Carnegie Mellon University
Heinz School (MSISPM)

THESIS REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science in Information Security and Policy Management

Title: **AVOIDING THE CYBER PANDEMIC: A Public Health Approach to Preventing Malware Propagation**

Presented by: Kim Zelonis

Thesis Advisor: Julie Downs

_____

Signature **Date**

Project/Thesis Presentation Date: 8 December 2004

AVOIDING THE CYBER PANDEMIC:

A Public Health Approach to Preventing Malware Propagation

Kim Zelonis

THESIS REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF

Master of Science in Information Security and Policy Management

Fall 2004

Abstract

The problem of malicious software (malware) is escalating to pandemic proportions. The enormity of the threat is evident by continual increases in four malware attributes: frequency of incidents, speed of propagation, damage done or intended, and the universality of the impact. Continuation of this trend threatens all systems dependent on the Internet.

Technological solutions to the malware problem have been long in coming and are likely to be vulnerable to be vulnerable to human action or inaction. As long as computer operation is a combination of technological capabilities and human control, a malware defense needs to combine these elements as well. Unfortunately, the computer security industry as a whole has made little effort to modify the risky behaviors adopted by the average computer user.

The public health discipline consistently combines scientific solutions and human interventions to prevent the spread of disease. One clear example of this has been the fight against HIV/AIDS. Medical technologies to treat and prevent HIV/AIDS have been strategically combined with behavioral interventions and awareness campaigns. By analyzing the effective elements of interventions that modify behaviors that enable the spread of HIV/AIDS, we can identify strategies for modifying the user behaviors that enable the spread of malware.

Just as there is little likelihood of eliminating all disease, it is unlikely that malware can be completely eliminated. However, effective strategies can keep malware outbreaks to controllable levels. This paper proposes analogous solutions to combined behavioral and technological approaches to fighting the malware epidemic based on successful strategies in the HIV/AIDS epidemic. These generally involve applying common characteristics and monitoring methodologies from public health interventions. Technology solutions should still be pursued but with the intent of working in combination with user behavioral strategies.

Acknowledgements

Producing a multi-disciplinary work such as this requires input from people with varied backgrounds. I was lucky to have assistance from a number of highly knowledgeable individuals, most notably:

- **Julie Downs, SDS, Thesis Advisor**
- Center for Risk Perception and Communication
- Dave Mundie, CERT/CC
- Dena Tsamitis, CyLab
- Jeanne Bertolli, CDC
- Karyn Moore, Heinz School
- Sumitha Rao, Heinz School

Special thanks, too, to Rita Harding of the US IHS for pointing me to Jeanne Bertolli, and my mother for asking Rita for recommended contacts in the first place. I, also, greatly appreciate the work done by Curt Connolly and John E. Lane, Jr. to help create graphics for my thesis presentation. Finally, thanks to everyone who did not see me much this semester as I worked on this project but supported me nonetheless.

TABLE OF CONTENTS

1 Introduction

The threat of malicious software (malware) emerged in the late 1980s. Since then, computer scientists have proposed a number of technical solutions to mitigate the threat of malicious code performing unauthorized actions on a computer, series of computers, or the network infrastructure. To date, no comprehensive and practical solution has emerged. Even if a solution were found to prevent all known types of attacks, the hacker/cracker realm would likely go on to discover new methods of control.

With the focus on technical solutions, the human element is often ignored. The disregard of end users is sometimes justified by stating that it is difficult to explain the problems to non-technical people and protecting a machine requires someone to be a computer expert [61]. Others argue that technology solutions are needed because recent threats spread so quickly that they do their damage before a human can intercede [12][56].

However, whether the computer science community wishes to acknowledge them or not, humans are a significant part of the system that propagates malware. Human action or inaction enables the spread and effectiveness of malware in most cases. Replacing these risky behaviors with risk mitigating behaviors will be an important step in controlling the malware threat.

That is not to say that technological change is not important. It forms the basis for what human users can or can not do. What is needed is a combined effort of technological and behavioral change. As long as computer use is a combination of technological capabilities and human action, a malware defense needs to combine these elements as well.

Because the computer security industry does not have a history of intervening with people to instill behavioral change, it makes sense to look at outside models for guidance. In this paper I look to public health methodologies. Public health professionals look at disease outbreaks with a broad scope rather than focusing on individual prevention and treatment. The discipline also pairs technological (specifically bio-medical) innovation

with human intervention in order to control epidemic outbreaks. One of the most highly publicized public health initiatives of the past 20 to 25 years has been the prevention and control of HIV/AIDS.

