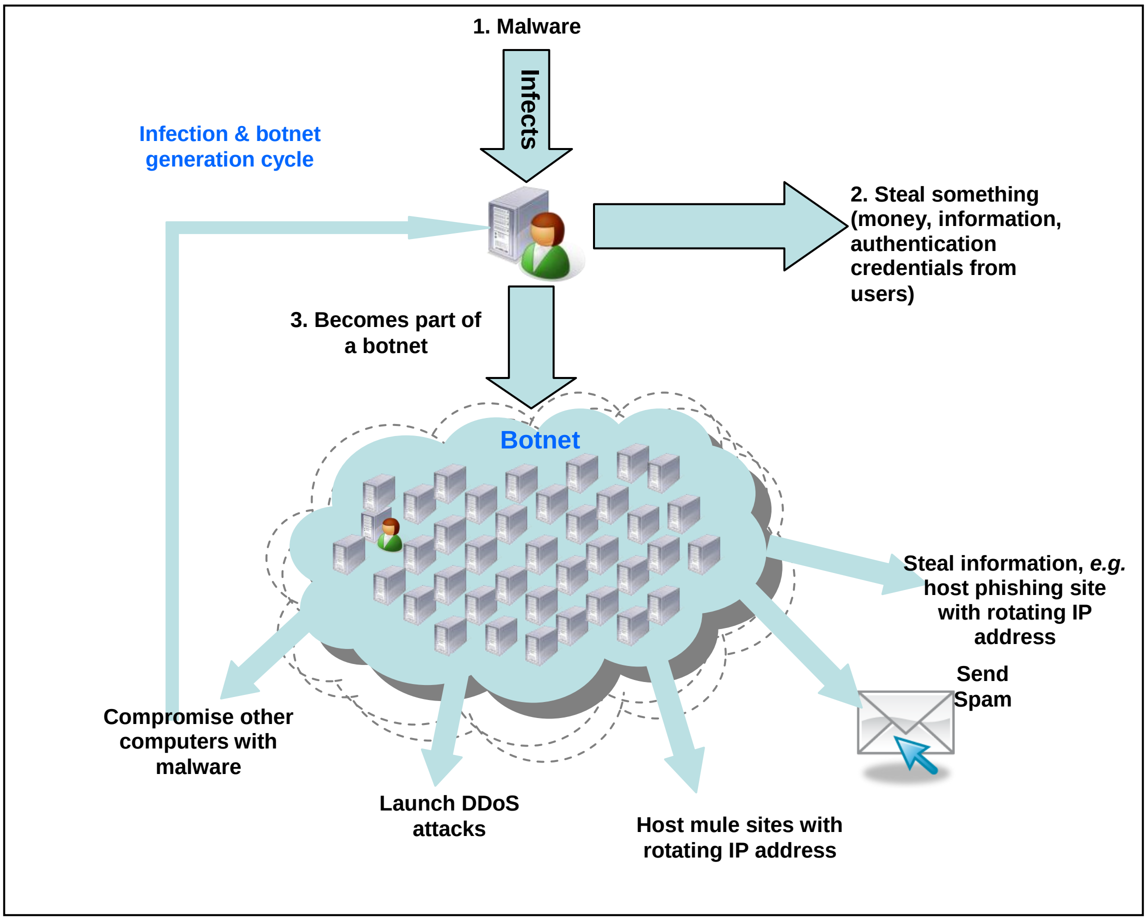
A now prevalent form of malware, botnets are key tools attackers use to conduct a variety of malicious activity and cybercrime. A botnet is a group of malware infected computers also called "zombies" or bots that can be used remotely to carry out attacks against other computer systems.[61]

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

Figure 3 demonstrates the relationship between malware and the botnet lifecycle. When malware infects an information system, two things can happen: something can be stolen (*e.g*, information, money, authentication credentials etc.) and the infected information system can become part of a botnet. When an infected information system becomes part of a botnet it is then used to scan for vulnerabilities in other information systems connected to the Internet, thus creating a cycle that rapidly infects vulnerable information systems.

[61] In this paper, the term "bot" refers to a malware-infected computer that a malicious actor can remotely control and turn into a "robot" or zombie machine. Thus "botnets" should be understood as networks of such bot machines. However, the term "bot" can be encountered in other contexts as it generally refers to a variety of software programme or script that executes automated tasks. It is most widely used in the context of Internet Relay Chat (IRC) where users can create and use bot scripts for online gaming, co–ordinating file transfers, and automating channel admin command (EggDrop is one of the oldest of such benign IRC bots). The fact that botnets often rely on IRC bots for command and control by botmasters might explain why the term "bot" is so popular in the literature and discussions related to malware.

Figure 3. The Botnet Lifecycle


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

What are botnets used for?

Botnets are mostly used for the following purposes:

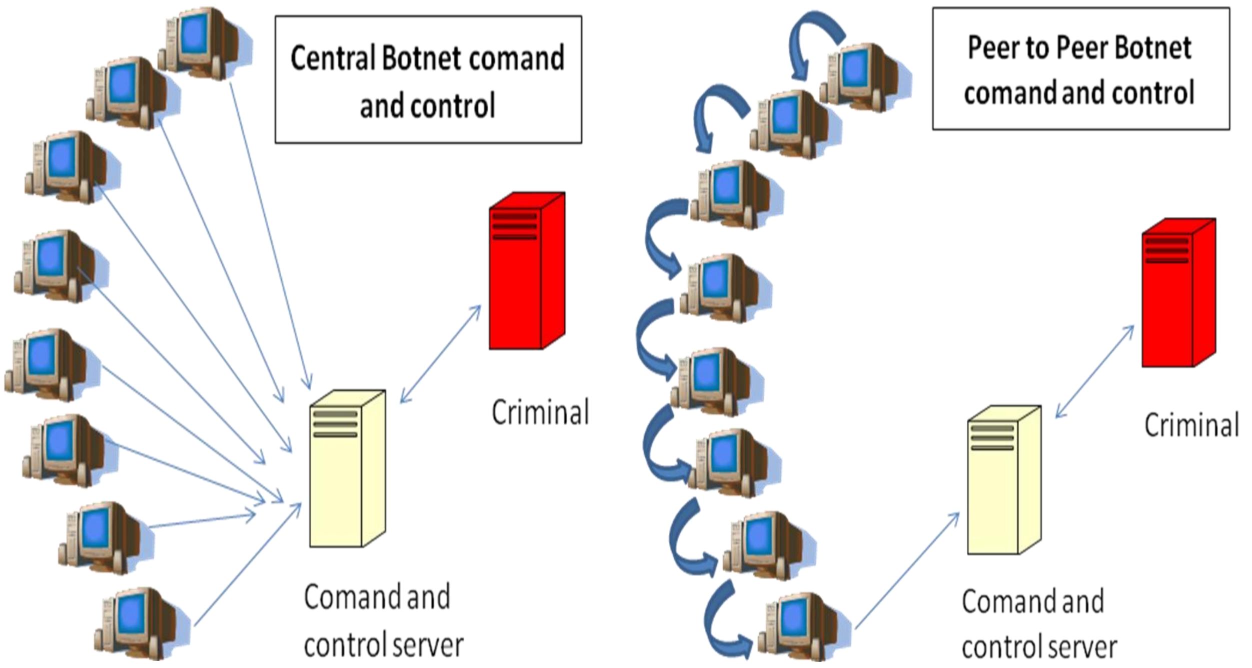
1. Locate and infect other information systems with bot programmes (and other malware). This functionality in particular allows attackers to maintain and build their supply of new bots to enable them to undertake the functions below, *inter alia*.
2. Conduct distributed denial of service attacks (DDoS).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

Botnets Command and Control (C&C) models

Typically, bots communicate with the bot master through an Internet Relay Chat (IRC) command and control (C&C) server which provides the instructions directing the operation of the botnet. The C&C server usually is also itself a compromised computer running various network services. After a computer system is infected and compromised by a bot program, the bot periodically connects back to the C&C server, checking for instructions. Although there are various C&C models, the most popular has traditionally been the centralised model (see Figure 4) where all bots report to a single location to wait for commands. The centralised model is popular among bot masters because it offers software tools that make it easy to operate. Furthermore, the centralised model results in few communication delays between the bot master and the bots.[62] Increasingly, attackers are also using the HTTP and HTTPS web protocols[63] as the communication method between bots and the C&C server. This means that it is more difficult for network operators to detect and block bot communications to or from their network as it is hidden among the vast volume of normal web traffic.

An alternative innovative C&C model designed to make it more difficult for security practitioners to stop botnet hosted attacks is the increasing use of the peer to peer (P2P) model (see Figure 4).[64] The peer to peer model lacks a central hierarchy of communication which makes the botnet more resilient to dismantling. [65] It is therefore extremely difficult to stop attacks launched from botnets that communicate using P2P as there is no single point of failure.

Figure 4. Command and control for Botnets


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

[62] Trend Micro (2005) p.8.

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

[64] Govcert.nl (2007) p. 11-12.

[65] Trend Micro (2005) p. 8-9.

In addition to the models above, botnets are increasingly using what is known as “fast flux” networks to evade detection. Fast flux networks are networks of compromised computer systems with public DNS records that change constantly thus making it more difficult to track and shut down malicious activity.[66] Furthermore, this model abandons the traditional centralised C&C server and uses proxies to hide the servers controlling the fast flux network.

Botnet figures

While botnets vary in size, they typically number tens of thousands of compromised computers. There have been exceptions including a group of attackers in The Netherlands who reportedly controlled 1.5 million bots.[67] Typically the number of bots being controlled by a single attacker will fluctuate depending on whether the compromised computers are connected to the Internet, whether they have been “cleaned”, or whether the attacker is using his botnet to locate and compromise more information systems to add to the botnet. Furthermore, there are incentives for bot herders to use smaller botnets and launch smaller, more targeted, attacks to avoid detection. For example, large botnets sending spam or conducting DDoS attacks generate a high volume of network traffic that is usually detectable by ISPs and network administrators whereas smaller attacks that use less bandwidth may go undetected.

Botnets have become a contracted commodity. Malicious actors can hire or buy a bot master to carry out an attack. One report averaged the weekly rental rate for a botnet at USD 50 – 60 per 1 000 – 2 000 bots or around 33 cents per compromised computer.[68] This is extraordinarily cheap compared to the cost of the computer to the legitimate owner in terms of hardware, software and bandwidth.

The prevalence of botnets has been increasing. Although estimates of the number of botnets can vary widely, most experts agree it is a large amount. For example, in 2006, the Chinese National Computer Network Emergency Response Technical Team Coordination Centre (CNCERT/CC) reported that 12 million IP addresses in China were controlled by botnets.[69] They also found more than 500 botnets and more than 16 000 botnet command and control servers outside China.

[66] The Honeynet Project (2007) p.1.

[67] Govcert.nl (2006) p. 8.

[68] MessageLabs (2006) p. 4.

[69] Dr. Du, Yuejun (2007) p.13.

Box 6. The Dutch Botnet case

In October 2005 the Dutch National Police arrested three men - members of a group of cyber criminals - suspected of large scale "hacking". The men controlled several botnets that were thought to have consisted of over 1.5 million infected computers.[70] The botnets played a key role in numerous cyber crimes including: phishing, identity theft, online fraud, and online extortion. In due course, it became clear that botnets played a central role in the activities of the cyber criminals by serving as the basic infrastructure that allowed for the successful attacks.

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

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

Botnets and broadband

The increased threat of botnets can partially be explained by the increased use of broadband connections to access the Internet. Further efforts are needed from users, as well as providers, to protect their security and privacy in the online environment. By 2004, broadband Internet connections were already widespread in OECD countries. For example, in Korea 86% of households and 92% of businesses had a broadband connection via a computer or mobile phone in 2004.[71] In the following two years, those numbers have continued to increase. At the end of 2005, there were around 265 million active subscribers to fixed Internet connections in OECD countries. Of these, 60% were using broadband access, and broadband subscriptions have increased by more than 60% a year over the last five years. By mid-2006, there were more than 178 million broadband subscribers in the OECD area. European countries have continued to advance, with Denmark, the Netherlands and Iceland overtaking Korea and Canada in terms of broadband penetration rates over the past year.[72]

The broadband transition to faster upload bandwidth via fibre could make the botnet problem much more severe. The potency of one infected computer on a fibre connection could be equivalent to 31 infected computers on DSL and 44 computers on cable networks.[73] This will be one of the key areas of concern for policy makers dealing with telecommunication networks and security in the near future.

[70] Govcert.nl (2006) p.8.

[71] OECD (2005).

[72] OECD (2007) p. 130.

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

Spam and botnets

There is a correlation between botnets and spam due to changes in spamming techniques over the last few years. Spam commonly refers to bulk, unsolicited, unwanted and potentially harmful electronic messages.[74] Attackers have found convenience in co-operating with spammers by using their e–mail lists to send mass quantities of spam – which often contain other malware as an e–mail attachment[75] - through botnets. For example, the second most common malicious code family reported from January - June 2006, Bomka, was a trojan downloadable from a link provided in a spam e–mail that used social engineering techniques to persuade the user that the link was the site of a video clip.[76] The problem of spam and malware is also cyclical and self-sustaining. Information systems compromised by malware are used to distribute spam and a proportion of the spam that is distributed is designed to distribute malware to new victims whose information systems will be used to undertake further online malicious activity.

It is important to note that not all spam contains malware and it is often difficult to determine how much spam *directly* contains malware. Manual analysis conducted by The Information and Communication Security Technology Center (ICST) in Chinese Taipei over the course of two years on 417 suspect e–mails found that of those 417 analysed, 287 (68%) contained malware attachments.[77] Other data shows that in 2006, only 1.5% or 1 in every 67.9 e–mails analysed contained a virus or trojan; and according to the same report, in 2005 the annual average was 2.8%, or 1 in every 36.1.[78] It is likely that the disparate nature of these findings can be explained by a lack of comparable techniques to determine when spam contains malware.

Recently, the Messaging and Anti-Abuse Working Group (MAAWG) reported that the percentage of email identified as "abusive"[79] has been oscillating between 75% and 80%.[80] They attribute the fluctuation to service providers dealing with new schemes introduced by abusers to escape service providers' detection methods, including filters. Nonetheless, it is widely accepted that the vast majority of spam is sent from botnets. The effectiveness and wide availability of compromised information systems with high speed broadband connections means that spam levels are at their highest levels ever despite many initiatives to reduce and prevent spam being distributed.

[74] OECD (2006) p. 25.

[75] SOPHOS (2006a) p. 2.

[76] Symantec (2006) p. 68.

[77] Liu, Pei-Wen (2007) p. 3, note that this data is based on self-selected spam that fits a certain category or type and therefore is representative of a smaller sample set. Furthermore, this data does not include the mass mailing worms/viruses.

[78] MessageLabs (2006) at 7.

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

[80] Messaging Anti-Abuse Working Group (MAAWG) (2007) p. 2.

Box 7. FTC v. Dugger

In one recent case, the US Federal Trade Commission (FTC) sought to stop the underlying use of botnets to send spam (FTC v. Dugger). The FTC alleged that the defendants relayed sexually-explicit commercial e-mails through other people's home computers without their knowledge or consent. They further alleged that the defendant's conduct violated the CAN-SPAM Act.[81] Under the final order, the defendants were barred from violating the CAN-SPAM Act and required to turn over USD8 000 in profits made through use of the botnet. The defendants were also required to obtain the authorisation of a computer's owner before using it to send commercial e–mail and to inform the owner how the computer will be used.

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

The role of blacklists in combating botnets

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

Most of the lists are free and run by volunteers, though their operations may be funded through external sources. Each DNSBL has its own criteria for including an IP address in the list and its own procedure for getting an address off the list. Spamhaus, an international nonprofit organisation funded through sponsors and donations, maintains several well-known blacklists – though they prefer the term block lists – which they claim are used to protect over 600 million user inboxes. One of their lists contains the addresses of "spam-sources, including spammers, spam gangs, spam operations and spam support services"; another list focuses on botnets which run open proxies. It should be noted at this point that blacklisting, while potentially powerful, has drawn its own criticisms – regarding, among other things, vigilantism of blacklist operators, listing false positives, the collateral damage that may come with blacklisting certain IP addresses or ranges, and the financial motives of some list operators. Furthermore, blacklists have faced legal challenges from spammers, who on occasion were successful in obtaining court verdicts against being blacklisted. According to interviewees in a recent empirical study,[82] most ISPs use blacklists.

Blacklisting and ISPs[83]

Blacklisting does provide an incentive to invest in security because it directly impacts an ISP's business model. For example, one medium-sized ISP reported a security incident where 419 spammers[84] set up over 1 000 e–mail accounts within their domain and then started pumping out spam. That got the ISP's outbound mail servers blacklisted, which resulted in a high volume of calls to their customer center

[81] More information on the CAN-SPAM Act is available at: http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.shtm

[82] OECD (2007b) p. 33.

[83] Note: this text has been extracted from the original report. See OECD (2007b) p. 33-34.

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

by customers who noticed their e–mail was no longer being delivered. That number doesn't include the incoming abuse notifications, of which there were purportedly "even more." In another example, a security officer at a large ISP explained that being blacklisted led to a much more proactive approach to remove bots from their network, including the purchase of equipment that automates the process of identifying infected machines on the network.[85] In mid-2007, this particular ISP identified around 50 customers per day and, if the customer did not resolve the problem, the connection was suspended.

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

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

Blacklisting and Domain Name Registrars

Registrars offering hosting and e–mail services are subject to blacklisting along the same lines as the ISPs. Blacklist operators also watch registrars and their responsiveness to abuse complaints. In extreme cases, blacklists may include the registrar itself. A case in point is the recent dispute between the blacklist operator Spamhaus and the Austrian registry/registrar Nic.at. Spamhaus had requested Nic.at to remove several domain names it said were associated with phishing by the "rock phish" gang. Nic.at did not comply with these requests, citing legal constraints. The registrar argued that it could not legally remove the sites, unless Spamhaus provided clear proof that the domain names had been registered using false information.[86] The conflict escalated when Spamhaus added the outbound mail server of Nic.at to one of its blacklists – listing them as "spam support" – so that the registrar's e–mail was no longer accepted by the multitude of servers using this popular blacklist. About ten days later Spamhaus changed the listing of Nic.at to a symbolic listing – no longer actually blocking the IP addresses, but keeping them listed as "spam support." Several of the offending domains had been removed, but Nic.at denies that it had complied with Spamhaus' request and asserts that the hosting providers took action.[87]

[85] OECD (2007b) p. 34.

[86] Sokolov, D. A. (2007).

[87] ORF (2007) and Spamhaus (2007) .

THE MALWARE ECONOMY

The malicious actors

Who are the malicious actors?

Research shows that the range of malicious actors developing and deploying malware spans from amateurs seeking fame to serious organised cyber criminals. It can also be assumed that nation states have the same capabilities. Figure 5 diagrams the malicious actors from the “Innovators” to “Organised Crime”[88] based on a recent report on criminal activity on line. It is important to note, however, that there is also a whole category of actors whose motivations are political or ideological rather than solely financial.

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

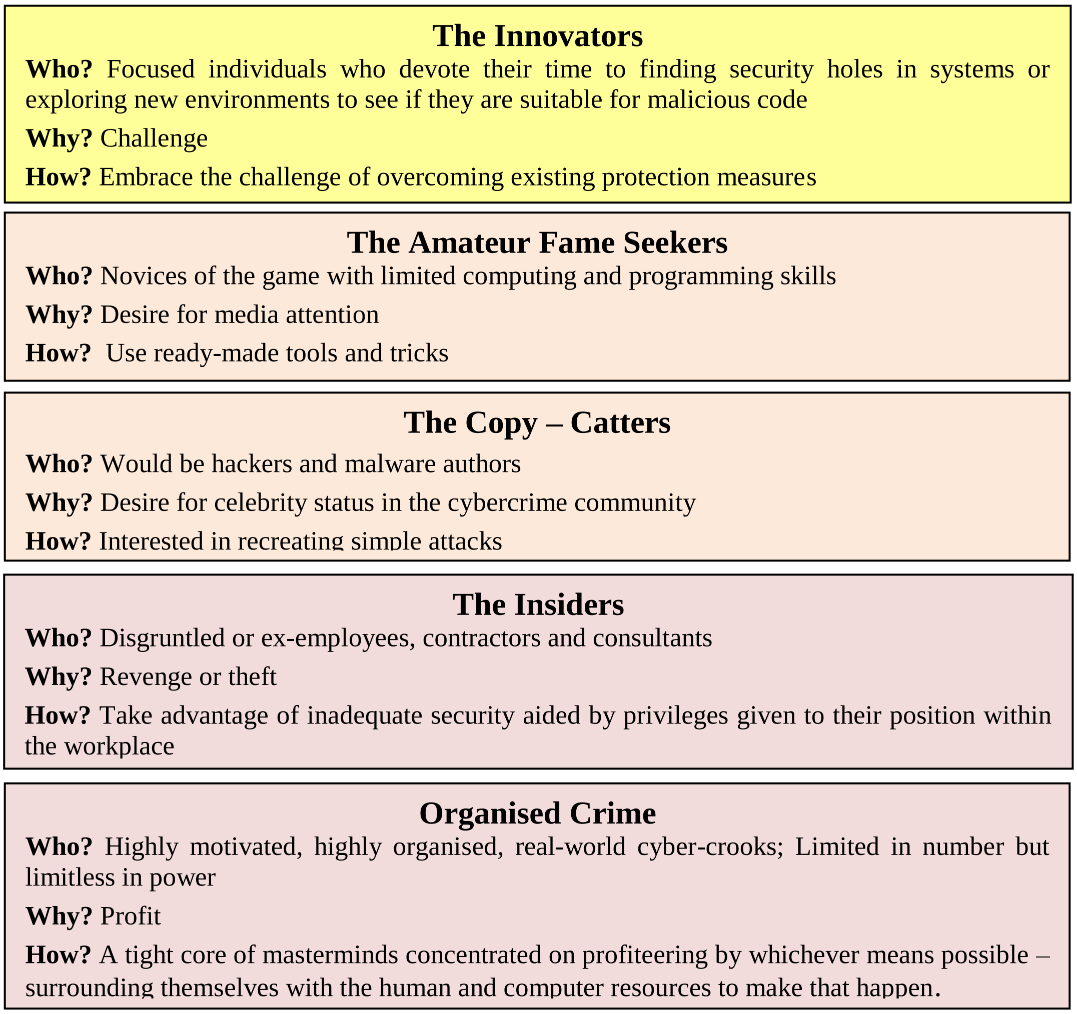
Figure 6 illustrates the evolution of malware in terms of malicious intent of the actors showing a clear evolution from fame seeking “techies” to criminals motivated by financial gain.