HIV/AIDS is a pandemic. The disease has spread throughout the world and threatens people of a wide variety of socioeconomic backgrounds. The generally recognized start of the HIV/AIDS crisis is a little less than a decade before the release of the Morris/Internet worm that is generally considered the start of the malware crisis. This positions HIV/AIDS to provide tested models for population-level behavioral change with an extra decade of experience over the malware fight. Additionally, approaches to HIV/AIDS have basis in many years of public health expertise to control the spread of sexually transmitted diseases and other contagions. It is this history which I hope to draw upon to inform the computer security industry.

Granted, the HIV/AIDS pandemic continues to spread and take lives; however, there have been some positive trends within the last decade. I pull examples from those public health programs shown to be effective by analyzing the attributes that made them work.

In this paper I explore the analogous attributes between malware and HIV/AIDS. From there I justify a basis of comparison for translating HIV/AIDS public health initiatives to computer security network initiatives.

1.1 Terminology Used in This Paper

1.1.1 Malware

Malicious software or malware is generally defined as any program that executes unauthorized commands, generally with some sort of nefarious intent. Different types of malware are given specific names based on how they are distributed and how they deliver their malicious payload. Worm, virus, Trojan horse, remote access Trojan (RAT), and backdoor are all types of malware, but these categories are not mutually exclusive[56]. As a result, some authors acknowledge the interchangeable use of these terms under certain circumstances [36][56][59][82][92].

In order to avoid getting lost in semantics, I generally use the term malware throughout this paper. I make periodic exceptions when referencing the work of an author who makes a clear delineation between certain types of malware or when I reference an attribute that, based on common definitions, only applies to a certain type of malware.

Other malware-related terms include malcode and payload. Malcode refers to the programming code that contains malware logic. Payload is the common term for the malicious processing that the malware is designed to perform. Much malware only has logic to propagate and deliver payload. In the case of a Trojan horse, there may be other functionality of the program besides propagation and payload in order to obfuscate the program's true intent.

1.1.2 HIV/AIDS

HIV/AIDS is the term generally used in current public health literature to describe the disease that originates with infection from the HIV virus. Historically, the term AIDS alone was used. AIDS stands for "Acquire Immune Deficiency Syndrome." Syndrome is a specific term used in the medical community for symptomatic diseases that are not clearly understood. As more has been learned about AIDS, understanding of the disease have moved beyond that of a vague syndrome. The disease is now more correctly termed "HIV disease." "HIV/AIDS" is also commonly used to clearly connect the disease to pre-existing awareness under the name AIDS.

In this paper, I try to use the extended yet more correct term HIV/AIDS rather than just AIDS. I use the term HIV if I am referring to the virus instead of the disease. I only use AIDS in reference to historical initiatives using that designation.

1.2 Scope of This Paper

The scope of this paper serves not to recommend behaviors for individual users but to set guidelines for creating high-level policies that, in turn, seek to modify user behavior. That is, I seek to recommend the equivalent of a public health approach not individual treatments.

Except for a few specific examples, I am looking for solutions to combat malware as a whole rather than just viruses or just worms, although some recommendations are likely to have a greater impact on a particular type of malware. Particularly, I will focus on malware that spreads over networks, either self-propagating or as a result of a user action, but many of the interventions would also prevent the spread of malware via infected disks as well.

When addressing HIV/AIDS risk behaviors, I focus primarily on sexual transmission of the HIV virus. Significant attributes of other methods of transmission are largely redundant for the purposes of analogy, but I mention them when applicable.

1.3 Structure of This Paper

Section 2 describes the nature of the pandemic threat of malware and the need for new approaches of controlling it. In Section 3, I review some malware analogies with biological disease. In Sections 4 and 5, I describe the history and trends of malware and HIV/AIDS respectively. In Section 7, I describe some successful and intriguing public health techniques used to change population behaviors that help to spread HIV, and I identify some common elements of successful interventions. In Section 7, I explore the analogous and disanalogous aspects of malware and HIV/AIDS, and I recommend ways in which the best practices of HIV/AIDS public health techniques could be applied to preventing the spread of malware. In Section 8, I introduce some emerging anti-malware strategies that seem to indicate moves in the right direction. In Section 9, I summarize my conclusions and recommendations. In Section 10, I make recommendations for future work in this area.

2 Overview of the Problem

The Internet is a commodity. Although the average kitchen still lacks the proverbial Internet toaster, the Internet is something that people have come to depend on in their personal and professional lives. Doomsayers sometimes presage coordinated cyber attacks that result in rampant physical destruction, even death. Although such scenarios are technically possible, few attackers would have resources to bring them to fruition.

However, much simpler attacks can easily result in widespread frustration, confusion, economic loss, or general chaos.

Some malware damages the host on which it is running, usually by corrupting files or consuming resources. However, most malware avoids complete destruction of the host because that would prevent its ability to spread further. Frequently, malcode is designed to gain control of numerous computers on the network simultaneously. Once an attacker has control of a large number of hosts he can launch a denial of service attack, steal or corrupt sensitive information, or disrupt network usage [84]. The result is an iniquitous threat that damages even hosts and data owners that were not directly infected.

2.1 A Pandemic Threat

Security pundit Bruce Schneier recently wrote, "We're in the middle of a huge virus/worm epidemic" [77]. In the past year, the Internet has been described as "polluted" [61] and "dead or dying" [28]. Anti-virus experts have been described as "fighting a losing battle" [42].

2003 was widely declared by the media as the "worst year ever" for worms and viruses and 2004 has only gotten worse [35]. Windows viruses increased 400% in the first half of 2004 versus 2003 [73]. Without action, this epidemic will increase in magnitude until the Internet is unusable.

The term "virus" itself is from the medical lexicon, so it is reasonable to borrow another medical term to describe the global, widespread emergency that may face us in the coming years. Whereas an epidemic is a widespread disease outbreak within a community, a pandemic is an outbreak that spans communities. As the malware threat gains momentum all connected computers are at constant risk as opposed to the spikes of outbreaks today.

The pandemic threat is evident by continual increases in four malware attributes:

- Frequency of incidents,
- Speed of infection,

- Damage created, and
- Universality of the threat.

2.1.1 Frequency

The frequency of attacks is continually increasing. It seems that there is always a new worm or virus on the loose. Part of this is due to the creation of many variants of existing malware, thus minimizing development efforts by reusing code. The latest malware is virulent for longer than its predecessors and spawns more variants [11]. The creation of such variants is enabled by readily downloadable malcode toolkits [56]. Such reuse allows for a Darwinian evolution in which the best code is passed on to the next generation.

2.1.2 Speed

The speed of infection is escalating due to innovations in propagation methods. The idea of a "Warhol Worm" that can infect all vulnerable hosts in about 15 minutes no longer seems unrealistic. In fact, some argue that this has already happened. SQL Slammer only took 10 minutes to infect 90 percent of its vulnerable hosts, but others argue that this was not a true Warhol Worm because the payload only performed a denial of service attack [13]. Still, it is not hard to believe that a more malicious, hyper-virulent worm is coming.

2.1.3 Damage

Malware is becoming more malicious. There was a time when the threat of most viruses was little more than nuisance, such as sending emails to contacts found on the infected computer. Now the payloads do much more, including granting someone else complete control over the infected machine. Additionally, malware can attack the network infrastructure itself or leak sensitive data from servers.

A number of malware variants open up rights on the infected computer for future use, sometimes even allowing the attacker complete remote access to the machine. Sometimes, very specific remote access is created. For example, Sobig creates spam email proxies on its infected hosts, and Fizzer sets up a web server that may be later used to serve porn content [35].

The dramatic emergence of distributed denial of service attacks in February 2000, which brought down many major web sites, forever changed the nature of the malware threat. No longer were infected computers the only potential target of the malware payload. These machines only served as zombies to attack other targets, such as prominent web servers.

The Computer Emergency Response Team (CERT/CC) at Carnegie Mellon University identifies increased infrastructure attacks as a significant, emerging trend in malware [21]. These attacks target the network itself or manipulate content on it. A denial of service attack can make a desired web site or entire portion of the network unavailable; worm infestations can slow down network traffic; content can be modified to yield false information; or sensitive information can be retrieved and distributed.