What are their capabilities and motivations?

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

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

Figure 5. Malicious Actors[89]



The Innovators

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

Why? Challenge

How? Embrace the challenge of overcoming existing protection measures

The Amateur Fame Seekers

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

Why? Desire for media attention

How? Use ready-made tools and tricks

The Copy – Catters

Who? Would be hackers and malware authors

Why? Desire for celebrity status in the cybercrime community

How? Interested in recreating simple attacks

The Insiders

Who? Disgruntled or ex-employees, contractors and consultants

Why? Revenge or theft

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

Organised Crime

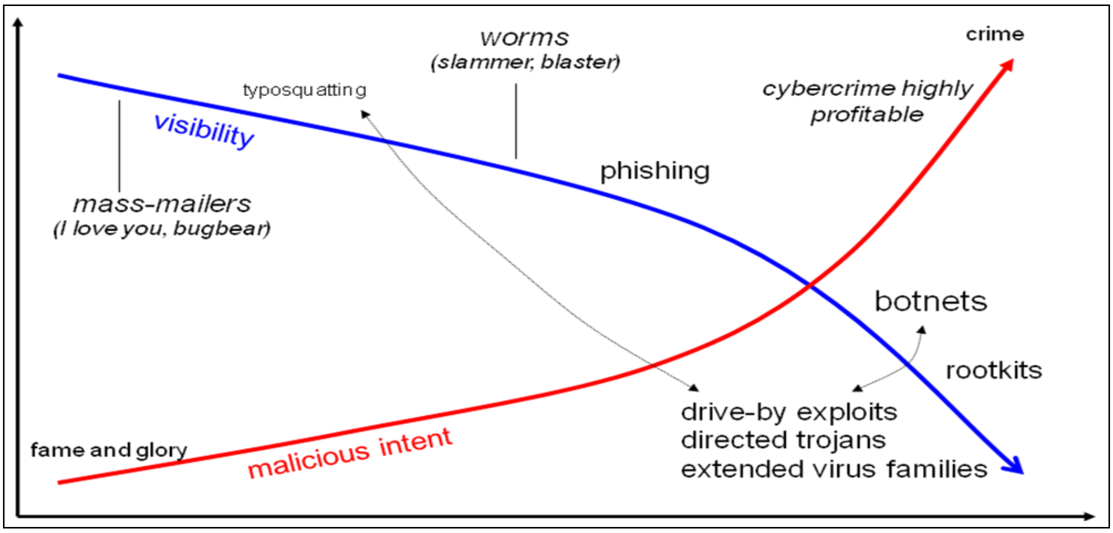
Who? Highly motivated, highly organised, real-world cyber-crooks; Limited in number but limitless in power

Why? Profit

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

[89] McAfee Inc. (2006) p.9.

Figure 6. Visibility of malware vs. malicious intent[90]



The malware business model

One expert recently noted that "creating one's own bot and setting up a botnet is now relatively easy. You don't need specialist knowledge, but can simply download the available tools or even source code."[91] In addition, "off-the-shelf" kits with ready-made trojans can be downloaded from the Internet. Some versions are guaranteed by the authors to remain undetected by security defences and some even include a "service level agreement" by which the author guarantees, for a certain period of time, to create new versions for the criminal once the original malware is detected. It has been estimated that this service can cost as little as USD 800.[92] In addition, many malicious services, such as botnets, are available for hire.[93]

Malware, and by extension its main propagation vector, spam,[94] are increasingly combined as key underpinnings of criminal techniques to make profit in the rapidly evolving "Internet economy". Malware has evolved into "mass market" money-making schemes because it offers such a profitable business model. Malware techniques are becoming increasingly sophisticated, but some users continue to lack appropriate protection. Understanding the malware business model can help industry participants and policy makers alike to more effectively combat malware threats by undermining their economic profitability. The spread of malware is driven by the very real prospect of economic gain although the information targeted by attackers can be sought for a variety of purposes (for pure identity theft or corporate espionage, or to gain access to privileged or proprietary information or to deny access to critical information systems).

As attackers continue to remain successful at launching attacks, the malware economy becomes self-perpetuating. Spammers, phishers, and other cyber criminals are becoming wealthier, and therefore have

[90] Chart provided by Govcert.nl (www.govcert.nl).

[91] McAfee Inc. (2006) p.6.

[92] MessageLabs (2006) p. 14.

[93] See infra p. 25.

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

more financial power to create larger engines of destruction. It is a big business, often led by wealthy individuals, with multiple employees and large bankrolls of illicit cash. In addition to an increased frequency and sophistication of attacks, the amount of damage is significant.[95]

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

Basic economic rationale for malware

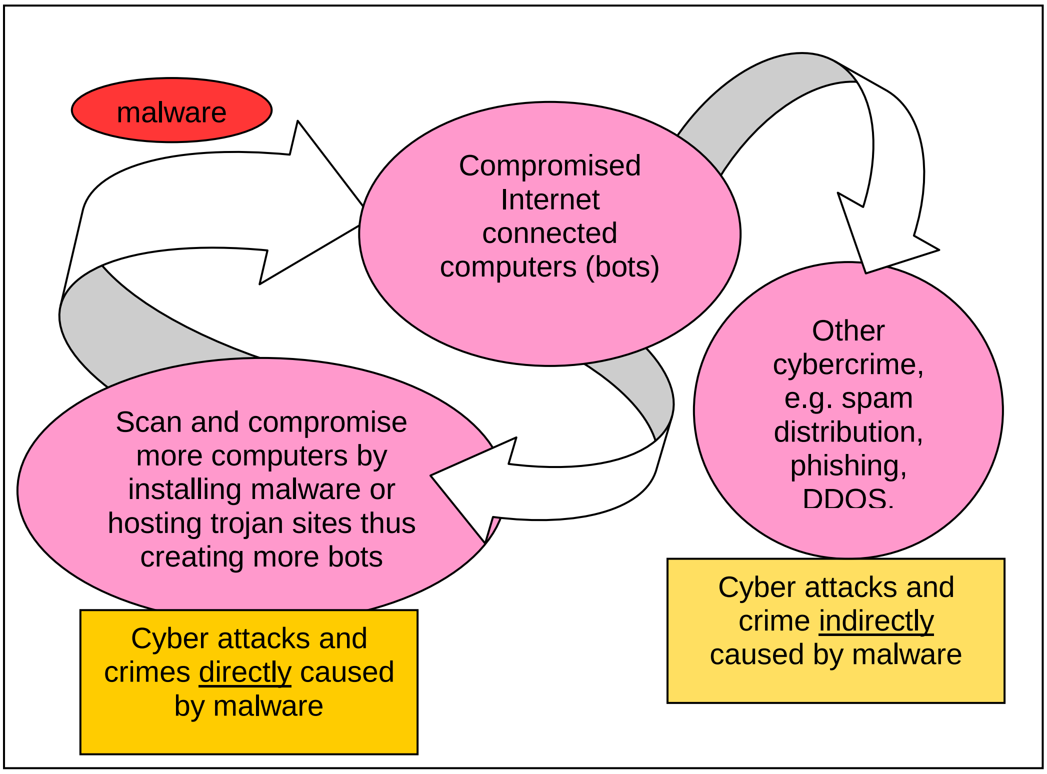
E-mail is not at an economic equilibrium between the sender and the recipient because it costs virtually nothing to send. All the costs of dealing with spam and malware are passed on to the Internet provider and the "unwilling" recipients, who are charged for protective measures, bandwidth and other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

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

Both the malware itself and the compromised computers being used to further launch malware attacks are a low cost, readily available and easily renewable resource. High speed Internet connections and increased bandwidth allow for the mass creation of compromised information systems that comprise a self sustaining attack system as illustrated by Figure 7. Furthermore, malicious actors can replace compromised information systems that have been disconnected or cleaned, and they can expand the number of compromised information systems as the demand for resources (namely malware and compromised information systems) for committing cybercrime also grows.

[95] See "Malware: Why should we be concerned?" for a discussion of the impacts from malware

Figure 7. Self sustaining attack system using malware


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

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

Underlying business process

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

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

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

Criminals develop, maintain and sell malware, botnets, spam transmission software, CDs full of addresses harvested from web pages, lists of open proxy servers and lists of open simple mail transfer protocol (SMTP)[96] relays. The lists of addresses or controls of a botnet are then rented out or sold. These lists are often inexpensive at around USD 100 for 10 million addresses. An entire online criminal operation could be carried out at little or no cost, the only hard costs are various “utilities” such as bandwidth, Internet connection, e–mail addresses, or web hosting, and even those can be financed illegally.

While the use of malware to facilitate cybercrime, particularly crimes motivated by illicit financial gain, has increased, the money made through malicious online activity has become increasingly difficult to trace. As in traditional criminal investigations, tracing where the money goes by analysing the cash flows could provide essential information on the attackers. However the victims of online malicious activity are increasingly asked to pay by wire transfers (46% of online scams transactions in the US in 2006), followed by card payment (28%), both much preferred for their speed and the potential to mask tracks easily, by comparison with cheques or cash, which now represent less than 10% of the payments.[97] These types of payments are fast and can be made almost anonymously through the use of multiple financial accounts across borders. Alternative payments systems such as ‘e-Gold’ or PayPal used by criminals further down the chain make it even more difficult to trace financial movements. Users of these online payment services can open an account using a fraudulent name and deploy a proxy server to shield the originating IP address.

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

[97] United States National Consumer League / National Fraud Information Center (2006) p. 2.

MALWARE: WHY SHOULD WE BE CONCERNED?

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

Malware-enabling factors

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

Broadband Internet and its users

In 2005, the International Telecommunication Union estimated 216 708 600 "fixed" broadband Internet subscribers in the world.[98] Furthermore, it is generally agreed that there are an average of 1 000 000 000 Internet users in the world today. As the number of subscribers and users increases, so does the number of available targets for malware. The increased prevalence of high speed Internet and the availability of broadband wireless connections make it easy for malicious actors to successfully carry out attacks as they can compromise computers at faster rates, use the bandwidth to send massive amounts of spam and conduct DDoS attacks. Furthermore, these "always on" connections allow malicious actors to be mobile and to attack from any location including public places such as Internet cafes, libraries, coffee shops or even from a PDA or mobile phone device.[99] Operating from public places allows attackers to conduct their activities anonymously thus making it difficult to detect and trace their activities.

It is important to note that while broadband technologies are an enabling factor, it is the behaviours associated with these technologies that are problematic. For example, people often fail to adopt appropriate security measures when using broadband technologies and therefore leave their connection open without the appropriate security software installed.[100]

Ever more services available on line

Most governments, consumers and businesses depend on the Internet to conduct their daily business. In 2004, the OECD found that, in most OECD countries, over 90% of businesses with 250 or more employees had access to the Internet. Firms with 50 to 249 employees also had very high rates of access.[101] Home users rely on the Internet for their day to day activities including shopping, banking or simply exchanging information and conducting e-government and e-commerce transactions. As the amount of these services continues to increase, so does the likely community of users accessing these services on line.

[98] International Telecommunications Union (ITU) (2007) p. 23.

[99] McAfee Inc. (2007) p. 02 and 10.

[100] This could be the case for any Internet connection, broadband or otherwise.

[101] OECD (2005) E-7.

This in turn increases the available targets for attack or exploitation which provides further incentive for criminals to conduct malicious activity.

Operating system and software vulnerabilities

The more vulnerable the technology, the more likely it is to be exploitable through malware. For example, the security firm Symantec[102] reported a 12% increase in the number of known vulnerabilities from the first half of 2006 (January – June 2006) to the second half (June – December 2006) which they largely attribute to the continued growth of vulnerabilities in web applications. Microsoft also reported an increase of nearly 2 000 disclosed vulnerabilities from 2005 to 2006.[103] The increase in vulnerabilities corresponds to an increase in incidents. Microsoft reported an increase in the number of machines disinfected by its Malicious Software Removal Tool from less than 4 million at the beginning of 2005 to more than 10 million at the end of 2006.[104]

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

Easy to target average Internet user

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

Many Internet users are not adequately informed about how they can securely manage their information systems. This lack of awareness and subsequent action or inaction contributes to the increasing prevalence of malware. Most malware requires some form of user action or acceptance to propagate. Recent surveys from various organisations show that while more users are taking measures to protect their information systems, a large percentage of the population lacks basic protective measures. For example, a 2005 report commissioned by the Australian Government, *Trust and Growth in the Online Environment*, found that only one in seven computers in Australia use a firewall and about one in three use up-to-date virus protection software.[105] Furthermore, it is estimated that 59 million users in the US have spyware or other types of malware on their computers.[106]

The European Commission's Eurobarometer E-communications Household survey[107] observed an increase in consumer concerns about spam and viruses in 2006. For some EU Member States, up to 45% of

[102] Symantec (2007) p. 38.

[103] Microsoft (2006b) p. 8.

[104] Microsoft (2006b) p. 20-21.

[105] OECD (2007c) p. 33 – 34.

[106] Brendler, Beau (2007) p. 4.

[107] European Commission Eurobarometer (2007) p.89 .

consumers had experienced significant problems. In 40% of the cases, the computer performance decreased significantly, in 27% of the cases a breakdown was observed. In the same survey, 19% of consumers had no protection system at all on their computers. Other data also suggests that home users are the most targeted of all the sectors[108] accounting for 93% of all targeted attacks[109]and thus highlighting that weak user security is one important enabler of malware.

Impacts of malware

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

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

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

Financial impacts – sample data

Although precise data on online criminal activity and the associated financial losses is difficult to collect, it is generally accepted that malware contributes significantly to these losses.[110] Further, where data on cybercrime and its economic impact is available, businesses and governments are often reluctant to share it publicly.

One association of banks in the United Kingdom estimated the direct losses caused by malware to its member organisations[111] at GBP 12.2 M in 2004, GBP 23.2 M in 2005, and GBP 33.5 M in 2006, an increase of 90% from 2004 and 44% from 2005. It is important to note that these direct losses are not fully representative of the actual financial impact as they do not measure diminished customer trust in online transactions, loss in reputation, impact on the brand, and other indirect and opportunity costs that are challenging to quantify. Likewise, they do not include costs such as labour expenses for analysing

[108] Symantec (2007) p. 5.

[109] For the purposes of this measurement, Symantec defines "targeted attack" as an IP address that attacks at least three Symantec sensors in a given sector while excluding the other sectors during that reporting period. See Symantec (2007) p. 85.

[110] A 2004 report from the U.S. Joint Council on Information Age Crime showed that 36% or less of organizations polled reported computer-related crimes to law enforcement. See US Joint Council (2004) p. 8.

[111] Whittaker, Colin (2007) p.11.

malware, repairing, and cleansing infected machines, costs associated with the procurement of security tools (such as anti-virus and anti-malware software), or loss of productivity caused by the inability of employees to interact with a system when affected by an attack.

One recent survey of 52 information technology professionals and managers estimated a slight decline in the direct damages associated with malware[112] from EUR 12.2 billion in 2004, to EUR 10 billion in 2005, to EUR 9.3 billion in 2006.[113] This decrease is largely attributed to the suspicion that indirect or secondary losses are actually increasing.[114] Furthermore, the same survey found that most organisations tracked the frequency of malware incidents but not the financial impacts.[115] Another survey estimated the annual loss to United States businesses at USD 67.2 billion.[116]

Although the malware related costs of security measures are considered proprietary, estimates provided by market players in a recent empirical study[117] ranged from 6-10% of the capital cost of operations. No clear estimates of the effects of malware on operating expenses were available, although the study found that most organisations did experience such effects. There was evidence throughout the empirical research of concern that such effects are important, although no specific indication as to their magnitude is available.

The cost to individual consumers may be even more difficult to measure, however it is likely significant. One example is the United States where consumers paid as much USD 7.8 billion over two years to repair or replace information systems infected with viruses and spyware.[118]

While most of this data is not comparable across studies and the surveys are often limited in scope, it does illustrate the magnitude of the financial impact, for both businesses and consumers, resulting from malware.

Impacts on market players[119]

The following briefly illustrates how some key market players are confronted with malware.

[112] Computer Economics (2007), p. 5.

[113] In this case direct damages refer to labour costs to analyse, repair and cleanse infected systems, loss of user productivity, loss of revenue due to loss or degraded performance of system, and other costs directly incurred as the result of a malware attack. Direct damages do not include preventive costs of antivirus hardware or software, ongoing personnel costs for IT security staff, secondary costs of subsequent attacks enabled by the original malware attack, insurance costs, damage to the organisation's brand, or loss of market value. [Note: Issues include limited sample sizes, limited responses, inability to accurately estimate the costs of a malware incident, the difficulty in detecting malware incidents, and so on. In all cases, references should be to estimated losses.]

[114] Note: such losses were not measured in the survey.

[115] Computer Economics (2007) p. 9.

[116] United States Government Accountability Office (2007), p. 2.

[117] OECD (2007b).

[118] Brendler, Beau (2007) (Souce: StopBadware Project).

[119] OECD (2007b).

Internet Service Providers (ISPs)

Both the costs and revenues of ISPs and hence their profitability are affected directly and indirectly by malware. The most immediate cost of malware is customer support and abuse management. These costs may rise further when the ISPs are impacted by blacklists trying to fight infected machines on their network. Forms of malware that increase traffic volume, such as botnets generating massive amounts of spam, if left uncontrolled, cause opportunity costs to the ISP. The level of these opportunity costs depends on the capacity utilisation of the existing network. If the network has significant spare capacity, the opportunity costs of additional traffic to the ISP will be low. However, if the network is near capacity utilisation, the opportunity costs may be significant as incremental malware-induced traffic may crowd out other traffic in the short run and require additional investment in network facilities, in particular routers and transmission capacity, in the medium and long run. Malware may also affect an ISP indirectly via reduced revenues if its brand name or customer reputation suffers, for example, because of blacklisting and reduced connectivity. ISPs will invest in preventative measures reducing malware, such as filters for incoming traffic or technology that enable them to quarantine infected customers, only if the cost is less than the direct and indirect cost inflicted by malware.

Electronic-commerce (E-commerce) companies

E-commerce companies are impacted by malware in a variety of ways. Many have to deal with DDoS attacks, often requiring them to buy more costly services from their ISPs so as to protect the availability of their services. Furthermore, malware has been used to capture confidential customer data, such as the credit card information registered with customers' accounts with e-commerce companies. Some sophisticated forms of malware have been able to defeat the security measures of online banking sites that rely on so-called multi-factor authentication – *i.e.* on more than just user login credentials. Even if customer information does not immediately allow access to financial resources, it can be used to personalise phishing e–mails that try to trick customers into revealing financial information. There are also cases where the malware is located on the servers of e-commerce companies, which are unaware that their website hosts malicious content that is distributed to its visitors. Typically, it is the e-commerce customers themselves that are harmed, though directly or indirectly the e-commerce company may also be affected. Financial service providers often compensate damages for their customers. For other companies there can be reputation effects.

Software vendors

Software vendors are affected in direct and indirect ways. Malware uses vulnerabilities in their products to infect machines. The damage resulting from these vulnerabilities does not impact the software vendors directly, though it may have reputation effects and require costly response measures. Developing, testing and applying vulnerability patches is costly, not only on the part of the vendor, but also for its customers. Software developers typically face difficult development trade-offs between security, openness of software as a platform, user friendliness, and development costs. Investments in security may delay time to market and hence have additional opportunity cost in the form of lost first-mover advantages. On the other hand, if reputation affects work, software vendors whose products have a reputation of poor security may experience costs in the form of lost revenues. These effects are mitigated, however, by the fact that many software markets tend to have dominant firms and thus lock-in customers to specific products.