Such attacks affect more than just the directly infected hosts. Even non-Internet users could be impacted by sensitive information leakage from corporate or government servers. For example, bugbear.b was designed to steal information from financial institutions. The malcode checked to see if an infected computer was on the network of any of 1300 banks; if so, it collected files meeting specific criteria and emailed them to a central computer [35]. Leaking sensitive account information would impact all bank customers, not just the Internet users among them.

Additionally, many attacks have larger economic impacts, the ripples of which can be far-reaching. For the first time, The 2004 CSI/FBI Computer Crime and Security Survey reported that virus attacks were the security incidents resulting in the highest cost to companies [40]. The next highest costs where the result of denial of service attacks caused by malware running elsewhere Previously, the most expensive security incident had always been theft of proprietary information.

Not surprisingly, future malware is predicted to do greater damage [36].

2.1.4 Universality

Until five years ago, malware attacks primarily impacted the owners/users of machines that were infected or were attempting to be infected as described above. Malware that propagates spam and hard porn can have broad reaching affects. Even more so, attacks that release sensitive data or attack the Internet infrastructure itself have the potential for significant damage to both individuals and organizations. As described above, even non-Internet users can be adversely affected by malware attacks. As a result, protecting one's own computer or being a Mac user in a Windows world may not shield a person from the impact of malware.

As computers become more ubiquitous, malware authors will have more systems that they can infect. The only limit to the malice that can be unleashed is whether or not someone chooses to do so. Malware is a societal threat. As a result, a comprehensive approach is necessary to minimize the damage we allow it.

2.2 No Solutions

In the aptly titled "A Failure to Learn from the Past," Spafford notes that the computer security community is still trying to solve the same problems that existed when the Morris Worm was released [82]. Additionally, we seem to be fighting malware in similar ways as we were over a decade ago.

Although malware has been evolving, our methods of combating it have remained disturbing stagnant. Ten years ago it was predicted that anti-virus scanner software would become insufficient [53]. Since then a number of other theoretical protections have been proposed, but none have become widely implemented. Although there have been incremental improvements to signature-based anti-virus software—including auto-updates and perimeter/email scans—this antiquated software concept remains our primary form of defense.

Cyber-security pundit Bruce Schneier writes that when asked what users can do about computer security he quips, "Nothing, you're screwed" [76]. Another author states that

there is no viable solution to the malware threat [34]. Another writer emphasizes that reactive solutions are not enough [11].

The prime difficulty in crafting malware solutions is determining how to defend the network without knowing the nature of the next attack [41]. Graham-Rowe decries current anti-virus strategies as "fundamentally flawed," noting that patching cannot keep up with spread, scanners slow down processing, and heuristics result in many false positives [42].

Even seemingly effective protections may be circumvented with future attack methodologies. The Klez virus and its derivatives attempt to disable popular anti-virus software. CERT cites an increased "permeability of firewalls" as a significant attack trend [21].

2.3 The Human Element

Seeking technological improvements to prevent malware propagation and payload is important to keeping this problem under control. However, as long as the processing, maintenance, and configuration of computers is a blend of automated and human-initiated actions, protection of those computers will need to blend automated and human-initiated actions in order to be effective.

Current anti-virus software can protect against many threats. But user vigilance is required to ensure that software is properly installed and updated. In order to protect a machine, a user must keep abreast of the latest threats and download updates or adapt the appropriate security configurations. Users are more likely to be vigilant after a previous infection, but this period of vigilance is temporary [90]. Lacking other motivators users become apathetic.

Despite the importance of the human element, end user involvement is often overlooked when creating anti-malware strategies. For example, in the conclusions section of a recent virus prevalence survey sponsored in part by Network Associates and Microsoft

Corporation, the recommended "intelligent risk management solution to virus problem" did not include any education or user awareness elements [11].

In a paper titled "Users Are Not the Enemy," Adams and Sasse note that, "Hackers pay more attention to the human link in the security chain than security designers do" [1]. Although the authors made this comment in reference to authentication systems, it appears to be true for all computer security issues as most attacks involve some sort of social engineering.

2.3.1 Social Engineering

Social engineering is when attackers employ tricks that convince users to break normal security protocols, many times without even realizing that they have done so [29]. For viruses and worms this means motivating the user to do whatever it takes to run the code.

The clearest examples of social engineering in malware propagation are the tricks used to persuade users to open email attachments. Some of these include:

- Address spoofing,
- Intriguing subject lines,
- Deceptive file extensions, and
- Embedded scripts.

Address spoofing is when a false sender address is associated with an email so that it looks like the message is from a trusted source such as a friend, computer support person, or the mail server. People are also likely to open mail with intriguing subject lines like a promise of pictures of Anna Kournikova. The Swen virus was sent in a message that appeared to be a Windows security update [35]. The MyDoom virus was made to look like an error message from an email that could not be delivered [58].

As malware propagation via email attachments became commonplace, some users were learned that certainly file extensions, like .exe or .vbs, were dangerous to open. The malware authors responded with tricks such as using double file extensions to obfuscate the true file type. One attack technique exploits the fact that ".com" is both an executable

file extension as well as a popular domain name suffix [78]. Furthermore, if a user's mail client is too permissively configured embedded scripts in email messages can automatically execute without the user having to click on an attachment at all.

Even malware that does not propagate via email can have a social engineering component to its design. By ensuring that the malcode can run with minimal system interruption on the infected computer, the program is likely to run without making the user suspicious and possibly prompting a thorough virus scan and clean-up.

2.4 Need for Intervention

In the public health realm, interventions are defined as programs with "a coherent objective to bring about behavioral change in order to produce identifiable outcomes" [80]. Interventions serve to change individual behaviors that create negative outcomes. In cyber security, there is a need to change behaviors in the user the community in order prevent malware propagation.

In October 2004, America Online and the National Cyber Security Alliance released the results of a survey that questioned computer users about security issues and scanned their computers for compliance [4]. The survey results show that users in general do not clearly understand the risks associated with their online behaviors, nor do they have the skills to properly protect themselves.

According to the survey, 77% of the respondents felt that their computers were "very safe" or "somewhat safe" from online threats. When asked specifically about viruses, 73% still felt "very safe" or "somewhat safe." Unfortunately, the state of their actual machines would give little reason to be that confident.

63% of the users surveyed have had a computer virus at some time. Another 18% were not sure. According to the computer scans, 19% of the computers were infected at the time of the survey. The average number of different viruses on a single computer was 2.4, and one machine had 213.

85% of the computers had anti-virus software installed. 71% of the users claimed that the software was updated at least once a week, either manually or automatically, but only 33% of the machines actually had software that had been updated within the past week. This left 67% of the machines with outdated anti-virus software or no anti-virus whatsoever.

The scanning revealed that 67% of the computers did not have a firewall running. Very few dial-up users had a firewall and only half of the broadband users had one. 14% of the users with firewalls were vulnerable by having open ports. In total 72% of the computers either had no firewall or the firewall was misconfigured.

Lest we dismiss the sample population as an uneducated group, it should be noted that 85% of the respondents had at least some education past high school. 51% had a bachelor's or master's degree. The average number of years online was 6.79.

This survey is very telling in that it demonstrates that computer users are not properly protecting themselves from malware infections.

Additionally, although most of the respondents' computers had been infected with a virus at some time, most of the respondents still felt safe from virus threats. Perhaps this indicates that they do not understand the potential damage that malware can perform.

3 Malware and Disease Analogies

This paper explores malware prevention and control and the analogous attributes of public health techniques used for prevention and control of HIV/AIDS. There are a number of examples of the use of other biological analogies, particularly disease analogies, in the study of malware. Many of these works are reviewed in brief below.

3.1 Biology-based Terminology

Although the first computer "bug" was literally a moth caught in the machine [58], viruses and worms received their names from biological metaphor rather than literal infestations. Spafford gives an in-depth description of the origins of the terms worm and

virus as they relate to computers [82]. The term worm is based on the self-propagating "tapeworm" programs described in the Science Fiction novel *The Shockwave Rider*. However, that reference was likely inspired by biological tapeworms. The term virus was first applied in a technical description of a theoretical program, but the term was popularized in the novel *When Harley Was One*.

Although virus and worm are the most commonly applied analogous biological terms for malware, their usage often leads to the application of other analogous terms. One early description of the Morris/Internet Worm called the incident "helminthiasis of the Internet," referencing the medical term for a worm infestation [74]. Another author extends the disease metaphor by describing highly infectious hosts as "Typhoid Marys" [34].

3.2 Epidemiological Analogy

A number of sources extend the virus analogy beyond the name and compare the spread of malware to the epidemiology of disease spread [12][26][59][89]. Boase and Wellman describe not only the similarities between computer and biological viruses but with viral marketing techniques as well [9].