Registrars

Registrars have become part of the security ecosystem. Their business practices and policies affect the costs of malware and of the criminal business models built around it. Registrars may derive additional revenues from domain name registrations, even if they are related to malware, but they do not incur any specific direct costs. Nonetheless, if their domains are associated with malicious activity, it may result in an increasing number of formal and informal abuse notifications. Dealing with such abuse notifications is costly, requiring registrars to commit and train staff. Suspending domains may also result in legal liabilities. Furthermore, many registrars may be ill-equipped to deal with malware deregistration requests. Malware domain de-registrations can be very complex to process compared to, for example, phishing domain de-registrations, which are normally a clear breach of trademark or copyright. Some experts report that registrar abuse handling teams will often cite insufficient evidence to process a de-registration request, although evidence sufficient for many incident response teams has been provided. Because of the risk of legal action where a legitimate domain would be incorrectly de-registered, registrars often prefer to support their customer rather than the complainant.

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

End users

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

Erosion of trust and confidence

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

The nature of malware is such that it is not possible to trust the confidentiality or integrity of data submitted or accessed by any computer host compromised by malware. It is often difficult to readily distinguish a compromised host from one that is not compromised and, as a result, in an environment like the Internet, in which malware has taken hold, connections from infected hosts must be treated as potentially suspect. Therefore, the ability to have trust and confidence in online transactions can be further reduced because traditional mechanisms for building trust and confidence in the information economy such as authentication, encryption and digital certificates can also be subverted, bypassed or manipulated by malware.[120]

In recent years, a number of surveys have been conducted which show that consumers are concerned about security and privacy risks associated with providing information online or conducting transactions online. [121] The key point of these surveys is that if security and privacy concerns were better able to be addressed, then many more consumers would use e-commerce, e-banking and various e-government services than currently is the case, thus enhancing the economic benefits and efficiencies expected from the use of these platforms.

There are other studies, however, which show that the convenience and efficiency of the online channel is driving growth in participation in e-commerce and e-banking despite these concerns. In 2006, RSA Security announced the first Internet Confidence Index designed to measure changes in US and European confidence in secure online transactions among consumers and businesses.[122] At the time, the annual Index, based on data gathered from business and consumer audiences in the United States, the United Kingdom, Germany and France, revealed that the willingness to transact online was on average outpacing trust and that both businesses and consumers were absorbing the risks in order to reap the benefits of online transactions.

These two seemingly contradictory pieces of evidence point out that the role and impact of trust is not yet adequately understood and that indeed it is difficult to measure consumer trust and confidence in the online environment. However, empirical evidence reveals that e-commerce companies benefit greatly from the ability to conduct business online[123]. Given the estimated efficiency gains in the financial sector, for example, the cost savings associated with the enormous volume of transactions translates into a very powerful incentive to move as much volume of these services as possible online. Repeatedly in the study, e-commerce companies indicated that security investment levels were much higher than justified by the direct losses, often by one or two orders of magnitude.[124] Clearly direct losses are not seen as indicative of the overall problem. It would be much more devastating, for example, if online fraud eroded customer trust or slowed down the uptake of online financial services.

Risk to critical information infrastructures

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

[120] See Annex B for a more detailed discussion of how malware may subvert these security technologies and counter-measures.

[121] Australian Government, Office of the Privacy Commissioner (2004); Consumer Reports WebWatch (2005), Gartner (2005); RSA Security (2006); TriCipher (2007).

[122] RSA Security (2006).

[123] OECD (2007b) p.43; For example, two interviewees from the financial sector estimated that online transactions were in the order of 100 times cheaper than processing those transactions off line, through their branch offices, mail or phone.

[124] OECD (2007b) p. 48.

Thus, the disruption of critical information infrastructure systems through malware has the potential to impact the public and private sectors and society as a whole.

There have been a few cases where attacks using malware have directly or indirectly affected critical information infrastructure. For example, in Russia, malicious hackers used a trojan to take control of a gas pipeline run by Gazprom.[125] In January 2003 the "Slammer" worm, which caused major problems for IT systems around the world, penetrated the safety monitoring system at a US nuclear plant for nearly five hours.[126] The US Nuclear Regulatory Commission investigated the incident and found that a contractor established an unprotected computer connection to its corporate network, through which the worm successfully infected the plant's network.[127] More recently, the United States indicted James Brewer for operating a botnet of over 10,000 computers across the world, including computers located at Cook County Bureau of Health Services (CCBHS). The malware caused the infected computers to, among other things, repeatedly freeze or reboot without notice, thereby causing significant delays in the provision of medical services and access to data by CCBHS staff.[128]

Although governments are often reluctant to disclose instances of attack against the critical infrastructure, it is apparent that protecting the information systems that support the critical infrastructure has become exceedingly important.[129] Despite only a few reported cases, it is widely understood that critical information systems are vulnerable to attack. For example, although the 2003 blackout in the northeast US and Canada was attributed to a software failure, analysis of the incident demonstrated that the systems were vulnerable to electronic attack, including through the use of malware.[130]

Challenges to fighting malware

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

Many security companies report an inability to keep up with the overwhelming amounts of malware despite committing significant resources to analysis. One vendor dedicates 50 engineers to analysing new malware samples and finding ways to block them, but notes that this is almost an impossible task, with about 200 new samples per day and growing.[131] Another company reported it receives an average of 15 000 files – and as many as 70 000 – per day from their product users as well as CSIRTs and others in the security community.[132] When samples and files are received, security companies undertake a process to

[125] Denning, Dorothy (2000).

[126] Poulsen, Kevin (2003).

[127] United States Nuclear Regulatory Commission (2003).

[128] United States District Court Northern District Of Illinois Eastern Division (2007).

[129] A recent OECD Report: *The Development of Policies to Protect the Critical Information Infrastructure* highlights this point. See DSTI/ICCP/REG(2007)20/FINAL.

[130] U.S.-Canada Power System Outage Task Force Final Report p. 131.

[131] Greene, Tim (2007).

[132] OECD (2007c) pg. 7.

determine if the file is indeed malicious. This is done by gathering data from other vendors, conducting automated analysis, or by conducting manual analysis when other methods fail to determine the malicious nature of the code. One vendor estimated that each iteration of this cycle takes about 40 minutes and that they release an average of 10 updates per day.[133] Furthermore, there are many security vendors who all have different insights into the malware problem.

Most security technologies such as anti-virus or anti-spyware products are signature–based meaning they can only detect those pieces of malware for which an identifier, known as a "signature" already exists and have been deployed. There is always a time lag between when new malware is released by attackers into the "wild", when it is discovered, when anti-virus vendors develop their signatures, and when those signatures are dated onto users and organisations' information systems. Attackers actively seek to exploit this period of heightened vulnerability. It is widely accepted that signature based solutions such as anti-virus programs are largely insufficient to combat today's complex and prevalent malware. For example, one analysis[134] that explores antivirus detection rates for 17 different anti-virus vendors reveals that, on average, only about 48.16% of malware was detected. Circumstantial evidence such as this indicates that attackers are actively testing new malware creations against popular anti-virus programs to ensure they stay undetected.

In addition, malicious actors exploit the distributed and global nature of the Internet as well as the complications of law and jurisdiction bound by traditional physical boundaries to diminish the risks of being identified and prosecuted. For example, a large portion of data trapped by attackers using keyloggers is transmitted internationally to countries where laws against cybercrime are nascent, non-existent or not easily enforceable. Although countries across the globe have recognised the seriousness of cybercrime and many have taken legislative action to help reprimand criminals, not all have legal frameworks that support the prosecution of cyber criminals.[135] The problem however is even more complicated as information may be compromised in one country by a criminal acting from another country through servers located in a third country, all together further complicating the problem.

Law enforcement agencies throughout the world have made efforts to prosecute cyber criminals. For example, the Computer Crime and Intellectual Property Section of the US Department of Justice has reported the prosecution of 118 computer crime cases from 1998 – 2006.[136] Although global statistics on arrests are hard to determine, one company estimated worldwide arrests at 100 in 2004, several hundred in 2005 and then 100 again in 2006.[137] While these cases did not necessarily involve malware, they help illustrate the activities of the law enforcement community. It is important to note that the individuals prosecuted are usually responsible for multiple attacks. These figures are low considering the prevalence of online incidents and crime. They highlight the complex challenges faced by law enforcement in investigating cybercrime.

Furthermore, the volatile nature of electronic evidence and the frequent lack of logged information can often mean that evidence is destroyed by the time law enforcement officers can get the necessary warrants to recover equipment. The bureaucracy of law enforcement provides good checks and balances,

[133] OECD (2007c) pg. 7.

[134] Information provided to the OECD by CERT.br, the national CSIRT for Brazil.

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

[136] United States Department of Justice Computer Crime & Intellectual Property Section.

[137] Green, Tim(2007a).

but is often too slow to cope with the speed of electronic crime. Additionally, incident responders often do not understand the needs of law enforcement and accidently destroy electronic evidence.

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

MALWARE: WHAT TO DO?

Many would agree that the damage caused by malware is significant and needs to be reduced although its economic and social impacts may be hard to quantify. That said, several factors should be considered in assessing what action to take, and by whom, against malware. These include: the roles and responsibilities of the various participants,[138] the incentives under which they operate as market players as well as the activities already undertaken by those communities more specifically involved in fighting malware.

Roles of individual, business and government participants - Highlights

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

Among the various participants, those concerned by malware are:

- Users (home users, small and medium–sized enterprises (SMEs), public and private sector organisations) whose data and information systems are potential targets and who have different levels of competence to protect them.

- Software vendors,who have a role in developing trustworthy, reliable, safe and secure software.

- Anti-virus vendors, who have a role in providing security solutions to users (such as updating anti-virus software with the latest information on malware).

- Internet Service Providers (ISPs), who have a role in managing the networks to which the aforementioned groups connect for access to the Internet;.

- Domain name registrars and regulators, who determine if a domain is allowed to be registered and potentially have the power to deregister a domain that is used to commit fraud or other criminal activity, including, for example, the distribution of malware.

- CSIRTs, frequently the national or leading ones (often government), which have a role, for example, in detecting, responding to and recovering from security incidents and issuing security bulletins about the latest computer network threats or vulnerabilities associated with malware

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

attacks; or in co–ordinating nationally and internationally the resolution of computer network attacks affecting its constituency or emanating from its constituency.

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

Incentives and disincentives - Highlights[139]

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

Very limited information as to how individual actors actually make their information security decisions is available in the public domain, which makes it difficult to calibrate any form of public policy. Economic decisions with regard to information security depend on the particular incentives[140] perceived by each market player. These incentives are rooted in economic, legal, and other mechanisms, including the specific economic conditions of the market, the interdependence with other players, formal legal rules as well as informal norms. Ideally, the relevant incentives should assure that private costs and benefits of security decisions match the social costs and benefits. Any policy strategy to combat malware therefore needs to take into account the existing incentive mechanisms and examine whether they could potentially be modified to produce more efficient outcomes at the societal level.

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

[139] OECD (2007b).

[140] Incentives are often classified in monetary (remunerative, financial) and non-monetary (non-financial, moral) factors. Financial incentives include factors such as tying the salary of an employee to corporate performance, the ability to make a super-normal profit by pursuing a risky innovation, or the bottom line effects of potential damage to a firm’s reputation. Non-financial incentives encompass norms and values, typically shared with peers, and result in a common understanding as to the right course of action or the set of possible actions that should be avoided in a particular situation. Financial incentives typically connect degrees of achievement of an objective with monetary payments. Non-financial incentives work through self-esteem (or guilt) and community recognition (or condemnation).

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

Externalities related to malware

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

Assessing the direct and indirect economic cost of malware and exploring countermeasures is an important issue. As the provision of security entails cost, tolerating a certain level of insecurity is economically rational. The resulting level of security is dependent on the costs and benefits of security. Relevant questions that need to be addressed include: are market players taking the full range of costs into account when making security decisions? What costs are externalised to other market players or society at large? Findings[141] regarding incentives and externalities across the value net of the different market players confronted with malware reveal three situations: no externalities, externalities that are borne by agents in the value net that can manage them, and externalities that are borne by agents who cannot manage them or by society at large.

No externalities

This concerns instances in which a decision-making unit, be it an individual user or an organisation, correctly assesses security risks, bears all the costs of protecting against security threats (including those associated with these risks) and adopts appropriate counter measures. Private and social costs and benefits of security decisions are aligned. This situation would be economically efficient but, due to the high degree of interdependency in the Internet, it is rare. Measures undertaken or neglected on one stage of the value net will typically affect the whole system. That does not mean these situations are non-existent. In principle, end users – be they large organisations or skilled home users – who use stringent security policies and successfully prevent their machines from being compromised generate no negative externalities for the rest of the value net. It is not unreasonable to assume that there are cases where malware is successfully fought off.

Externalities that are borne by agents in the value net that can manage them

This concerns instances in which an individual unit correctly assesses the security risks but, due to the existence of (positive or negative) externalities, the resulting decision deviates from the social optimum. Such deviations may be based on lack of incentives to take costs imposed on others into account, but can also result from a lack of skills to cope with security risks, or financial constraints faced by an individual or organisation. As long as somebody in the value net internalizes these costs and this agent is in a position to influence these costs – *i.e.* it can influence the security tradeoffs of the agents generating the externality – then the security level achieved by the whole value net may not be too far from the optimum. This scenario depicts a relatively frequent case and numerous examples in the empirical study were found that confirm externalities were being internalised by other market players.

[141] OECD (2007b) p.49.

Externalities that are borne by agents who cannot manage them or by society at large

An individual unit correctly assesses the security risks given its perceived incentives but, due to the existence of externalities, this decision deviates from the social optimum. Unlike the previous scenario, no other agents in the information and communication value net absorb the cost or, if they do, they are not in a position to influence these costs – *i.e.*, influence the security tradeoffs of the agents generating the externality. Hence, costs are generated for the whole sector and society at large. These are the costs of illegal and criminal activity associated with malware, the costs of restitution of victims, the cost of law enforcement associated with these activities, and so forth. Furthermore, they may take on the more indirect form of slower growth of e–commerce and other activities. Slower growth may entail a significant opportunity cost for society at large if the delayed activities would have contributed to economic efficiency gains and accelerated growth. A comprehensive assessment of these additional costs will demand a concerted effort but will be necessary to determine the optimal level of action to fight it.

Overall incentive structures for market players

A research project[142] conducted to better understand current incentive structures and possible externalities shows that the overall response to malware emerges from the interaction of the market players and the degree of compatibility (or incompatibility) of their respective incentive structures. It seems that the incentives of many of the commercial stakeholders are reasonably aligned with minimizing the effects of externalities on the sector as a whole. The incentives vary in strength and in some cases they are fairly weak. However, the study shows that the market players studied experience at least some consequences of their security tradeoffs on others. In other words, feedback loops bring some of the costs imposed on others back to the agent that caused them – even if in some cases the force of the feedback loop has so far been too weak or too localised to bring their behaviour in line with the social optimum.

For some players an important mechanism to achieve this approximate result is the interdependence between them. In other instances it is reputation effects that align incentives with the socially optimal choice. Both effects may operate independently or jointly, as in the case of ISPs. For instance, a user with insufficient malware protection may cause an externality whose cost is, in part, borne by the service provider, in part by other ISPs, and in part by society at large (*e.g*, costs of law enforcement, overall reduced trust in e-commerce). An ISP may incur costs to enable its network to isolate single users that might spread malware due to insufficient protection of that user’s machine. Part of this externality is thus internalised by the ISP because of the incentives of the provider to protect the integrity of its services and to avoid blacklisting and the negative effects this might entail for its operating costs, its reputation and consequently its revenues and growth prospects.

Among other findings, the research also shows that whereas some external effects are internalised at the level of the whole information economy ecosystem, there are some effects that need to be considered as externalities to society at large. For example, malware and its effects may tarnish the reputation of industries that rely heavily on electronic transactions, such as banking or insurance. If electronic platforms are used less frequently than would otherwise be the case, then the forgone efficiency improvements can be considered an externality cost to society of malware. Moreover, malware may diminish trust in the working and security of e-commerce overall. Again, if this results in slower diffusion and growth, one could consider the unrealised potential efficiency gains as a cost to society. Such potential gains could occur at the sector level but they could also manifest themselves in lower overall economic growth rates. There is

[142] OECD (2007b) – The research conducted in-depth interviews in five countries with representatives of market players including Internet Service Providers (ISPs), e-commerce companies including online financial services, software vendors, hardware vendors, registrars and end users – complemented by interviews with regulators, CSIRTs, ICANN, security services providers and researchers.

evidence throughout the study of concern that such effects are important, although no specific indication as to their magnitude is available.

Security problems and the related economic costs to society may have two roots: *i*) they are the outcome of relentless attacks on the information and communication infrastructure by criminals, and *ii*) given an overall external threat level, they may be aggravated by discrepancies between private and social costs and benefits which are the outcome of decentralized decision-making in a highly interrelated ecosystem. Both actors in the criminal world and within the information and communications system respond to the economic incentives they face. For the market players assessed in the empirical study mentioned above, a mixed incentive structure exists which includes positive incentives as well as disincentives to take action against malware.

What is already being done - Highlights

Better understanding of the nature, successes and limitations of ongoing action by communities more specifically involved in fighting malware is also important to assessing how to enhance prevention of and response to malware. Substantial efforts by various participants have been made within OECD countries and APEC economies and at the international level to, *inter alia,* raise awareness, measure malware, develop or amend legal frameworks, strengthen law enforcement, and improve response.[143] For example:

- Many websites and resources exist to help end users and SMEs secure their information systems.
- Many entities track, measure and sometimes even publish data on their experience with malware and related threats.[144] Furthermore, schemas [145] exist to provide single, common identifiers to new virus threats and to the most prevalent virus threats in the wild to reduce public confusion during malware incidents.
- Several informal networks have been created that are a key element of the response community's ability to respond to incidents resulting from malware. CERT/CC has catalogued 38 national CSIRT teams, 19 of which are in OECD countries, and 16 of which are in APEC economies.[146] In addition, they hold annual meetings for national CSIRT teams to gather and share information about numerous issues, including malware.
- Numerous countries across the world have legal provisions against hacking, spam, data interference, and system interference. Furthermore, the Convention of the Council of Europe on cybercrime is the first and only legally binding multilateral treaty addressing the problems posed by the spread of criminal activity online and 43 countries across the globe are now party to the Convention.

[143] For a detailed breakdown of specific efforts, see Annex C.

[144] See Annex A – Data on Malware.

[145] One example of such a scheme is the Common Malware Enumeration (CME), the last notification of which was published on January 19, 2007 (see http://cme.mitre.org/data/list.html - it is difficult to know whether the delay in assigning CME references is a result of political problems with the project, a lack of co-operation from vendors, or attacks becoming more targeted and therefore falling outside the original scope of malware that CME addresses). Some experts consider that tracking malware consistently across the industry is as large a problem as it was several years ago or even greater today due to the significant increases in the number of in-the-wild samples. Therefore, the problem of common malware identifiers is an issue that could still need to be addressed practically.

[146] CERT Coordination Center (2006).

- Law enforcement agencies and organisations across the world have made important efforts to find malicious actors and bring them to justice for the crimes they commit. The law enforcement community has created points of contact networks and other similar schema to help cross-border co-operation in recognition that the majority of these crimes cross legal and jurisdictional boundaries. Law enforcement agencies and business typically use tools which implement the Whois protocol to query database servers operated by the domain name registrars and Regional Internet Registries for data on domain name owners, Internet Protocol address and Autonomous System Number allocations that can identify the asserted physical locations where unlawful activity is taking place, and the relevant service providers (ISPs), which, in turn, can provide information regarding their customers.
- ISPs are operating in highly competitive markets and are taking proactive steps in the fight against malware, such as quarantining infected machines.
- Software vendors have increased efforts to improve the security of their software. The deployment of vulnerability patches has improved. Arguably more important, many software vendors put software development processes in place that are increasingly aware of and focusing on security issues.
- Governments across OECD countries and APEC economies are taking policy, legislative and technical measures to address malware [147]. In particular, they are working, in co-operation with the private sector, to protect their government critical information infrastructure from electronic attack.

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

Possible next steps

This report has only begun to lay the foundation for understanding the malware phenomenon and how it is evolving. Further work in many areas could and should be done to reach a better understanding. Fighting malware is complex and would benefit from more comprehensive measurement, co–ordination and policy solutions. While many ongoing initiatives[148] are contributing important resources to combating malware, there remain a number of areas for improvement.

A global partnership against malware

The need for a consistent approach to a global problem is not new but malware presents particular complexities due to the wide variety of actors with responsibility for combating malware. The communities involved in fighting malware, whether governments, businesses, users, or the technical community, need to improve their understanding of the challenges each of them faces and co-operate – within their

[147] See Annex C.

[148] Ibid.

communities and across communities – to address the problem. Furthermore, their co-operation must occur at the global level. It is not enough for one country or one community to effectively self organise if others do not do so as well.

In light of the need for a holistic and comprehensive approach to malware, a common point of departure from which to build co-operation and collective action could be to launch at the international level a global "Anti-Malware Partnership" involving government, the private sector, the technical community, and civil society. Such collaboration across the various communities involved with fighting malware could benefit from the experience gained from developing the OECD's Anti-Spam Toolkit. Different international public and private organisations including the OECD and APEC could partner and lead the work in their area of competence. They could then produce joined-up policy guidance to fight malware on all fronts (proactive prevention strategies, co-operation for response, legal frameworks/law enforcement, technical measures, economic aspects, measurement of malware, global co-operation). Specifically, the "Anti-Malware Partnership" could examine the following elements[149]:

Proactive prevention strategies

This element could examine all or part of the following:

- Reduction of software vulnerabilities (*e.g.* secure software development could be encouraged; governments could maximize their influence as buyers of software by requiring more secure software products as part of their procurement process).
- Awareness raising and education (*e.g.* further efforts should be made to improve online users awareness of the risks related to malware and of the measures they should take to enhance the security of their information systems).
- The possibility to include security and abuse management in registrar accreditation procedures and contracts.
- Standards and guidelines (*e.g.* update of security manuals such as the IETF Security Handbook RFCs should be encouraged to include new challenges such as those presented by malware).
- R&D (*e.g.* malware detection and analysis, security usability - how people interact with machines, software and online resources).

Co-operation for response

This element could examine, *inter alia*, the following:

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

[149] See Annex F for preliminary suggestions on these topics.

Legal frameworks/Law enforcement

This element could examine, *inter alia,* the following:

- Government efforts to provide mutual assistance and share information for the successful attribution and prosecution of cybercriminals.
- Co-operation between CSIRT teams and law enforcement entities.
- Resources necessary for specialised cybercrime law enforcement agencies to be able to investigate and prosecute cybercrime in co-operation with other concerned public and private stakeholders.

Technical measures

This element could examine, *inter alia*, the following:

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

The economics of malware

This element could examine, *inter alia*, the following:

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

Measuring the malware problem

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

Global co-operation

This element could examine the following:

- The cross-cutting need for information sharing, co–ordination and cross-border co-operation.
- Suggestions for disseminating the anti-malware guidance at the global level and following up on its implementation.

Only a holistic approach involving an integrated mix of policy, operational procedure and technical defences can ensure that information sharing, co–ordination and cross–border co-operation are effectively integrated and addressed. The success of such a global "Anti-Malware Partnership" would require active engagement from all participants. Such an effort, however, would demonstrate significant advances in the international community's ability to overcome obstacles to addressing a global threat like malware through global co–ordinated action.

CONCLUSION

There is no simple solution to the complex problems presented by malware. The openness of the online environment and the distributed nature of the Internet while important factors for growth and innovation, also present challenges for securing information systems and networks. Malware has the potential to adversely affect any and all Internet users from enterprises to governments to end users. While malware often propagates through the Internet, it is important to remember that it is software which can be introduced into Internet connected and non-Internet connected computer systems. Malware whether used directly, or indirectly, to conduct malicious activity online erodes trust and confidence in the Internet and the digital economy.

The 2002 *OECD Guidelines for the Security of Information Systems and Networks* provide a list of broad information security principles all of which are relevant and applicable to the fight against malware. The nine principles (Awareness, Responsibility, Response, Ethics, Democracy, Risk assessment, Security design and implementation, Security management, Reassessment) concern participants at all levels, including at the policy and operational levels. *The Guidelines* can and should be applied to the challenges raised by malware today.

The rapidly evolving nature of malware makes international co-operation essential to addressing the problem. This co-operation should be supported and enhanced by accurate and quantitative measurement of the problem and the underlying economics at play. While this paper details many of the problems presented by malware, it is only a first step in moving towards a solution. A holistic and multi-stakeholder proactive approach is needed to take advantage of all opportunities for improvement across the various communities addressing malware.

ANNEX A - DATA ON MALWARE

Overview

Although malware as we know it today is a relatively new phenomenon compared to the early days of worms and viruses, it is growing and evolving at impressive rates. Trends in data show that while the categories of malware used to conduct malicious activity (*i.e.* virus verses trojan) change and evolve over time, the use of malware is steadily increasing.

Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs), software and anti-virus vendors, and more generally security companies are examples of entities that track and monitor the existence of malware. While the data provided below is helpful in understanding elements of the malware problem, it is not easily comparable in real and absolute terms and thus this paper does not attempt to make comparisons or draw conclusions across disparate sets of data. This section is primarily intended to demonstrate the type of information available and different analytical perspectives from the organisations listed below.

Data provided by CSIRTS

AusCERT

AusCERT is the national Computer Emergency Response Team for Australia. AusCERT provides computer incident prevention, response and mitigation strategies for members.

In Figure 1, each incident represents a single unique URL or domain name that is hosted by one or more compromised computers for the purpose of stealing sensitive information and access credentials from other computers. Multiple incidents can be associated with one attack, which is the set of compromised computers needed to launch the attack and collect the stolen data. The number of IP addresses associated in a single incident and a single attack is variable but can range from 1 to around 100.

Figure 1

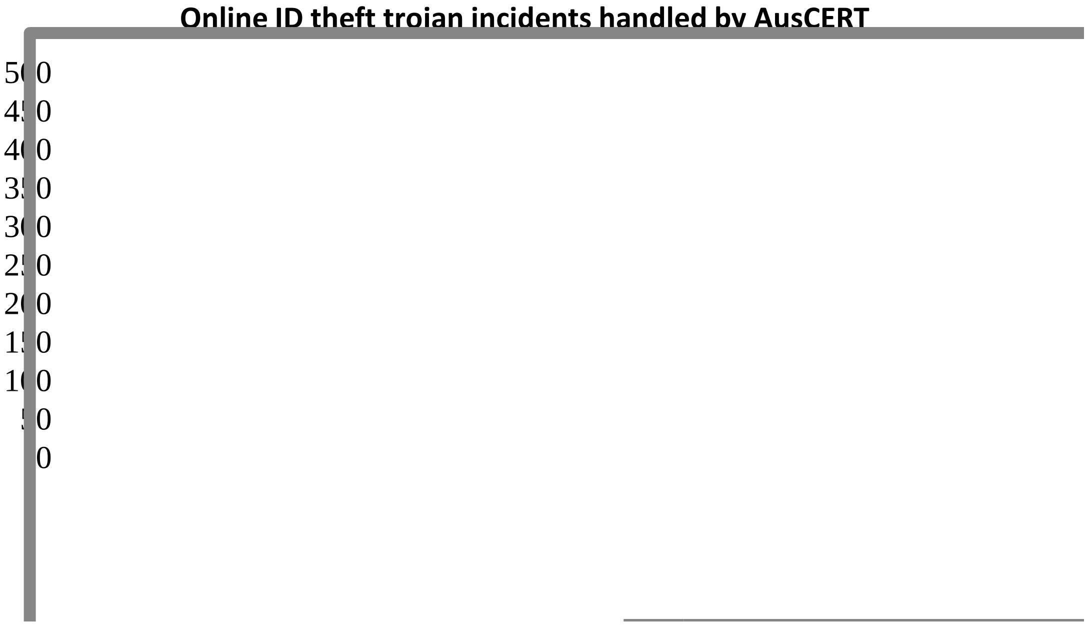


Figure 1 does not include specific compromised hosts involved in any single attack or incident - only URLs and domain names. Nor does this depict the number of computer infections (compromised hosts) that occur due to each attack of which there are generally many hundreds or thousands.

The high figures for July 2007 are due to the storm trojan (often incorrectly referred to as a worm). It does not automatically propagate and has P2P botnet C&C functionality, *inter alia*.

CERT Brazil (CERT.BR)

CERT.br is a national CERT which collects public statistics on the incidents that are reported to them voluntarily. For example, a home user can report when he/she received an e–mail that is clearly a fraud attempt, with a link to a malware executable. CERT.br tests to see if the executable is still on–line and then reports the occurrence to the host of the site. They also submit a sample of this malware to several antivirus vendors to ensure that it has been widely detected.

CERT.br data is divided into four categories: intrusions, web attacks, denial of service, and fraud.

Table 1. CERT.BR Incident Reports

Year	Total number of incidents reported	Worm[150]	DoS	Intrusion[151]	Fraud[152]
2004	75 722	42 268	104	248	4 015
2005	68 000	17 332	96	448	27 292
2006	197 892	109 676	277	523	41 776

CERT/CC, United States

The Computer Emergency Response Team Coordination Centre (CERT/CC) at Carnegie Mellon University collects data on malware from public and private sources. Since 2006, CERT/CC has been collecting, analysing and cataloguing every piece of malware it is able to find that has been distributed via the Internet or which otherwise has found itself onto computer systems. While many malware artefacts have similar functionality, each one is considered to be a unique variant if it generates a unique MD5 or SHA1 hash function.[153] Therefore, some types of self-propagating malware such as viruses and worms which produce many thousands of identical replicas would be counted as a single variant.[154]

Hence the figures below from CERT/CC, while not necessarily complete, are nonetheless significant in their depiction of malware trends, which show an exponential increase in malware artefacts[155] from January 2006 to March 2007. From less than 50 000 in January 2006, the total number of artifacts rose to 350 000 in March 2007, as represented in Figure 2 below. For each month of the same period, Figure 3

[150] The worm category are reports received of worm/bot propagation, *e.g.* port scans of commons ports used by worms/bots to propagate (445, 135, 5900, etc). These reports are usually sent by firewall administrators and even home user using personal firewalls, etc. It is important to note that the worm category does not try to count machines infected by worms, but incidents regarding worm propagation attempts.

[151] Intrusion, according to CERT.BR classification, is a system compromise – this is determined by the system owner/administrator and reported to CERT.BR. For example, a Linux server administrator sends CERT.BR a report saying his/her machine was compromised, a rootkit was found, etc.

[152] The fraud category refer to various fraud types: copyright infringements, credit card fraud, traditional phishing and malware related fraud. The last one is the majority of the cases in Brazil.

[153] Attackers often generate a new malware variant from an existing piece of malware by simply changing the manner in which the code is ‘compressed and packed’, rather than changing the malware code itself. For example, see: http://us.trendmicro.com/us/threats/enterprise/glossary/c/compression/index.php. New variants produced in this manner are not each given a new CME number. Multiple variants, which are considered to be identical in functionality and form will have the same CME number, whereas even small variations in malware byte code will produce a new CME number. See: http://cme.mitre.org/cme/process.html

[154] This approach is important as counting each infection from a single large worm or virus outbreak can skew the results and does not reflect the actual level of development of new variants by many attackers specifically in order to evade detection by anti-virus products.

[155] An artifact is a file or collection of files which may be used by adversaries in the course of attacks involving networked computer systems, the Internet, and related technologies.

represents the proportion of those artifacts that were newly discovered by CERT/CC. Although the increase is less steady in Figure 3, the discovery of new artefacts reached an all time high in March 2007 up to 90 000.

Figure 2 –Total Artifact by month from January 2006 to March 2007

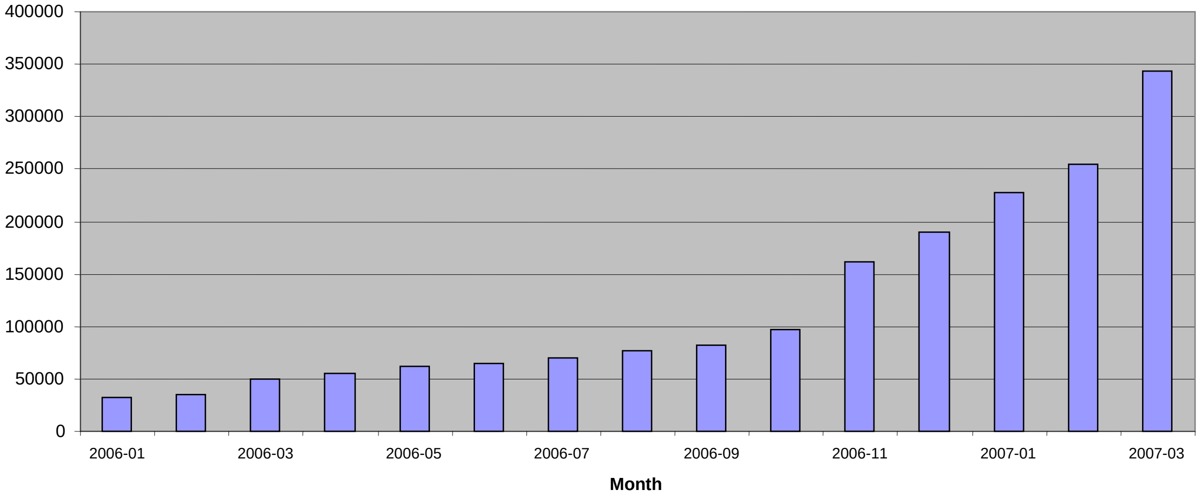
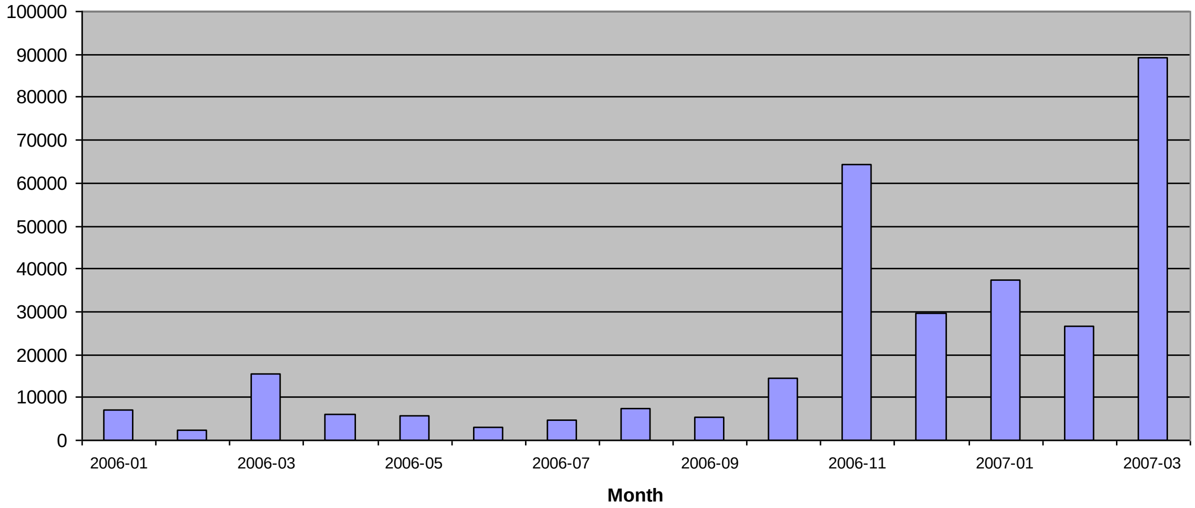


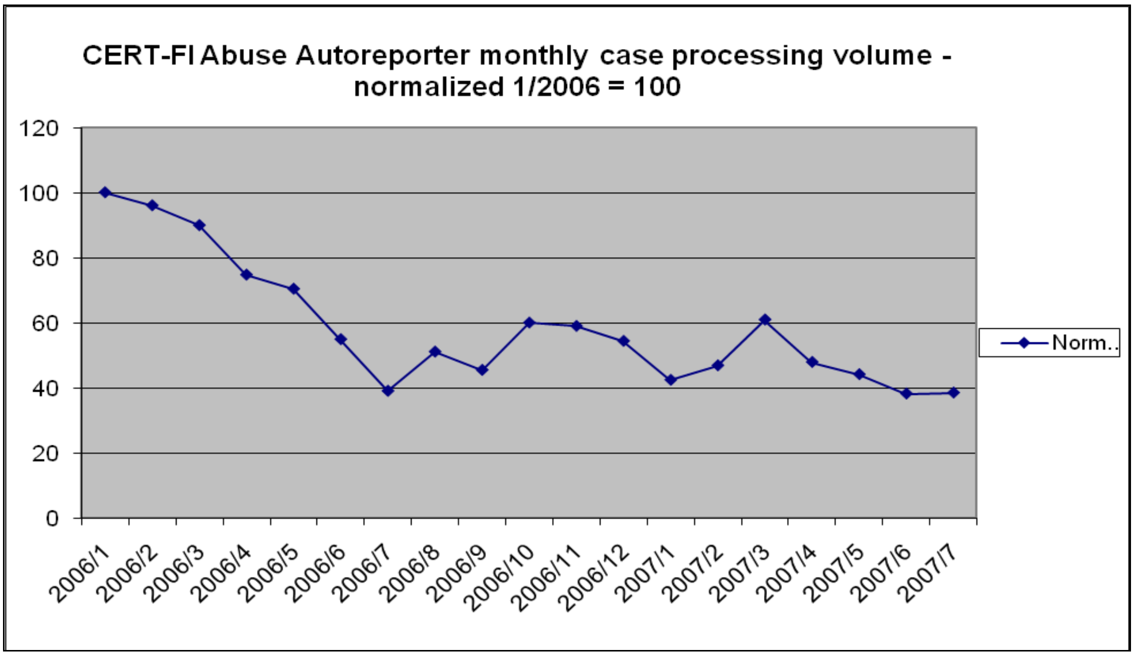
Figure 3 – New artifacts per month from January 2006 to March 2007



CERT-FI, Finland

CERT-FI is the Finnish national Computer Emergency Response Team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. Figure 4 represents the cases handled by CERT-FI Abuse Autoreporter system, their automated abuse case processor. The graph is cases / month, normalised to 100 = 1/2006.

Figure 4



KrCERT/CC

KrCERT/CC gathers data from honeynets[156] and incidents reports. Between 2005 and 2006 data from both incident reports and honeypots showed a decrease in the number of worms and an increase in the number of trojan horses from 2005 – 2006 (see Figures 5 and 6).

[156] In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated, (un)protected and monitored, and which seems to contain information or a resource that would be of value to attackers. Two or more honeypots on a network form a honeynet.

Figure 5: Incident Reporting to KrCERT/CC by Month (2005-2006)

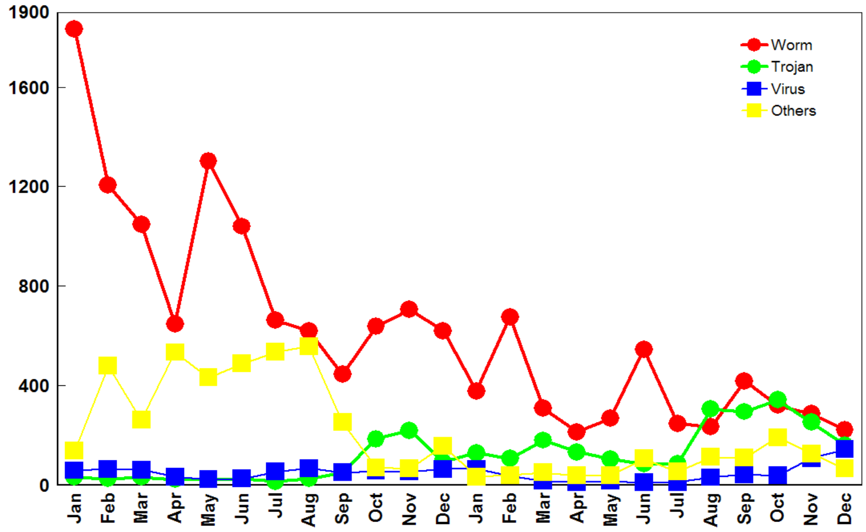
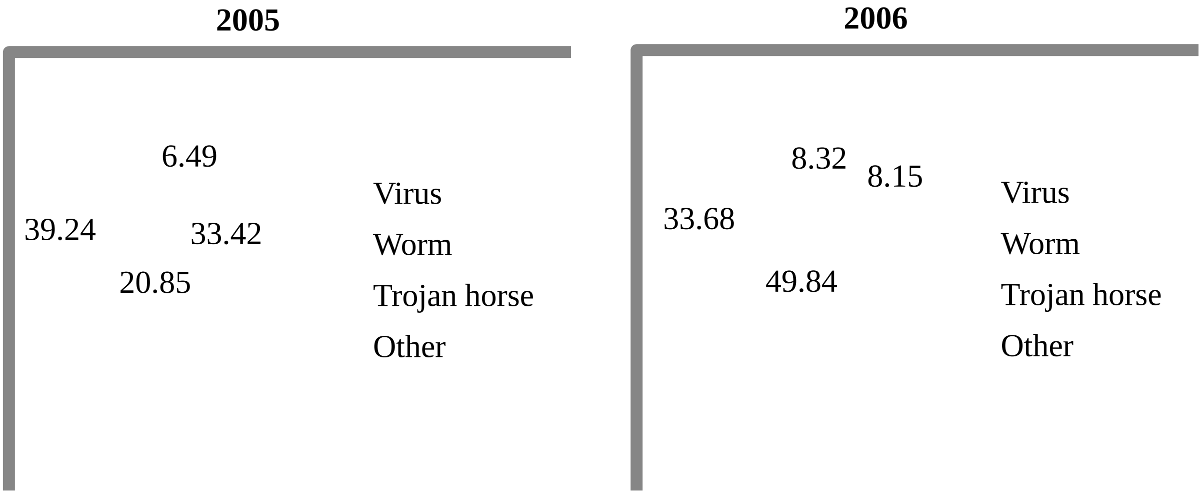


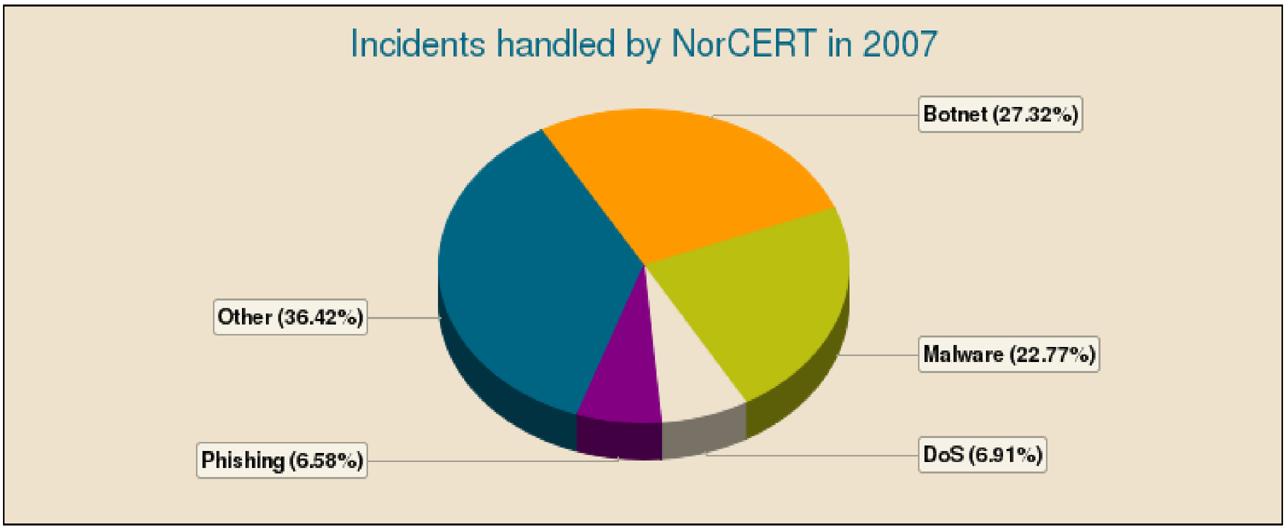
Figure 6: Information gathered from KrCERTr honeynets



NorCERT, Norway

The Norwegian Computer Emergency Response Team (NorCERT) co–ordinates preventative work and responses against IT security breaches aimed at vital infrastructure in Norway. NorCERT is a department of the Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet - NSM).