Although the comparison with disease epidemics is generally in observance of the spread patterns, others have used the analogy of malware as infectious agents that create threats analogous to medical trauma [15]. Another author looks to the genetic diversity that enables survivability from epidemic outbreaks and uses it as an argument for operating system heterogeneity [83].

3.3 Immunological Analogy

Several proposed malware solutions are based on animal immune systems [3][33][53][95]. Williams also explores the immune system analogy but does not recommend any specific solution based on it [95]. The solution described by Kephart creates host-based immune systems that communicate with the network to generate antibodies to fight new attacks while minimizing auto-immune responses that would identify good software as malicious [53]. Forrest uses the analogy in a different way by

envisioning an intrusion detection system that incorporates the immune system attributes of disposability, self-repair, mutual protection, and dynamic coverage [33]. The "cooperative immunization system" described by Anagnostakis et al. disseminates defense mechanisms to vulnerable computers based on information sharing from the infected [3].

3.4 Vaccination and Quarantine

Other medical solutions have also served as inspiration for technical research. For example, Ghosh and Voas describe an inoculation solution that uses the contagion (in this case the malcode rather than a biological virus) in a controlled way to fight the outbreak [37]. Sidiroglou and Keromytis propose a "vaccine architecture" using short term fixes to slow the spread of a virus before a more comprehensive cure is available [79].

Moore et al. attempt to model a variety quarantine strategies for worm outbreaks [62]. The authors note that it is quicker and easier to identify a worm than to understand it; therefore, it makes sense to isolate malware activity until a proper response can be identified. Their simulations show that a containment solution is desirable but in order to be effective major innovations would need to be made to develop algorithms to rapidly identify outbreaks; enhance router systems to enable complex and efficient content filtering; and coordinate cooperation amongst major ISPs.

3.5 Some Other Biological Analogies

Other biological analogies have also been explored. Spafford explored, and largely discredited, arguments that computer viruses constitute artificial life [81]. Williams looked at malware from a number of infectious analogies including parasites, but the description was largely illustrative without provide much guidance for action [95]. Gorman et al. look at malware from a predator-prey perspective, exploring the impact of ecological diversification on survivability [41].

3.6 Cyber Center for Disease Control and Prevention

One analogy that is relevant to the public health approach evaluated in this paper is that of Staniford et al., who propose a Cyber-Center for Disease Control (a CCDC) based on the public health CDC model [84]. The authors suggest that the CCDC would identify

outbreaks, rapidly analyze pathogens, fight infections, anticipate new vectors, proactively devise detectors, and resist future threats.

The CCDC concept would likely be supported by Williams who noted that, unlike the medical industry, cyber security has few experts that can be called upon for diagnosis and help [95]. The solution proposed by Anagnostakis et al. builds on the CCDC idea by adding automated distribution of protection based on the information pooled therein [3].

Initially, a CCDC may seem similar to the Computer Emergency Response Team/Coordination Center (CERT/CC) or the various computer security incident response teams (CSIRTs) that have been established since the initial creation of CERT; however the scope of a CCDC as defined by Staniford et al. or as implied by comparison to the existing CDC goes beyond that of what is taken on by CERT. Initially, CERT was almost completely a reactionary organization dealing with historical or on-going outbreaks. In 1992, a vulnerability team was formed at CERT to start to address problems proactively [64]. However, based on CERT's own statement of mission, the organization deals primarily with computer security professionals, such as systems administrators and network managers, and vendors [20]. The organization has little focus on the user population at large as would be expected of a public health inspired organization.

However, even if CERT were to extend its focus, there are arguments against the creation of a centralized security authority. It has been suggested that the public is not likely to trust a central authority for systems patches [79]. Additionally, a single central authority may not be the most efficient solution. Spafford questions the existing CERT model, instead proposing that a distributed, coordinated response would be more effective than a single center of expertise [82].

I attempt to take these criticisms into consideration as I further analyze public health analogies.

3.7 Biological Pragmatism

Much of the use of biological analogy is done with the implied intent of finding a cure for malware and eradicating the threat, but other authors focus on the goal of survivability rather than constant health. Kephart et al. note that we will always need to coexist with computer viruses just as we coexist with biological ones [54]. Williams articulates that just as we do not expect to go our whole lives without ever being sick, we cannot expect our computers to never get viruses [95].