Figure 7



United States Computer Emergency Readiness Team (US-CERT)

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

Figure 8 displays the overall distribution of cyber security incidents as reported to US-CERT across the six major categories. US-CERT utilises the reporting categories outlined in the National Institute for Standards and Technology (NIST) Special Publication 800-61.[157] The number of incidents involving malware (malicious code) has significantly increased from 2006 to 2007.

[157] United States Computer Emergency Response Team (US-CERT).

Figure 8: US-CERT Incident Reporting Trends for January 2006 – August 2007

Overall distribution of cybersecurity incidents and events across the six major categories Year 2006 to Year 2007 (through 31 August)

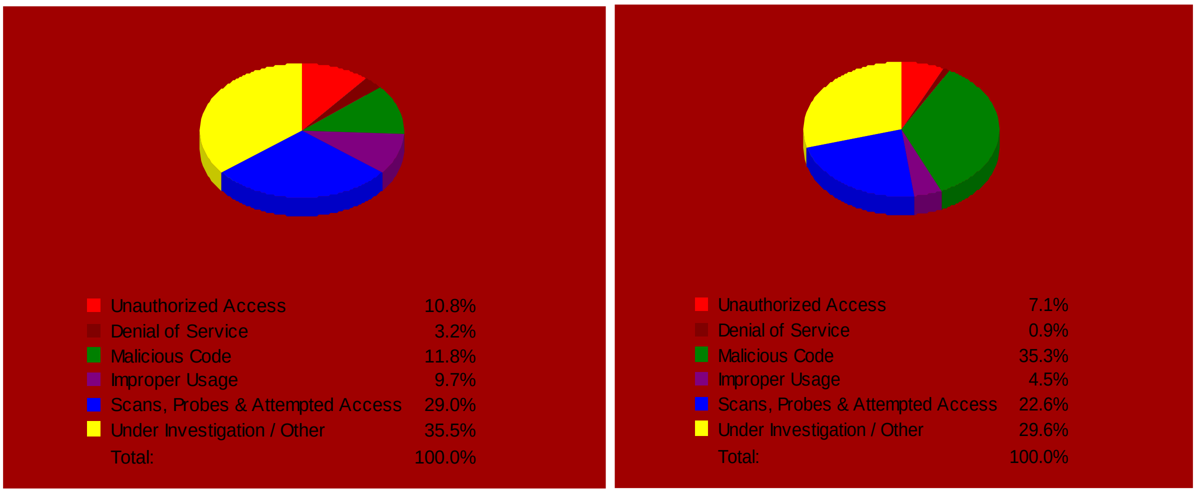
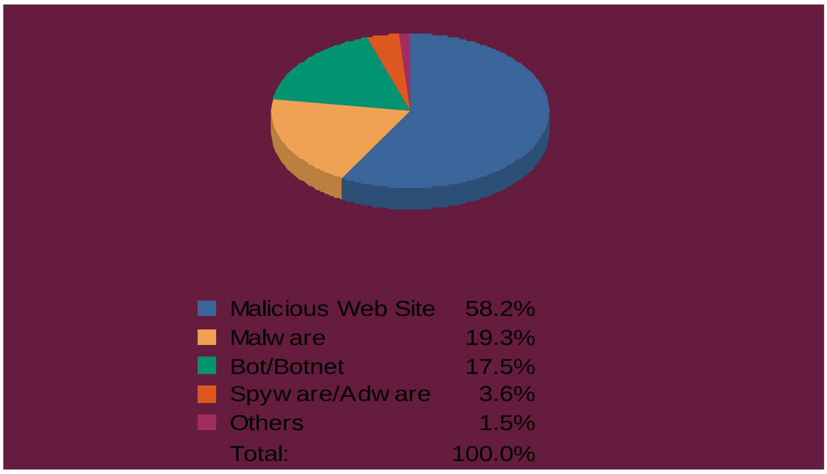


Figure 9 depicts the top five malware sub-categories being reported to US-CERT. The category labelled as "Malware" includes trojans, worms and viruses. The graph shows "Malicious websites" as the most commonly reported sub-category.

Figure 9: Top 5 Malware - 2007

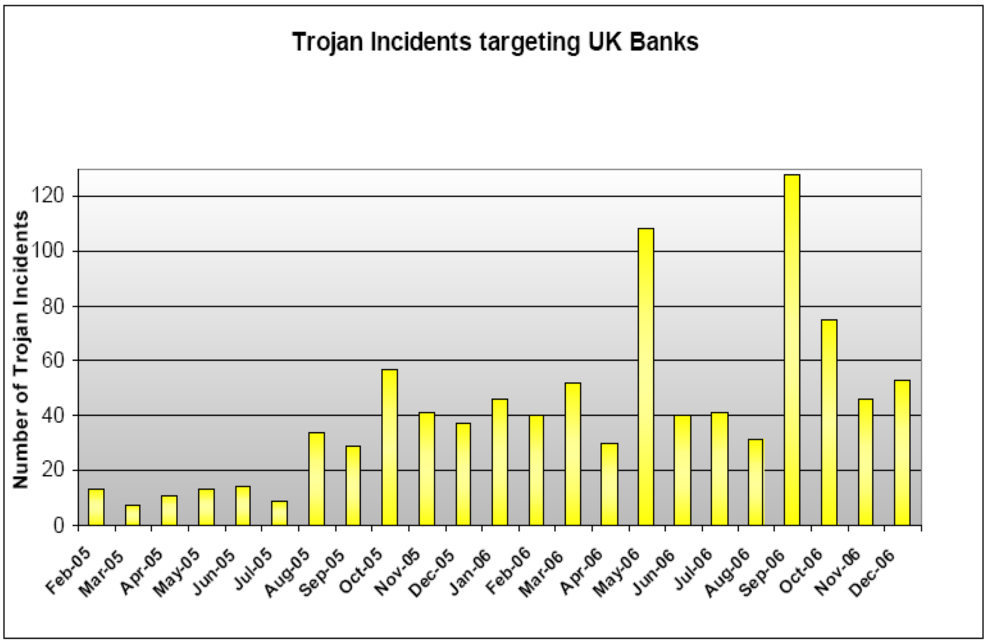


Data from software and anti-virus vendors

Association of payment

APACS, the UK payments association, is a trade association for institutions delivering payments services to end customers. It enables the forum to address co-operative aspects of payments and their development. It is also the main industry voice on issues such as plastic cards, card fraud, cheques, e-banking security, electronic payments and cash. Working Groups address co-operative areas such as developing authentication solutions and responding to attacks on e-banking customers. Figure 10 tracks the number of trojan incidents targeting UK banks from February 2005 – December 2006.

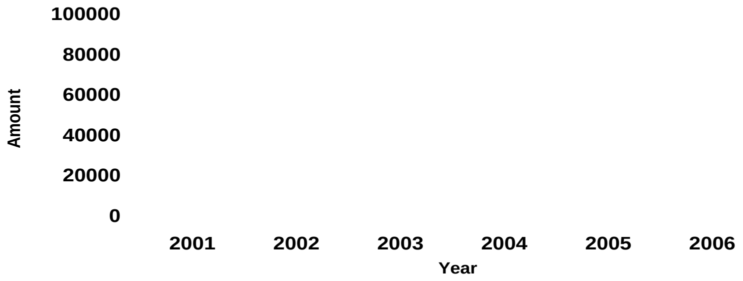
Figure 10



Kaspersky Lab

Kaspersky Lab is an international information security software vendor. Kaspersky Lab is headquartered in Moscow. Kaspersky labs reported an exponential increase in previously unknown malicious programmes from 2001 – 2006, as illustrated in Figure 11. They also reported a steady increase in the number of trojan spy programmes designed to steal information from users' online accounts.[158]

Figure 11: Increase in the number of new malicious programmes*[159]*



[158] Kaspersky Labs (2006).

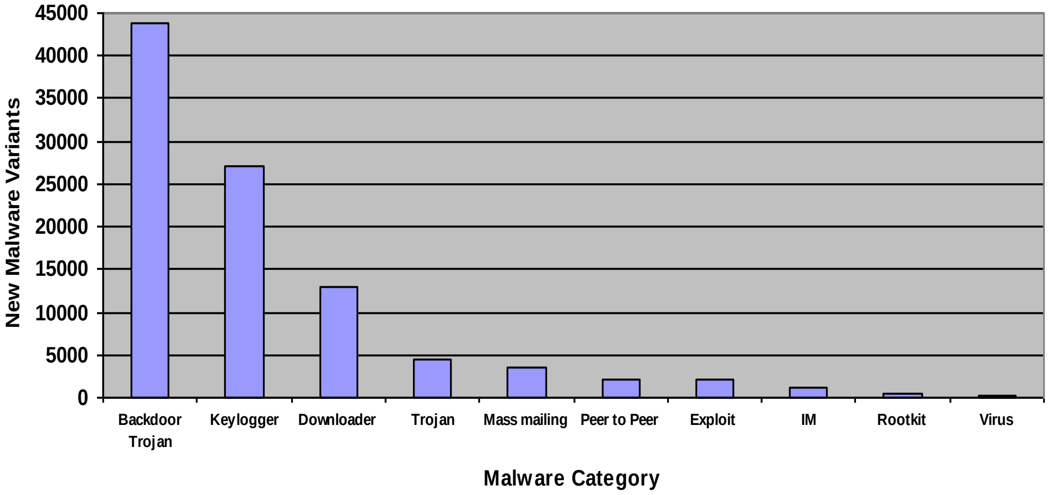
[159] Mashevsky, Yury (2007).

Microsoft

Microsoft gathers data from several anti-malware products and services deployed on information systems running Microsoft products.[160] Based on activity observed from January to June 2006, Microsoft reported the existence of more than 43 000 new malware variants between January and June of 2006.[161] This can at least partially be attributed to the public availability of malware for purchase on the Internet; it is easier for attackers to modify a piece of existing malicious code rather than create a new "family" of malicious code.

Microsoft also reported that among new malware variants backdoor Trojans accounted for the highest number (see Figure 12). The figures demonstrate that the four most common categories where new variants have been created were of the non-self-propagating varieties, which are typically associated with smaller scale cyber attacks aimed at illicit financial gain, particularly financial fraud.

Figure 12: - Microsoft Malicious Software Activity from January – June 2006[162]



SOPHOS

SOPHOS gathers data from 35 million users in 150 countries that deploy its products. SOPHOS attributed 80% of all detected malware in 2006 to trojans (see Figure 13). [163]

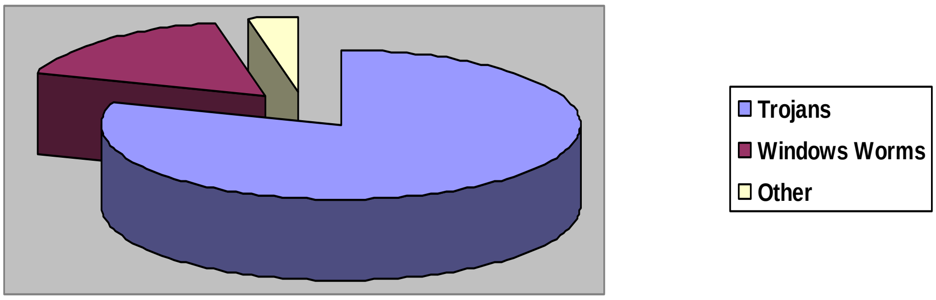
[160] Microsoft (2006a) p. 1.

[161] Microsoft (2006a) p. 1.

[162] Microsoft (2006a) p. 6.

[163] Supra Sophos (2007a) p. 5.

Figure 13: Trojans verses Windows Worms and Viruses in 2006

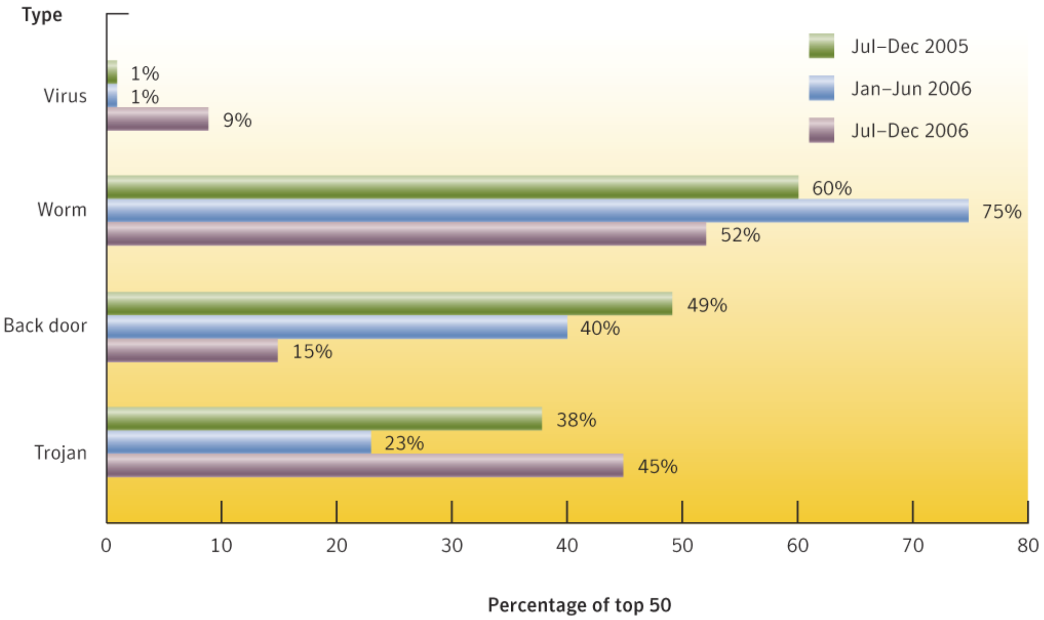


Symantec

Symantec gathers information from 40 000 registered sensors in 180 countries, 120 million desktop computers, and gateway and server antivirus installations, and 2 000 000 decoy accounts in the Symantec Probe Network. Symantec operations are conducted from four security operations centers and eight research centers. Symantec software products are deployed on more than 370 million computers or e–mail accounts worldwide.

Recently, Symantec reported a decrease in the amount of worms[164] and backdoors and an increase in the amount of viruses and Trojans (see Figure 14).

Figure 14 - Malicious code types by volume[165]



[164] This drop can largely be attributed to the decline in reports of major worms such as Sober.X, Blackmal.E, and Netsky.P75 since the first half of 2006.

[165] Symantec (2007) p. 55.

In addition to this data, the Symantec Corporation reported an increase in previously unseen malware, or new families. Between July and December 2006, Symantec honeypots discovered 136 previously unseen malware families, an increase of 98 from the previous6 months.[166] It is important to note that while information gathered from honeypots and honeynets is useful, it is not necessarily representative of a global trend.

Observations on the data

The data on malware presented above comes from a variety of very different and incomparable sources (national CSIRTs, software vendors, and security vendors). The definitions, types of incidents, type of damage, time frame, and scope are not harmonised across these various organisations and therefore it is necessary to be prudent in comparing such disparate data.

However, it is more or less possible to highlight certain tendencies that seem to be shared: *i*) an significant and noticeable rise in security incidents related to malware ; and, *ii*) trojan malware becoming more and more prevalent when looking across types of malware. As has often been reported, there are fewer serious outbreaks of worms and viruses and thus a large part of the increase in malware variants can generally be attributed to non-propagating varieties which usually have a more harmful payload/functionality and tend to be financially motivated.

An agreement by certain stakeholders interested in measuring malware on definitions and common methodology for gathering data would help in more systematically evaluating the extent of this reality and its role in the ever changing universe of the Internet and ICTs.

From some of the data, it is possible to summarise and highlight several points to demonstrate that the problem of malware is becoming more and more significant.

Box 8. Summary of sample data on malware

Table 1: Total number of incidents reported ~ + 225%

Figure 2 Total artefacts in the last year ~ +250%

Figure 6 Decline of Worms related incidents ~ -25%/; Increase of trojan related incidents: ~ + 30%

Figure 11 Malicious programmes increase by 800% in the last 5 years

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

[166] Symantec (2007) p. 54.

ANNEX B - FURTHER DETAIL ON TYPES OF MALWARE ATTACKS

Attacks on the DNS

Just like other systems, servers that host DNS can be vulnerable to attacks using malware. For example, malicious actors may try to overwhelm DNS servers by launching a DDoS attack. If part of the DNS goes down or is taken off–line it usually results in websites becoming unreachable and e–mail becoming unavailable. Threats to the DNS infrastructure include: *i)* loss of service; *ii)* hijacking; and, *iii)* loss of coherence [167] While there is significant work underway to secure the infrastructure, it is a costly undertaking to fully address the problem.

Attacks against the DNS are not new and they can be launched against high value targets such as the DNS root servers. For example, in 2002 a large scale attack was launched against the DNS root servers however the system as a whole continued to function despite the degraded or impaired performance of individual root servers. More recently, on 5 February, 2007 several key DNS root servers experienced significant increases in traffic, causing 2 of the 13, which were not anycasted[168], to succumb to the attack. Despite the immense capacity and seemingly co–ordinated nature of the attack, the DNS system proved resilient. Although both attacks against the root servers were largely unsuccessful, it is widely recognised that the continuation of attacks of this nature could harm the functioning of the DNS system and critical backbone of the Internet.

Attacks using the DNS

There has also been a recent series of DNS attacks utilising “recursive resolvers”. Although these attacks use recursive resolvers as their force-multiplier, they need not be directed at DNS targets at all, although that’s where they do the most damage. They can just as easily use the DNS to conduct DDoS attacks against other targets. This type of attack uses the DNS as a weapon against something else, whereas the attacks against the DNS root servers, described above, use something else as a weapon against the DNS. These attacks are often possible due to poor configuration of an organisation’s DNS server which allows it to service DNS requests from anywhere on the Internet – not just from its own network. Recursive DNS attacks are indirectly related to malware only in so far as they use a small number of compromised information systems to send fake DNS requests. Unlike other forms of DDoS attack it does not depend on a large number of bots to work or be more effective. It is important to note that the purpose of recursive or amplification attack is not to deny service to the DNS system itself, but rather to a single organisation’s DNS server. This has the impact of making the IP routing unresolved to the entity’s domain name and making outbound DNS requests for the organisation difficult because of the consumption of resources of the organisation’s DNS server. Although malware is not always directly involved, it is also an example of how a user or entity’s configuration can have a negative impact on others’ security.

[167] Twomey, Paul p. 8-9.

[168] Anycast is a network addressing and routing scheme whereby data is routed to the "nearest" or "best" destination as viewed by the routing topology.

Another trend in which malware may be implicated but not directly involved is the practice of domain name tasting. Domain name tasting is a practice employed by registrants to use the add-grace period[169] to register domain names in order to test their profitability. During this period, registrants conduct a cost-benefit analysis to determine if the tested domain names return enough traffic to offset the registration fee paid to the registry over the course of the registration period. Domain name tasting allows registrants to exploit the add-grace period. When a domain name generates unsatisfactory profitability, it is returned before the fifth day for a full refund. Originally, the add-grace period was created to allow registrants to receive a refund in the case of mistake or grant registrars a refund in the event a registrant's credit card was declined. The process has been exploited to permit the registration of domain names in bulk. Although difficult to prove, it is likely that these "tasted" domains are used to distribute malware.

Box 9. A closer look at DNS[170]

The Domain Name System (DNS) is like an address book for the Internet. It helps users to navigate, send and receive information over the Internet. Every computer connected to the Internet uses a unique address which is a string of numbers called an "IP address" (IP stands for "Internet Protocol").[171] Because IP addresses are difficult to remember, the DNS makes using the Internet easier by allowing a familiar string of letters (called the "domain name") to be used instead of the numeric IP address. For example, instead of typing 193.51.65.37, users can type www.oecd.org. It is a "mnemonic" device that makes the addresses for computer hosts easier to remember.

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

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

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

Attacks that modify data

By its very nature, when malware infects or compromises a computer system, it involves an attack on the integrity of the information system in two fundamental ways. First, the steps involved in compromising the system result in unauthorised changes to the system itself and potentially any data stored, input or accessed via that system, including user input (keyboard or mouse), output (screen or printer), and storage (USB, hard disk or memory). Second, once a system is compromised, the integrity (*i.e.* trustworthiness) of the entire system can no longer be relied upon. Attacks on integrity are generally a

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

[170] Information available at http://www.icann.org/general/glossary.htm.

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

precursor to other attacks, such as the theft of sensitive data, or can be a feature of an attack on authentication. However, attacks on integrity may be an end goal. For example, modifying entries in a database to facilitate fraud or deleting a company's customer database for commercial sabotage or modifying settings on a SCADA system used for gas distribution may be designed to lead to a harmful malfunction of that system.[172]

Another currently popular attack that modifies data is compromising a website and inserting an Iframe[173] which infects regular visitors to that site. Iframes can be inserted into legimitate websites to link to malware hosting sites that can then compromise the user.

Attacks on identity

There are substantial differences between statistical information gathered on ID theft by public authorities for policy purposes and by private businesses for commercial purposes. Some sources conclude that the scale of ID theft has gone down in the past years, resulting in growing consumer confidence. In contrast, other sources advance figures reflecting an increase in ID theft. Furthermore, some financial institutions, which say that the costs are relatively modest, are not willing to reveal their own financial losses. On the other hand, other private bodies advance figures reflecting an increase in ID theft. To further complicate the landscape, some financial institutions even claim that none of their customers has ever been affected by a phishing attack.[174] Below is some data to illustrate the debate around ID theft:

- In 2006, the Netcraft toolbar, an anti-phishing tool developed by the Netcraft toolbar Community,[175] blocked more than 609 000 confirmed phishing URLs, a substantive jump from 41 000 only in 2005.[176] Netcraft views this dramatic surge, mainly concentrated in November – December 2006, as the result of recent techniques implemented by phishers to automate and propagate networks of spoof pages, enabling the rapid deployment of entire networks of phishing sites on cracked web servers.[177]

- In 2006, The Anti-Phishing Working Group reported an increase in cyber attacks from July to November 2006.[178] In November 2006, 37 439 new phishing sites were detected, a 90% increase since September 2006. However, in its December 2006 report the APWG notes a decrease in the number of new phishing sites (which dropped to 28 531).[179]

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

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

[174] Devillard, Arnaud (2006).

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

[176] Netcraft Toolbar Community (2007).

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

[178] APWG, 2006a p. 1.

[179] APWG, 2006b p. 1.

- The US Federal Trade Commission reported in 2003 that ID theft affected approximately 10 million Americans each year.[180] In 2007, another report found that ID fraud had fallen about 12% from USD 55.7 billion to 49.3 billion.[181]
- However, the Javelin report was criticised and regarded as trying to persuade the opinion that "business are doing an adequate job in protecting consumers' personal information and that the onus in on consumers to better protect themselves."[182] A recent McAfee survey noted this discrepancy, considering Javelin's percentages as "surprisingly low" and comparing them to Gartner statistics, which, in contrast, in 2007, counted 15 million of Americans as victims of ID theft.[183]

Attacks on single and multi-factor authentication

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

Attacks on some forms of multi-factor authentication are also possible and have occurred. For example, most simple forms of multi-factor authentication, including the use of a hardware token which generates a one time password and challenge-response with a short time to live are vulnerable to malware attack. For example, a trojan, once installed on the user's computer simply waits for the user to establish a legitimate login session with their bank using their multi-factor credentials. Then the trojan conducts a funds transfer in the background without the user's authorisation or knowledge. To the financial institution, the funds appear to have been transferred and authorised by the account user. [184]

The feasibility of this type of malware attack has been demonstrated as recently as May 2007[185] and as early as 2005. For example, a trojan was able to compromise the E-gold payment[186] system by waiting for the victim to successfully authenticate to E-gold's website, then creating a hidden browser session, and using various spoofing tricks to empty the victim's account. Because the stealing and spoofing started after the authentication is completed, it circumvented any authentication that was put in place. While the e-gold trojan did not attack multi-factor authentication *per se*, it was an early example of malware able to transfer funds in the background after the user legitimately logs on to their e-gold account which could have defeated any type of multi-factor logon authentication that did not also implement transaction signing.[187]

[180] US FTC, 2003, p. 4 (Note: this includes all types of ID Theft, online and offline).

[181] Javelin Research and Strategy p. 1.

[182] Shin, Anneys (2007) .

[183] McAfee (2007) p. 11.

[184] F-Secure (2007b).

[185] Dearne, Karen (2007).

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

[187] Stewart, Joe (2004).

Box 10. The two-factor token attack

A slight variation of the two-factor token attack involving a hybrid phishing and malware attack, reportedly targeted ABN AMRO's online banking customers recently. The attacker sent potential victims an e–mail purporting to be from their bank (*i.e.* ABN AMRO). If recipients opened an attachment to the e–mail, malware was installed on their computers without their knowledge. When the customers next visited their banking site, the malware redirected them to the attacker-controlled website that requested their security details, (*i.e.* their PIN) and one-time password (OTP) generated by the hardware token. As soon as the attackers received these details they were able to log into the customer's account at the real ABN Amro site, before the expiry of the automatically generated number enabling them to transfer the customer's money.[188] As single-factor authentication for high value transactions are replaced by multi-factor authentication, this type of attack will become more commonplace.

Attacks on digital certificates and secure socket layer (SSL)

Digital certificates and Secure Socket Layer (SSL) connections are often used to protect the confidentiality and integrity of data sent over the Internet and to verify the authenticity of the remote host (most commonly to authenticate a remote server). While these protections are useful, they do not provide security at the end points of a transaction but generally only the channel in between. While an SSL session is established, data needs to be encrypted and decrypted as data is transferred back and forth between the end points. When a users' machine has been compromised by malware,[189] the data being sent can be captured *before* encryption occurs – and for data received – *after* it has been decrypted. Efforts to provide a higher level of assurance for some types of digital certificates will not address this problem.

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

- Errors and warnings due to invalid SSL certificates are frequently highly technical in nature and therefore confusing to users.
- According to one usability study performed, consumers most often ignore the absence of an SSL connection before entering personal data, or ignore warnings provided.[190]
- When organisations use self-signed certificates, "untrusted signer" warnings may be displayed and generate confusion for users.
- In some cases, malicious site operators have been able to obtain legitimate SSL[191] certificates from Certificate Authorities.[192]

[188] Outlaw.com and The Registar.

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

[190] Dhamija, Rachna (2007).

[191] Krebs, Brian (2006).

[192] A certificate authority is an entity, such as Verisign, that issues certificates.

Box 11. A closer look at digital certificates and SSL

A digital certificate[193] is a mechanism to establish the credentials of a person or entity conducting business or transactions online. It is often used within SSL[194] protected sessions. The use of digital certificates within SSL protected sessions is a means of building trust and confidence in e-commerce and e-government transactions. However, some form of malware when installed on a user's computer can wait for a legitimate SSL session to be established with a particular website, for example a specific online banking site and inject HTML code into the browser interface before the remote web site page renders on the user's computer. This has the effect of changing the content and appearance of the web page to the user (even though the remote site has not been modified), while the user's computer still maintains a valid SSL connection with the remote host. A check of the SSL digital certificate, by the user, will show that it is a valid certificate for the remote host. What the user sees on their screen and the data the user is prompted to input differs from the legitimate remote site. By manipulating the compromised computer's browser interface attackers make it virtually impossible for users to know whether or not they should trust they have a secure connection with a particular remote host – and by inference – whether what they see in the browser window is content served by the legitimate remote host. Therefore, the use of digital certificates within SSL protected sessions as a means of reliably verifying the identity of a remote web domain has been fundamentally undermined.[195]

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

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

[195] More recent versions of the Haxdoor trojan also have the ability to use HTML injection. See AusCERT (2006).

ANNEX C - SAMPLE INSTRUMENTS, STRUCTURES AND INITIATIVES FOR ADDRESSING MALWARE

This section provides an illustrative example rather than a comprehensive list of instruments, structures and initiatives at the national and international levels that exist to help address malware.

Awareness raising

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

Australia - E-Security National Agenda (ESNA)

The Australian Government established the ESNA in 2001 to create a secure and trusted electronic operating environment for both the public and private sectors. A review of the ENSA in 2006 found that the online environment is highly interconnected and that e-security threats to different segments of the Australian economy can no longer be addressed in isolation. In this context, the Australian Government announced AUS$73.6 million over four years for new measures to strengthen the electronic operating environment for business, home users and government agencies.[196] In addition, the Australian government is undertaking the following initiatives:

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

The Australian Government has also developed a number of booklets to encourage Australian consumers and small businesses to protect themselves against e-security threats.[197]

[196] The revised ESNA can be found at: http://www.dcita.gov.au/communications_for_consumers/security/e-security.

[197] Information available at:http://www.dcita.gov.au/communications_and_technology/publications_and_reports.

Australia Netalert[198]

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

Australia Stay Smart Online website

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

EU Safer Internet Plus Programme[199]

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

Get Safe Online[200]

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

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

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

[198] Information available at www.netalert.gov.au.

[199] Information available at http://ec.europa.eu/information_society/activities/sip/index_en.htm.

[200] Information available at http://www.getsafeonline.org/.

New Zealand Netsafe[201]

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

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

United Kingdom ITsafe[202]

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

United States Onguard Online[203]

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

United States StaySafeOnline[204]

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

Untied States – National Awareness Week

The United States Government in collaboration with industry holds an annual National Cyber Security Awareness Month (NCSAM). The month aims to raise awareness about online security and how to adopt

[201] NetSafe at www.netsafe.org.nz is an initiative of the Internet Safety Group (ISG).

[202] Information available at: www.itsafe.gov.uk

[203] Information available at: http://onguardonline.gov/index.html

[204] Information available at: http://www.staysafeonline.org

safe online practices. The activities and events held in the month focus on home Internet users, SMEs, government, education and the corporate sector.

Teenangels[205]

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

Conventions

Council of Europe Convention on Cybercrime

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

This instrument, which cites OECD actions as a means to further advance international understanding and co-operation in combating cybercrime, aims to "pursue … a common criminal policy for the protection of society against cybercrime by adopting appropriate legislation and fostering international co-operation." To achieve these goals, the signatories commit to establish certain substantive offences in their laws which apply to computer crime. Although malware is not *per se* mentioned in the Convention among the illegal activities that signatories must criminalise, it is indirectly covered under closely related listed crimes including illegal access to information systems, computer data, and computer-related fraud.[206]

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

To date, the Convention has been ratified by 21countries and signed by 22 additional countries.[207] Some companies in the private sector have taken some initiatives to help ensure a larger impact of the Convention's principles.[208]

Detection and response

Many countries have a watch, warning and incident response function in the form of a CSIRTs or CERT. It is important to recognise that not all CSIRTs and CERTs are alike. Some are public entities

[205] Information available at: http://www.teenangels.org/index.html.

[206] Council of Europe (2001) Articles 2, 3, 8.

[207] Council of Europe.

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

residing in the government structure, some are publicly and privately funded entities with multiple mandates and still others are associated with academic institutions.[209] It is widely accepted good practice that governments develop or appoint a CSIRT or CERT with national responsibility.[210]

In some cases, entities within a country are required to report information security incidents to a central government authority competent to handle them. In some cases this entity is a CSIRT/CERT. For example, in Finland it is obligatory that significant violations of information security, faults and disturbances in public telecommunications be reported to the national CSIRT of Finland, CERT-FI.[211] One example of a "significant violation" is considered activation of malware in telecommunication service providers' own systems". In order to fulfill this regulation for external incident reporting, the telecommunications service provider must have adequate internal processes for detection and reporting of as well as recovery from information security incidents and threats. This model has been successful in Finland because the government has proven to the reporting parties to be trustworthy and capable of handling sensitive information and they actively meet with major carriers in one-on-one sessions to share information.

In the United States, all civilian government agencies are required to report information security incidents to US-CERT.[212] In both Finland and the United States a standard incident report form is provided.

International initiatives

Forum of Incident Response Security Teams (FIRST)

FIRST brings together a variety of computer security incident response teams (CSIRTs) from government, commercial, and educational organisations in 37 countries. FIRST aims to foster co-operation and co–ordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.[213] Membership in FIRST enables incident response teams to reach counterparts in other countries that can help them to more effectively respond to security incidents.

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

[210] In 2006, CERT/CC began hosting an annual meeting of CSIRTs with national responsibility; information available at: http://www.cert.org/csirts/national/conference2007.html. They also keep a list of CSIRTs with national responsibility at: http://www.cert.org/csirts/national/contact.html

[211] Finnish Communications and Regulatory Authority (FICORA) 9 B/2004 M; available on line at: http://www.ficora.fi/attachments/englanti/1156489108198/Files/CurrentFile/FICORA09B2004M.pdf.

[212] Federal Information Security and Management Act (FISMA); http://www.pearlsw.com/resources/Experts/OMBRequirements.pdf.

[213] Available online at: http://www.first.org.

Regional CSIRT Activity

Asia Pacific CERT (APCERT)[214]

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

Caribbean Telecommunication Union

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

The European Government CERT Group (EGC)

The EGC[215] group is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe. To achieve this goal, the EGC members jointly develop measures to deal with large-scale or regional network security incidents, facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities, share knowledge and expertise, identify areas of collaborative research and development on subjects of mutual interest, and encourage formation of government CSIRTs in European countries

Gulf Coordination Council CERT (GCC CERT)

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

[214] APCERT website: http://www.apcert.org/about/structure/members.htm

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

Task Force CSIRT (TF CSIRT)[216]

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

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

Enforcement

Domestic structures

Under EU legislation the provisions detailed on page 85 may be enforced by administrative bodies and/or criminal law authorities. Where this is the case, the Commission has stressed that at national level the responsibilities of different authorities and co-operation procedures need to be clearly spelled out. To date, the increasingly entwined criminal and administrative aspects of spam and other threats have not been reflected in a corresponding growth of co-operation procedures in Member States that brings together the technical and investigative skills of different agencies. Co-operation protocols are needed to cover such areas as exchange of information and intelligence, contact details, assistance, and transfer of cases.

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

International mechanisms

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

The Contact Network of Spam Authorities (CNSA[217])

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

[216] Information available at: http://www.terena.org/activities/tf-csirt/

[217] Information available at: http://stopspamalliance.org/?page_id=11

procedure to facilitate cross-border handling of spam complaints and is working on the issue of spyware and malware.

G8 24/7 Cybercrime Network

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

Interpol

Interpol[218] is an international police organisation with a mission to prevent or combat international crime. Interpol has decentralised its cybercrime expert teams around the world through the establishment of regional Working Parties on Information Technology Crime for Europe, Latin America, Asia, South Pacific, and Africa.[219] Interpol’s European Working Party on Information Technology Crime (EWPITC) has for example compiled a best practice guide for experienced investigators from law enforcement agencies.[220] It has also set up a rapid information exchange system under an international 24-hour response scheme, listing responsible experts within more than 100 countries. This scheme was notably endorsed by the G8 24/7 HTCN.

London Action Plan (LAP)[221]

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

International Consumer Protection Enforcement Network (ICPEN)

The International Consumer Protection and Enforcement Network (ICPEN) is a network of governmental organisations involved in the enforcement of fair trade practice laws and other consumer protection activities. ICPEN was founded in 1992 by 20 countries and in co-operation with the OECD and the EU; the network now has 29 participant countries. A Memorandum on the Establishment and Operation of ICPEN governs this network. The primary objective of the ICPEN is to facilitate practical action and information exchange among its members to prevent and redress deceptive marketing practices

[218] Interpol includes 186 member countries. Information available at: www.interpol.int/public/icpo/default.asp.

[219] Information available at: www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa.

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

[221] Information available at: http://www.londonactionplan.com.

across international borders. To accomplish this, the ICPEN fosters co-operative efforts to address the problems consumers face in conducting cross-border transactions for goods and services. ICPEN co-operation does not include the regulation of financial services and product safety and it does not provide a platform for the procurement of specific redress for individual consumers.

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

Legislation

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

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

- Sending unsolicited communications (spam).[222]

- Unlawful access to terminal equipment; either to store information – such as adware and spyware programs- or to access information stored on that equipment.[223]

- Infecting terminal equipment by inserting malware such as worms and viruses and turning PCs into botnets or usage for other purposes.[224]

- Misleading users into giving away sensitive information such as passwords and credit card details by so–called phishing messages.[225] Some of these practices also fall under criminal law, including the Framework Decision on attacks against information systems.[226] According to the latter, Member States have to provide for a maximum penalty of at least three years imprisonment, or five years if committed by organised crime.

Some additional recent examples of legal developments include:

- The UK Police and Justice Bill 2006.[227] This law, among other provisions, updated the Computer Misuse Act 1990 (CMA) to prohibit the preventing or hindering access to a programme or data held on a computer, or impairing the operation of any programme or data held on a computer. The law also increased the maximum penalty for such cybercrimes from five to ten years and refined the definition of computer abuse to cover denial of service attacks.

[222] Official Journal of the European Communities (2002).

[223] Official Journal of the European Communities (2002) Article. 5 (3).

[224] Ibid.

[225] Official Journal of the European Communities (1995) Article 6 (a).

[226] Official Journal of the European Communities (2005).

[227] Introduced into UK law in November 2006.

- Germany's August 2007 anti-hacking law, making hacking[228], denial-of-service, and computer sabotage attacks on individuals[229] illegal. The provisions extend criminal liability to the intentional "preparation of criminal offences" by producing, distributing, procuring etc. of devices or data designed for such purposes. Offenders could face sentences of up to ten years in prison for major offenses.

- The United States Congress is considering legislation that would create a law that would establish that the use of spyware to collect personal information or to commit a federal criminal offense is a federal crime. If passed by and signed into law, it would authorise the appropriation of USD 40 million for the prosecution of violations of the new law from 2008 to 2011.[230] In addition, the US FTC has actively pursued spyware companies using its authority under Section 5 of the FTC Act. The FTC has brought eleven law enforcement actions during the past two years against spyware distributors. These actions have reaffirmed three key principles. First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures about software and its effects are not adequate, just as they have never been adequate in traditional areas of commerce. And third, if a distributor puts an unwanted program on a consumer's computer, he or she must be able to uninstall or disable it.

Public-private structures

Domestic initiatives

Australia - Internet Security Initiative[231]

The Australian Internet security initiative, administered by the Australian Communications Media Authority, provides information free of charge to Internet service providers about 'zombie' computers operating on their networks. The program operates by forwarding information on bot–infected computers to Australian ISPs.[232] These ISPS then contact their customers to assist them to 'disinfect' their computer.

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

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

[229] Existing law already limits sabotage to businesses and public authorities.

[230] Congressional Budget Office Cost Summary p.1.

[231] Information available at: http://www.acma.gov.au/WEB/STANDARD//pc=PC_100882.

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

United States

One example of public-private-partnership in the US is in critical infrastructure protection, under the National Infrastructure Protection Plan (NIPP) managed by the US Department of Homeland Security. The framework under the NIPP includes a government entity ("Government Coordinating Council", GCC) made up of government agencies and industry entities ("Sector Coordinating Council", SCC) in each of the determined critical infrastructure sectors, including the Information Technology and Communications sectors. The NIPP is a framework for assessing and managing the risk to each of the sectors, including threat, vulnerabilities, and consequences.[233]

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

Finally, the US National Cyber-Forensics and Training Alliance, is a joint partnership between law enforcement, academia, and industry that collaborates on cybercrime issues. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations.[234]

International initiatives

Council of Europe/Microsoft

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

Anti Phishing Working Group

The Anti-Phishing Working Group (APWG) is a volunteer–run consortium of industry and law enforcement focused on eliminating the results from phishing, pharming[235] and e–mail spoofing of all types. The APWG has over 2 600 members including 1 600 companies and agencies as well as national and provincial law enforcement. It provides a forum to examine phishing issues, define the scope of the phishing problem in terms of costs, and share information and best practices for eliminating the problem.[236] The APWG website provides a public resource for reporting phishing attacks. When phishing is reported, the APWG analyses the information provided and adds it to its online phishing archive. The APWG also works to share information about phishing attacks with law enforcement when appropriate. In addition to phishing, the APWG tracks phishing-based trojans, keyloggers and other malware.

[233] The NIPP is available at: http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

[234] Information available at: http://www.ncfta.net/default2.asp.

[235] Pharming" (or "warkitting") uses similar techniques as a classic phishing attack, but in addition redirects users from an authentic website (from a bank for instance) to a fraudulent site that replicates the original in appearance. When a user connects its computer to, for instance, a bank web server, a hostname lookup is performed to translate the bank's domain name (such as "bank.com") into an IP address containing a series of numbers (such as 193.51.65.37). It is during that process that malicious actors will interfere and change the IP address. See Scoping Paper on Online Identity Theft, OECD Committee on Consumer Policy, DSTI/CP(2007)3/FINAL.

[236] Information available at http://www.antiphishing.org/index.html.

Messaging Anti-Abuse Working Group[237]

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

Microsoft's Botnet Task Force

Through its international Botnet Task Force, first held in 2004, Microsoft provides training to law enforcement officials from around the world who have been confronted with the task of investigating Botnet abuses. [238]

PhishTank

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

Anti-Spyware Coalition (ASC)

The ASC is a group composed of anti-spyware software companies, academics, and consumer groups which focuses on the development of standard definitions in relation to spyware. On 25 January 2007, ASC published working documents on best practices[239] aimed to detail the process by which anti-spyware companies identify software applications as spyware or other potentially unwanted technologies.

Private sector partnerships

One example of private sector partnerships in the United States is the creation and continued development of the Information Technology Information Sharing and Analysis Center (IT-ISAC). The IT-ISAC is a trusted community of security specialists from companies across the Information Technology industry dedicated to protecting the Information Technology infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to quickly and properly address them.[240]

Standards and guidelines

Institute of Electrical and Electronics Engineers (IEEE)[241]

The IEEE is a non-profit organisation for the advancement of technology. Through its global membership, the IEEE is a leading authority on areas ranging from aerospace systems, computers and

[237] Information available at: www.maawg.org.

[238] Charney, Scott (2005).

[239] Information available at: www.antispywarecoalition.org/documents/BestPractices.htm.

[240] Information available at: http://www.it-isac.org.

[241] Information available at: www.ieee.org.

telecommunications to biomedical engineering, electric power and consumer electronics among others. Members rely on the IEEE as a source of technical and professional information, resources and services. The IEEE is a leading developer of standards for telecommunications and information technology.

International Standards Organisation (ISO)

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

Some relevant ISO/IEC standards include the following:

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

In June 2007, the ISO and IEC joint technical committee (JTC) 1 subcommittee (SC) 27 proposed a new work Item on “Guidelines for cybersecurity (27032)”.[242] This standard would provide comprehensive guidelines on cybersecurity[243] to both service providers and users (organisations and end users) and, in particular address behavioural, organisational and procedural issues. More specifically, it would offer ‘best practice’ guidance in achieving and maintaining security in the cyber environment for audiences in a number of areas, and address the requirement for a high level of co-operation, information-sharing and joint action in tackling the technical issues involved in cybersecurity. This needs to be achieved both between individuals and organizations at a national level and internationally.

National Institute of Standards and Technology

Founded in 1901, NIST is a non-regulatory federal agency within the US Department of Commerce. NIST's mission is to promote US. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. In November 2005, NIST published the *Guide to Malware Incident Prevention and Handling* as NIST Special Publication (SP) 800-83.[244]

World Wide Web Consortium

The World Wide Web Consortium (W3C)[245] is an international consortium where member organisations, a full-time staff, and the public work together to develop web standards. W3C's mission is

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

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

[244] Information available at : http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

[245] Information available at: www.w3c.org.

"To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web."

Technical solutions and resources

Sample domestic initiatives

Japan - Cyber Clean Center (CCC)

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

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

Korea – Automated Security Update Programme (ASUP)

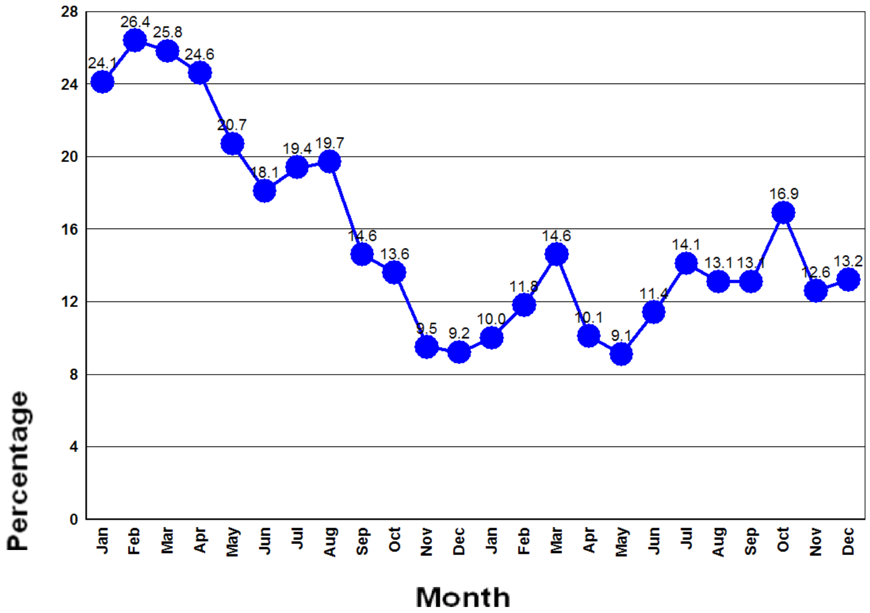
To reduce the damage from vulnerabilities in Microsoft Windows, Korea Internet Security Center (KrCERT/CC) and Microsoft Korea collaborated to develop and deploy the Automated Security Update Programme (ASUP) to home and SME users. The programme seeks to make all Internet connected information systems install Windows security related patches without user intervention once they have installed ASUP. When users visit major Korean websites, such as portals, online game sites, a popup window appears in the screen to confirm the installation of the ASUP. While offering the same functionality as Windows automatic updates, ASUP allows users to just click once to approve ASUP installation without having to modify the configuration of Windows updates.[246] Microsoft Korea has distributed the programme in accordance with Microsoft headquarters centralised patch policy, balancing user convenience and company's philosophy on security.

Sinkhole System

The sinkhole system works to prevent bots from connecting to botnet command and control (C&C) servers by subverting the IP address of the botnet C&C server. When a bot-infected zombie makes a query to a DNS server, the answer to the query (IP address for the botnet C&C server) will be the address of the Sinkhole System. The connection attempt is then redirected to a sinkhole system in KrCERT/CC, rather than to the C&C server. The sinkhole system can track and analyze all activities of connected botnets. As shown in Figure 15, after the adoption of this sinkhole system in 2005, the botnet infection rate of Korea has reportedly dropped to almost one third at the end of 2005, compared with that of January or February 2005.

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

Figure 15: Botnet Infection Rate of Korea (2005 ~ 2006)



MC Finder

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

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

Domain Name System Security (DNSSEC)

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

Domain level authentication

Domain-level authentication is a means to enable a receiving mail server to verify that an e–mail message actually came from the sender's purported domain. In other words, if a message claimed to be from abc@ftc.gov, the private market authentication proposals would authenticate that the message came from the domain "ftc.gov," but would not authenticate that the message came from the particular e–mail address "abc" at this domain. Hypothetically, if a phisher sent e–mail claiming to be from citibank.com, the message would be filtered by ISPs because the message would not have come from a designated

Citibank mail server. Consequently, ISPs and other operators of receiving mail servers could choose to reject unauthenticated e–mail or subject such messages to more rigorous filtering.

Spam filtering[247]

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

Common Vulnerability Exposure (CVE)[248]

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

Common Malware Enumeration (CME)[249]

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

Internet Engineering Task Force (IETF)

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

World Wide Web Consortium

The World Wide Web Consortium (W3C)[250] is an international consortium where Member organizations, a full-time staff, and the public work together to develop web standards. W3C's mission is "To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web."

[247] See DSTI/CP/ICCP/SPAM(2005)3/FINAL

[248] Information available at http://cve.mitre.org/

[249] Information available at http://cme.mitre.org /

[250] Information available at: www.w3c.org.

ANNEX D - EXAMPLES OF MALWARE PROPAGATION VECTORS

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

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

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

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

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

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

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

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

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

ANNEX E - GLOSSARY OF TERMS

Types of malware

There are many forms of malware and they are all capable of causing harm to computer systems. Below is a description of some of the main types of malware.

Backdoors.[251]. A backdoor is malicious code that allows unauthorised access to a computer system or network by accepting remote commands from an attacker elsewhere on the Internet. Backdoors allow attackers to execute remote commands and install other software, which may in turn compromise passwords or other personal data, or allow the machine to be used for further nefarious purposes. Remote access or backdoor functionality is typically now included in most trojan and bot programmes. A bot programme is a type of 'backdoor' programme that allows attackers to remotely control many compromised information systems (often thousands) simultaneously (or individually). Backdoors intentionally but ill-advisedly included in legitimate software products to facilitate remote customer support become exploitable vulnerabilities when discovered by malicious actors.

Keystroke loggers.[252]. A keystroke logger is a hidden programme that records and "logs" each key that's pressed on the compromised system's keyboard, as the legitimate user of the system is typing, in the process recording personal data like usernames, passwords, credit card and bank account numbers. Keystroke loggers secretly store the data away in hidden files that is eventually transmitted to a remote collection point, elsewhere across the network. Keystroke logging functionality is typically included in most trojan programmes.

It has been noted by experts that the popularity of keystroke loggers that log each keystroke pressed has decreased significantly over the last two years (anecdotal evidence only). Currently, the most popular malware data-capture technique is to intercept the submitted data stream before it is transmitted by the web browser. For a criminal, the benefits of this approach are many: cleaner data (you don't see mis-typed keys in the data, or data from other applications), the use of a simple "virtual keyboard" requiring mouse-clicks is defeated, data can be identified on a semantic level for each targeted institution (*e.g.* the username and password can be identified at the client end) and closer ties to the web browsing application. Often, the definition of "keystroke logger" is expanded to include this technique, though it is sometimes classified as spyware also *Rootkit*: A rootkit is a set of programmes designed to conceal the compromise of a computer at the most privileged "root" level, by modifying operating system files or inserting code into the memory of running processes. As with most malware, rootkits require administrative access to run effectively, and once installed can be virtually impossible to detect. [253]

The role of the rootkit is simply to conceal evidence of the compromise to the user, the operating system and other applications (*e.g.* anti-virus or anti-spyware products) designed to detect the presence of the malicious files that have been installed on the computer. In most cases, once a rootkit is installed anti-virus and anti-spyware products will not work. However, a rootkit is not required to effectively conceal the presence of the malware. Many types of malware disable, or have mechanisms for bypassing security counter-measures installed on a computer without using a rootkit.

[251] NIST p. 2-12.

[252] Ibid.

[253] AusCERT (2005).

Spam: Spam is commonly understood to mean bulk, unsolicited, unwanted and potentially harmful electronic messages.[254] There appears to be a growing correlation between malware and spam. It is important to note that only a discussion of spam that is used as a vector for the distribution of malware is within the scope of this report.

Spyware: Spyware is a form of malware that is capable of capturing a range of data from user input (keyboards, mice) and output (screens) and other storage (memory, hard drive etc.) and sending this information to the attacker without the user's permission or knowledge. Some spyware tracks the websites a user visits and then sends this information to an advertising agency while malicious variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or other applications.

Trojan horses: A Trojan horse is a computer program that appears legitimate but actually has hidden functionality used to circumvent security measures and carry out attacks. A trojan horse may enter a user's computer by presenting itself as a compellingly attractive tool of some sort, which the user intentionally downloads and installs, unaware of its ulterior purpose. Trojans typically build in the functionality of keyloggers and other spyware and a range of other functions to disable system security.

Virus: Directly analogous to its biological namesake, a virus is hidden code that spreads by infecting another program and inserting a copy of itself into that program. A virus requires its host program to run before the virus can become active and generally requires human interaction to activate. Viruses deliver a payload which could contain a simple message or image thus consuming storage space and memory, and degrading the overall performance of a computer, or in the case of a more malicious payload, destroy files, format[255] a hard drive, or cause other damage. Viruses were the very earliest form of malware, appearing first in the 1970s as escaped experiments from academic computer science labs and experimental teenagers, and most of the early ones would be better characterised as the effects of bad judgment rather than ill intent.

Worm: A worm is a type of malware that self replicates without the need for a host programme or human interaction. Worms generally exploit weaknesses in a computer's operating system or other installed software and spread rapidly from computer to computer across a network and/or the Internet. Worms and viruses are the only types of malware that can self-propagate. Increasingly, the terms 'virus' and 'worm' are used interchangeably.

Other useful information security terms

Availability

The property of ensuring that digital data within an information system and the system itself are available to authorised users.

Authentication/Authenticity

Authentication is the security goal of being able to prove or verify a person's or entity's identity with a certain level of assurance. Authentication mechanisms are used to provide access control to information systems.

[254] OECD (2006).

[255] Formatting is the process of completely deleting the operating system, all applications and user data from a computer.

Authenticity is the security goal of being able to prove or verify that an electronic message or transaction originated from a particular person or source with a certain level of assurance.

Confidentiality

Confidentiality is the security goal of being able to protect information and data from unauthorised access.

Domain Name

A Domain Name is the identifier or address of any entity on the Internet.

Domain Name System

The domain name system is the way Internet domain names are located and translated into an Internet Protocol, or IP, address. For example, the domain name www.oecd.org is a more user friendly and memorable alternative to the IP address 193.51.65.71.

Integrity

Integrity protection is a primary security goal of information systems which seeks to ensure that the system as a whole (people, data, software) have not been compromised and can continue to be trusted. Data integrity refers specifically to the ability to detect if data has been modified without authorisation.

There are a wide range of mechanisms which are designed to check data integrity, ranging from weak error-checking mechanisms, and simple hash functions[256] to stronger mechanisms using public key cryptography, such as digital signatures. Common and effective mechanisms for detecting deliberate data changes are to calculate and compare hash functions or to verify a digital signature (which is a special type of keyed hash function). Any malware compromise of a computer is an attack on data and system integrity as the malware modifies key system files and can insert any other file or programme the attacker desires and may, potentially, corrupt or modify any file on the system or generate data or conduct online transactions allegedly using the identity of the computer user.

Internet Protocol

The Internet Protocol is the native language of programmatic communication on the Internet. The Internet Protocol allows large, geographically diverse networks of information systems to communicate with each other quickly and economically over a variety of physical links. An IP address is the numerical address by which an Internet-connected computer is identified. Information systems on the Internet use IP addresses to route traffic and establish connections among themselves.

Non-repudiation

Non-repudiation is a security goal which seeks to prevent a person from denying they undertook an electronic transaction when they did. A mechanism that provides a non-repudiation service is a digital signature combining public key cryptography and a timestamp with the message to be secured. A digital signature is a unique string which can be used by a party to verify both the authenticity and integrity of an

[256] A hash function is a reproducible method of turning some kind of data into a (relatively) small number that may serve as a digital "fingerprint" of the data.

online transaction or message. The signature (or keyed hash) is a mathematical function derived from the user's private or secret key and the transaction details or message.

If non-repudiation is to work, it relies on the assumption that the signer alone has access to the private key and passphrase. However, an attacker can use malware to potentially subvert the computer on which the private key and passphrase is stored and hijack the signing process without the knowledge or authorisation of the owner of the key. In this way, the non-repudiation mechanism can be subverted.

See also transaction signing. Transaction signing in the manner described provides non-repudiation services, as there exists a high level of assurance that the legitimate user undertook the transaction.

Operating System

An operating system (OS) is a computer program that manages the hardware and software on a computer. An operating system performs basic tasks such as controlling and allocating memory, prioritizing system requests, controlling input and output devices, facilitating networking, and managing files. It also may provide a graphical user interface for higher level functions. It is the underlying environment within which all other software on the machine exists.

Patch/Workaround

A patch is a small piece of software code which is produced by a vendor and which is designed to correct or rectify an existing bug or flaw in an operating system or application programme. Mostly patches are produced to correct security–related flaws, which an attacker could exploit to compromise the security of a system.

A work-around is a set of actions that network security managers or administrators can take to reduce their exposure to a particular known software vulnerability. For example, a work-around may entail blocking traffic to or from certain ports; or disabling particular services which may carry a vulnerability. Generally, work-arounds are implemented if no patch is currently available.

Packet

A packet is the minimum autonomously-routable quantum of data which can be transmitted across a modern digital “packet switched network.” It consists of a “header” of routing, addressing, and protocol information, followed by a “payload” of data. A packet is a message containing data as well as the destination address that is transmitted over a network that transmits packets, or “packet switching networks.”

Payload

A payload is the essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination. Note that what constitutes the payload may depend on the point-of-view. To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include the part of the overhead data that this layer handles. However, in more general usage, the payload is the bits that get delivered to the end user at the destination.

Malware payload

This refers to the primary function of a piece of malware. For example, a mass mailing virus which propagates via e–mail may also have the additional primary function to delete user files on the infected computer.

Social engineering

This refers to techniques designed to fool human beings into providing information or taking an action which leads to the subsequent breach in information systems security. Examples of social engineering include telephoning the IT help desk and pretending to be an employee and asking for your password to be reset in order to gain unauthorised access to an employee’s computer account and the network; or sending an e–mail impersonating a victim’s bank in order to get the victim to click on a phishing URL and provide their bank account password into the fake attacker-controlled website. Social engineering is the computer industry’s term for what are more generally referred to as “confidence scams.” The term is intended to make a distinction from computer engineering or software engineering, in that social engineering uniquely attacks the human component of an information system.

Transaction signing

Transaction signing or digital transaction signing is the process of calculating a keyed hash function to generate a unique string which can be used to verify both the authenticity and integrity of an online transaction. A keyed hash is a function of the user’s private or secret key and the transaction details, such as the transfer to account number and the transfer amount. To provide a high level of assurance of the authenticity and integrity of the hash it is essential to calculate the hash on a trusted device, such as a separate smart card reader. Calculating a hash on an Internet connected PC or mobile device such as a mobile telephone/PDA would be counter-productive as malware and attackers can attack these platforms and potentially subvert the signing process itself.

Authentication factors

Single or multi-factor authentication refers to the number of ‘factors’ an authentication mechanism uses. The factors are something the user *knows* (such as a reusable PIN or password); something the user *has* (such as a credit or debit card or a token which generates a one-time password); or something the user *is* (such as a biometric e.g. a photograph or thumbprint). It is often assumed incorrectly that the assurance level of an authentication mechanism increases as the number of factors increase. However, it is not possible to assess assurance by the number of factors being used. How the authentication mechanism is implemented is critical. This paper shows that even strong forms of two-factor authentication using an OTP and challenge response can be subverted by malware.

Vulnerability

A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management of software that could be exploited to violate the system's security policy.

ANNEX F – AREAS FOR IMPROVEMENT AND FURTHER EXPLORATION

Awareness raising

Many websites and resources exist to help end users and SMEs secure their information systems but few of those programmes specifically address and explain the problems of malware.[257] Also, the number of resources can be overwhelming to users as information and guidance can vary from entity to entity. Furthermore, some advice is inconsistent and maybe inadequate in dealing with the rapidly changing nature of the threat. For example advice that implies that the only necessary countermeasure is keeping one's anti-virus patches up to date is inadequate.

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

Improved legal frameworks

Laws and regulations

International harmonisation/interoperation of cybercrime laws is essential. Widespread adoption of the Council of Europe's Convention on cybercrime may be effective in this respect. While 25 out of 30 OECD member countries have signed the Convention, only 8 of those 25 have actually ratified it. Furthermore, only 3 out of 21 APEC economies have signed the Convention and of those 3 only 1 has ratified the Convention. The Convention provides a framework for co-operation and is a general commitment to co-operate internationally against cybercrime.

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

Malware analysis can play an important role in recovering evidence and generating leads for law enforcement to investigate cybercrime. Malware analysis is often conducted using methods such as hard drive imaging, "real-time" forensics, antivirus testing, and reverse engineering.[258] In some cases these practices may not be permitted under laws that protect intellectual property.

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

There may be tensions between the protection of privacy and actions to fight malware. For example, CSIRTs may need to share information, such as an IP address, among themselves and with ISPs. However, IP addresses may be considered as personal data in some countries. This may present challenges for

[257] Industry organisations, such as APACS, have reported no reduction in the level of phishing due to awareness campaigns and public figures highlighting the problems and scale of the attack. APACS (2006) Vulnerability and threat assessment of authentication mechanisms used for Internet based financial services – 2006 review, page 3 and 4.

[258] CERT Coordination Center (2007) p. 24.

sharing the information which may in turn hinder the efforts to, for example, dismantle botnets and conduct investigation into the malicious activity.

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

Better policies and practices

Whois data is an important resource for attributing incidents of malware and therefore it should remain accurate and accessible to law enforcement.[259] Furthermore, malicious actors often abuse domain name registration policies, such as ICANN's "add-grace period" or the minimal information requirements set out by some domain name registrars (DNRs), to avoid detection by authorities.

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

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

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

As is the case with DNRs, there are thousands of ISPs that all have different policies and practices for addressing malicious online activity. ISPs are perhaps the best placed actors in the chain to help stop some types of malware attacks such at DDoS and botnets sending spam. While many ISPs are working to improve security policies some tend to have a higher than average amount of malicious activity. These different practices and policies may result in a different outcome each time an ISP is asked to take action against malware which impairs the ability to fight against malware in an effective and consistent manner**.**

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

Strengthened law enforcement

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

[259] Civil liberties groups have recommended that ICANN limit the use and scope of the Whois database to its original purpose and to establish its policies based on internationally accepted data protection standards. Public availability of Whois data may also conflict with the EU Data Protection Directive, which limits access and collection rights to the database's original technical purposes.

Government efforts to provide mutual assistance, and share information for the successful attribution and prosecution of cybercriminals should be strengthened.

Given the increased convergence between incident response and the gathering of evidence by law enforcement entities, co-operation between CSIRT teams and law enforcement entities should be strongly encouraged.

It is important for governments to commit adequate resources for specialised cybercrime law enforcement agencies to be able to investigate and prosecute cybercrime in co-operation with other concerned public and private stakeholders.

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

Improved response

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

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

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

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

Measuring of malware

Many entities track, measure and sometimes even publish data on their experience with malware and related threats.[260] However, vendors, CSIRTs, and the business community all have different data and ways of measuring the magnitude of the malware problem and its associated trends. Furthermore, there are many types of malware and little consistency of naming conventions in the technical community for identical types of malware. While existing data is helpful in understanding parts of the malware problem, it is not easily comparable in real and absolute terms.

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

Measures to address vulnerabilities in software

Vulnerabilities can be discovered by researchers either in the private sector or academia or by malicious actors with a motive for profit or to conduct a targeted attack for espionage or other purposes.

[260] See Annex A – Data on Malware.

Most vendors[261] support the use of 'responsible vulnerability disclosure' practices in which researchers inform the vendor about newly discovered software vulnerabilities and delay public disclosure to an agreed time to allow the vendor time to develop an appropriate software fix (patch).

Responsible behaviour by researchers should be promoted, such as contacting the affected company first rather than going public before a solution is available.

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

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

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

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

Technical measures

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

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

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

Research and development

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

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

[261] As an example, Microsoft is one: http://www.microsoft.com/technet/community/columns/secmgmt/default.mspx.

Standards, guidelines and good practice

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

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

Information sharing and the overall need for co–ordination and cross-border co-operation

All of the aforementioned areas for action illustrate the cross-cutting need for information sharing, coordination and cross-border co-operation. However, the communities of actors described above do not always collaborate in an effective manner to combat malware. Information sharing and co–ordination among the private sector, the government and other stakeholders is not always adequate to detect, respond, mitigate and take appropriate enforcement measures against malware. This can be at least partially attributed to the fact that no comprehensive international partnership for collaboration against malware does yet exist despite the significant work underway. (See Annex C).

A more holistic approach involving an integrated mix of policy, operational procedure and technical defences could be considered to ensure that information sharing, co–ordination and cross border co-operation are effectively integrated and addressed.

Economic aspects

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

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

Effectiveness and economic effects of assigning alternative forms and levels of legal rights and obligations (*e.g.* liability) to the different stakeholders. This would include legal constraints for ISPs to monitor and manage their networks (*e.g.* related to privacy, 'mere conduit', 'safe harbour' provisions).

Effectiveness and economic effects of blacklisting on ISP and end user security.

Effectiveness and economic effects of global measures to strengthen law enforcement and collaboration in the area of malware.

Effectiveness and economic effects of technological solutions to the problem of malware (*e.g.* 'security moving into the cloud' and 'tethered devices' for end users).

Strength of reputation effects and other feedbacks in mitigating the problem of information security.

Efforts to quantify the magnitude of the overall social externality due to lack of trust in the e–commerce system (growth effects, GDP impact).

Better assessment of the strength of the trade-offs between usability, availability, functionality, performance, cost and security.

Malware in next-generation networks and system architectures (*e.g*, more mobile, EoIP-everything over IP-networks, Web 2.0).

Obstacles to and means to enhance incentives for information security of individual users.

BIBLIOGRAPHY

1. Anti-Phishing Working Group ("APWG") (2006a), *Phishing Activity Trends Report*, available online at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf (last accessed 14 December 2007.

2. Anti-Phishing Working Group ("APWG") (2006b), *Phishing Activity Trends Report*, available online at: http://www.websense.com/securitylabs/resource/PDF/apwg_report_december_2006.pdf (last accessed 14 December 2007).

3. AusCERT (2005), *Windows Rootkit, Prevention, Detection and Response*, reference available online at:https://www.auscert.org.au/search.html?search_keywords=Windows+Rootkit%2C+Prevention%2C+Detection+and+Respons&search=GO (last accessed 11 December 2007).

4. AusCERT (2006), *Haxdoor – An anatomy of an online ID theft trojan*; reference available at :http://www.auscert.org.au/render.html?cid=1920 (last accessed 10 December, 2007)

5. Australian Government, Office of the Privacy Commissioner (2004), *Community Attitudes Towards Privacy 2004*, available online at: http://www.privacy.gov.au/publications/rcommunity/chap10.html (last accessed 11 December 2007).

6. BBC News online (2004), *MyDoom virus biggest in months* available online at: http://news.bbc.co.uk/1/hi/technology/3432639.stm (last accessed 14 December 2007).

7. BBC News online (2007); *Burgers paid for by mobile phone*, available at: http://news.bbc.co.uk/2/hi/technology/6400217.stm (last accessed 7 December, 2007)

8. Brendler, Beau; "Spyware/Malware Impact on Consumers"; APEC-OECD Malware Workshop; April 2007 (Source: StopBadware Project); available online at: http://www.oecd.org/dataoecd/33/55/38652920.pdf (last accessed 13 December 2007).

9. CERT Coordination Center (2006), *List of CSIRTs with national responsibility*, available online at http://www.cert.org/csirts/national/contact.html (last accessed 10 December 2007).

10. CERT Coordination Center (2007), *The Use of Malware Analysis in Support of Law Enforcement*, available online at:http://www.securitynewsportal.com/securitynews/article.php?title=The_Use_of_Malware_Analysis_in_Support_of_Law_Enforcement (last accessed 11 December 2007).

11. Charney, Scott (2005), Microsoft Corporation, *Combating Cybercrime: A Public-Private Strategy in the Digital Environment*, available online at: http://www.nwacc.org/programs/conf05/UNCrimeCongressPaper.doc (last accessed 11 December 2007).

12. Computer Economics (2007), *2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code*, reference available at:http://www.computereconomics.com/page.cfm?name=Malware%20Report.

13. Congressional Budget Office Cost Summary, *H.R. 1525 Internet Spyware (I-SPY) Prevention Act of 2007*, available at: http://www.cbo.gov/ftpdocs/80xx/doc8076/hr1525.pdf.

14. Consumer Reports WebWatch (2005), "Leap of Faith: Using the Internet Despite the Dangers". Results of a National Survey of Internet Users for Consumer Reports WebWatch, available online at: http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm ;

15. Council of Europe (2001), *Convention on Cybercrime*, available online at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

16. Council of Europe, Status of Signatories and Parties to the Convention on Cybercrime, available online at:http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/04&CL=ENG (last accessed 11 December 2007).

17. CSI/FBI Computer Crime and Security Survey (2006), available online at:www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=4SCJQ3Y0PCPTOQSNDLPCKHSCJUNN2JVN.

18. Dancho Danchev (2006), *Malware – future trends*, available online at:www.linuxsecurity.com/docs/malware-trends.pdf (last accessed 7 December, 2007)

19. Dearne, Karen (2007), *Online security begins at home*, Australian IT News , available online at:http://australianit.news.com.au/articles/0,7204,21675098%5E24169%5E%5Enbv%5E,00.html (last accessed 11 December 2007).

20. Denning, Dorothy (2000), *Statement by Dorothy Denning*, available online at: http://ftp.fas.org/irp/congress/2000_hr/00-05-23denning.htm

21. Devillard, Arnaud (2006), *Le « phishing » en France, peu de victimes mais une menace grandissante*, 01net., available online at : www.01net.com/editorial/311785/cybercriminalite/le-phishing-en-france-peu-de-victimes-mais-une-menace-grandissante/ (last accessed 11 December 2007).

22. Dhamija, Rachna; Fischer, Ian; Ozment, Andy; Schechter, Stuart E (2007); *The Emperor's New Security Indicators, An evaluation of website authentication and the effect of role playing on usability*, available online at: http://usablesecurity.org/emperor/.

23. Du, Yuejun Dr. (2007); APEC-OECD Malware Workshop; Presentation by CNCERT; available online at: http://www.oecd.org/dataoecd/33/59/38653107.pdf (last accessed 10 December, 2007)

24. Edwards, L., (2004), *Reconstruction Consumer Privacy Protection Online*, International Review of Law – Computers & Technology, Volume 18, No. 3, page 315.

25. European Commission Eurobarometer (2007), *E-Communication Household Survey*, available online at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_274_en.pdf (last accessed 10 December 2007).

26. F-Secure (2007a), *APEC-OECD Joint Malware Workshop Summary Record*, available online at:www.oecd.org/sti/security-privacy.

27. F-Secure (2007b), IT Security Threat Summary for H1 2007, available online at: http://www.f-secure.com/2007/1/.

28. Gartner (2005), *Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce*, available online at :http://www.gartner.com/press_releases/asset_129754_11.html.

29. Google Inc; *The Ghost In The Browser Analysis of Web-based Malware*; available online at: http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf (last accessed 12 December 2007).

30. Govcert.nl (2006), *Annual Review*, available online at: http://www.govcert.nl/render.html?it=147 (last accessed 13 December 2007).

31. Govcert.nl (2007), APEC-OECD Malware Workshop, [presentation available at: http://www.oecd.org/dataoecd/34/36/38653287.pdf (last accessed 10 December 2007).

32. Greene, Tim (2007), *Kapersky seeks help from international police to fight cybercrime*, Network World, available online at: http://www.networkworld.com/news/2007/013107-kaspersky-cybercrime.html (last accessed 14 December 2007).

33. Hypponen, Mikko (2006); "*Malware goes mobile"*; *Scientific American* p.70-77; available at:http://www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf (last accessed 13 December 2007).

34. iGillottResearch Inc (2006), *The Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks*, Available at:https://www.trustedcomputinggroup.org/groups/mobile/Final_iGR_mobile_security_white_paper_sept_2006.pdf (last accessed 7 December, 2007).

35. International Telecommunications Union (ITU) (2007), World Information Society Report 2007, available online at:http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07-summary.pdf.

36. Javelin Strategy & Research; *2007 Identity Fraud Survey Report—Consumer Version How Consumers Can Protect Themselves*; available online at:http://www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf (last accessed 14 December 2007).

37. Kaspersky Labs (2006), *Malware Evolution 2006: Executive Summary*, available online at: http://www.kaspersky.com/malware_evolution_2006_summary.

38. Krebs, Brian (2006), "The New Face of Phishing", *The Washington Post*, available online at: http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html.

39. Lemos, Robert (2007), *Estonia gets respite from web attacks*; Security Focus, available online at: http://www.securityfocus.com/brief/504.

40. Liu, Pei-Wen (2007), Information and Communication Security Technology Center, Chinese Taipei, OECD-APEC Tel Malware Workshop, available online at:http://www.oecd.org/dataoecd/34/19/38653499.pdf (last accessed 10 December 2007).

41. Mashevsky, Yury (2007), *The Virtual Conflict – Who Will Triumph?*, The Virtualist, Available online at: http://www.viruslist.com/en/analysis?pubid=204791915.

42. McAfee Inc. (2006), *Virtual Criminology Report 2007 Organized Crime and the Internet*, available online at: http://www.mcafee.com/us/threat_center/white_paper.html.

43. McAfee Inc. (2007), *Identity Thef,;* available online at: http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf

44. McCarthy, Caroline (2007), *Study: Identity theft keeps climbing*, Cnet News, available online at:http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html.

45. MessageLabs Intelligence (2006), *2006 Annual Security Report - A Year of Spamming Dangerously: The Personal Approach to Attacking*, available online at:http://www.messagelabs.com/mlireport/2006_annual_security_report_5.pdf (last accessed 10 December 2007).

46. Messagelabs (2007), *2007 Annual Security Report - A year of storms, spam and socializing…*; available online at: http://www.messagelabs.com/resources/mlireports (last accessed 10 December 2007).

47. Messaging Anti-Abuse Working Group (2007), *Email Metrics Program: The Network Operators' Perspective; Report #5 - First Quarter 2007* (Issued June 2007), available online at:http://www.maawg.org/about/MAAWG20071Q_Metrics_Report.pdf (last accessed 10 December 2007).

48. Messmer, Ellen and Pappalardo, Denise (2005), *Extortion via DDoS on the rise: Criminals are using the attacks to extort money from victimized companies*; Computerworld: http://www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html (last accessed 7 December, 2007).

49. Microsoft (2006a), *Security Intelligence Report; January – June 2006*; available online at: http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en.

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

51. Netcraft Toolbar Community (2007), *Phishing By The Numbers: 609,000 Blocked Sites in 2006*, available online at: http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html (last accessed 11 December 2007).

52. McNamara, Paul (2007), *Survey: Identity theft on the decline*, Network World, available online at: www.networkworld.com/community/?q=node/11009 (last accessed 11 December 2007).

53. NIST Special Publication 800-83, *Guide to Malware and Incident Handling*; page 2-10; available online at: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

54. Oberoi, Sabeena (2007); *Addressing the malware Problem*, APEC-OECD Malware Workshop, available online at: www.oecd.org/sti/security-privacy.

55. OECD (2005), *Science, Technology, and Industry Scoreboard 2005*, OECD, Paris; http://lysander.sourceoecd.org/vl=8111498/cl=14/nw=1/rpsv/scoreboard/d06.htm

56. OECD (2006), *OECD Anti-Spam Toolkit of Recommended Policies and Measures*, available online at: http://www.oecd-antispam.org/ (last accessed 13 December 2007).

57. OECD (2007a), *Communications Outlook,*OECD, Paris available online at:http://puck.sourceoecd.org/vl=8231979/cl=59/nw=1/rpsv/~6681/v2007n2/s1/p1l.

58. OECD (2007b), Bauer Johannes M., de Bruijne Mark, Groenewegen John P., Lemstra Wolter, and Van Eeten Michel, Delft University of Technology and Michigan State University, consultants to the OECD, *Economics of Malware: Security Decisions, Incentives and Externalities* (forthcoming).

59. OECD (2007c); *Summary Record of the APEC-OECD Malware Workshop;* available online at http://www.oecd.org/dataoecd/37/60/38738890.pdf.

60. Official Journal of the European Communities (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (last accessed 11 December 2007).

61. Official Journal of the European Communities (2002), Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector, available online

at:http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf (last accessed 11 December 2007).

62. Official Journal of the European Communities (2005), *Council Framework Decision 2005/222/JHA Of 24 February 2005 on attacks against information systems*, available online at:http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

63. ORF (2007), *Spamhaus antwortet auf nic.at*. futurezone, available online at: http://futurezone.orf.at/it/stories/201738/; last accessed 25 November 2007.

64. Outlaw.com, *Phishing attack evades ABN Amro's two-factor authentication*, available online at: www.out-law.com/page-7967 (last accessed 11 December 2007).

65. Poulsen, Kevin (2003), *Slammer worm crashed Ohio nuke plant network*, Security Focus, available online at: http://www.securityfocus.com/news/6767 (last accessed 11 December 2007).

66. RSA Security (2006), Internet Confidence Index Shows that – for Businesses and Consumers – Transactions are Outpacing Trust, available online at: http://www.rsa.com/press_release.aspx?id=6502 (last accessed 14 December 2007)

67. Shin, Annys (2007a); "Is Identity Theft Decreasing*"?;* The *Washington Post*, available online at http://blog.washingtonpost.com/thecheckout/2007/02/is_identity_theft_decreasing.html.

68. Shin, Annys (2007b), *The Checkout*, available online at:http://blog.washingtonpost.com/thecheckout/2007/02/looking_for_a_job_phishers_are.html.

69. Sokolov, D. A. (2007) *Spamhaus.org setzt Österreichs Domainverwaltung unter Druck;* available online at: http://www.heise.de/newsticker/meldung/91417; last accessed 25 November2007.

70. Sophos (2006a), *The Growing Scale of the Threat Problem*, available online at:http://www.sophos.com/sophos/docs/eng/papers/Growing-threat-wpus.pdf (last accessed 7 December, 2007).

71. Sophos (2006b), *Devious Arhiveus ransomware kidnaps data from victims' computers*, available online at: http://www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html (last accessed December 7, 2007).

72. Sophos (2006c), *Married couple formally charged over spyware Trojan horse*, available online at: "http://www.sophos.com/pressoffice/news/articles/2006/03/israeliesp2.html (last accessed 13 December 2007).

73. Sophos (2007a), *Security Threat Report* available online at: http://www.sophos.com/security/whitepapers/ (last accessed 12 December 2007).

74. Sophos (2007b), *Security Threat Report Update July 2007*, available online at: http://www.sophos.com/security/whitepapers/ (last accessed 12 December 2007).

75. Spamhaus (2007), *Report on the criminal 'Rock Phish' domains registered at Nic.at*. available online at http://www.spamhaus.org/organization/statement.lasso?ref=7; last accessed 25 November 2007.

76. Stewart, Joe (2004), *Win32.Grams E-Gold Account Siphoner Analysis*; available online at http://www.lurhq.com/grams.html (last accessed 11 December 2007).

77. Symantec (2006), *Internet Security Threat Report Volume X*, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf (last accessed December 10, 2007).

78. Symantec (2007), *Internet Security Threat Report Volume XI*, available online at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

79. *The Economist* (2007), "A cyber riot", http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598 (last accessed 4 December, 2007).

80. The Honeynet Project and Research Alliance (2007), *Know your enemy: Fast-Flux Service Networks*, available online at: http://www.honeynet.org/papers/ff/ (last accessed 13 December, 2007).

81. *The Sydney Morning Herald*; "Cyber attacks force Estonian bank to close website": http://www.smh.com.au/news/breaking-news/cyber-attacks-force-estonian-bank-to-close-website/2007/05/16/1178995171916.html (last accessed 4 December, 2007).

82. The Register, *Phishing attack evades bank's two-factor authentication*, available online at: http://www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/.

83. TriCipher (2007), *Consumer Online Banking Study*, available online at:http://www.tricipher.com/news/pr134.htm (last accessed 14 December 2007)

84. Tippett, Peter (2006), *The Fourth Generation of Malware*, CIO Update, http://www.cioupdate.com/article.php/3598621 (last accessed December 7, 2007)

85. Twomey, Paul, *Current Countermeasures and Responses by the Domain Name System Community*, APEC-OECD Malware workshop; available online at: http://www.oecd.org/dataoecd/34/40/38653402.pdf .

86. *Trend Micro* (November 2005), "Taxanomy of Botnet Threats"; available online at http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/botnettaxonomywhitepapernovember2006.pdf (last accessed 10 December 2007).

87. United Kingdom Centre for the Protection of the National Infrastructure (2005), *NISCC Briefing Targeted Trojan*, available online at: http://www.cpni.gov.uk/docs/ttea.pdf (last accessed 7 December, 2007).

88. United States – Canada Power System Outage Task Force (2003), *Blackout in the United States and Canada: Causes and Recommendations*; available online at: https://reports.energy.gov/BlackoutFinal-Web.pdf (last accessed 14 December 2007).

89. United States Computer Emergency Response Team (US-CERT), *Federal Incident Reporting Guidelines*: http://www.us-cert.gov/federal/reportingRequirements.html.

90. United States Department of Justice Computer Crime & Intellectual Property Section, *Computer Crime Cases (as of 11 December 2007)*, available online at: www.cybercrime.gov/cccases.html.

91. United States District Court Northern District Of Illinois Eastern Division (2007), *US v. James Brewer*: http://www.spamsuite.com/book/export/html/148 (last accessed 14 December 2007).

92. United States Federal Trade Commission (2003), *ID Theft Survey Report*, available online at:http://www.ftc.gov/os/2003/09/synovatereport.pdf (last accessed 14 December 2007).

93. United States Government Accountability Office (2007), *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, available online at: http://www.gao.gov/new.items/d07705.pdf.

94. United States Joint Council on Information Age Crime (2004), *Computer-related Crime Impact: Measuring the Incidence and Cost January 2004*: http://www.jciac.org/docs/Computer-Related%20Crime%20Impact%20010904.pdf.

95. United States National Consumer League / National Fraud Information Center (2006), *Top 10 Internet Scam Trends from NCL's Fraud Center*, available online at:: http://fraud.org/stats/2006/internet.pdf (last accessed 10 December 2007).

96. United States Nuclear Regulatory Commision (NRC) (2003), *Information Notice On Potential Of Nuclear Power Plant Network To Worm Infection*, issued 2 September 2003, available online at: http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html (last accessed 11 December 2007).

97. Whittaker, Colin, APACS, APEC-OECD Malware Workshop presentation; available at:http://www.oecd.org/dataoecd/33/53/38652807.pdf (last accessed 10 December, 2007).