Although these views may seem defeatist, they allow for the consideration of more manageable solutions without the requirement of a definitive cure. Just being able to ease the symptoms of malware is an improvement. This paradigm is particularly apt in the HIV/AIDS analogy wherein no cure currently exists so efforts focus on prevention, quality of life, and decreased mortality rates.

3.8 HIV/AIDS

Several authors have described similarities in the propagation networks of HIV/AIDS and malware [7][9][26]. One paper analyzes HIV/AIDS in terms of the malware problem only, using the analogy to attempt to predict future malware propagation trends [15]. I am aware of no work that explores the possibility of applying HIV/AIDS public health solutions to the malware problem as I do herein.

4 History and Trends in Malware

Every year, malware becomes more pervasive and more malevolent, despite new strategies and tools being proposed to prevent and control the spread of malware. This section explores the characteristics of malware and the threat it creates.

4.1 A Brief Malware History

Although some viruses and worms existed before, the release of the Morris/Internet worm on November 2, 1988 is generally considered to be the first significant malware event. Since that time, there has been a steady increase in malware [82].

Within a month after Morris Worm outbreak, the Computer Emergency Response Team/Coordination Center (CERT/CC) was established at Carnegie Mellon University to

help to address security incidents. Soon thereafter the Forum of Incident Response and Security Teams (FIRST) was established to facilitate the rollout of numerous computer security incident response teams (CSIRTs) and was most active in doing so during the 1990s [64]. In 1991, the first commercial anti-virus software was released [49]. In 1992, CERT formed a vulnerability team in an effort to move to proactive analysis of threats [64].

In the early to mid 1990s, the establishment of the World Wide Web and the commercialization of the Internet significantly increased the number of nodes and users on the network. As the Internet grew, malware evolved and thrived. Some notable outbreaks include the following:

- 1999, Melissa—emerges as first major malware to proactively email itself [29],
- 2000, "I Love You"—uses similar self-mailing method as Melissa, but also sends stored passwords and usernames from the infected machine back to the author [58],
- 2000, mass Distributed Denial of Service (DDoS) attacks—brought many high profile web sites brought off line [58],
- 2001, Code Red—exists in memory rather than infects files (Emm 2004) and coordinated an attack against the White House web site at a predetermined date [58],
- 2001, Nimda—demonstrates a sophisticated combination of multiple methods of infection and propagation [58],
- 2002, Klez—attempts to disable virus scanners and fills files with zeros [58],
- 2003, Slammer—astonishes experts by infecting 90% of its vulnerable hosts within ten minutes [13] and hundreds of thousands of computers in under three hours to be considered the fastest spreading computer worm ever [58], and
- 2004, MyDoom—the fastest spreading email worm to date [58].

A disturbing new trend links the two greatest Internet toxins: malware and spam. There are indications that spammers and hackers have begun to collaborate [73]. Spammers can

help spread email viruses for hackers. Hackers can sell spammers computers that are 0wn3d[1].

4.2 The Malware Network Environment

The topography of the Internet, particularly the World Wide Web, has been identified as a scale-free network [7][26]. Scale-free networks are characterized by rapid growth and preferential attachment [6]. These characteristics create an environment in which malware can thrive.

The continuous growth of the Internet extends virus lifetimes [71]. Preferential attachment refers to the creation of key hubs with many connections. As a result, a virus that reaches a few strategic points is likely to be able to spread to all vulnerable nodes [36]. Additionally, high error tolerance in scale-free networks makes them particularly vulnerable to attack [2].

Pastor-Satorras and Vespignani show that epidemic threshold on the Internet is zero, which means that malware can spread at the rate for which they are designed [71]. Software homogeneity and high-bandwidth connections also facilitate worm attacks [62].

4.3 Risky Behaviors that Contribute to Malware Propagation

The most basic malware-associated risk is connecting to the Internet. Vulnerable computers can be identified and infected without any user action other than setting up the connection.

Specific threats evolve with specific malcode, but, in general, any behavior that exposes a computer to outside programs or scripts puts that computer more at risk. Email remains the most popular propagation tool for malware [56]. Opening email attachments or messages formatted in HTML open a computer up for attack.

Other activities such as allowing web sites to run embedded scripts and participating in peer-to-peer file sharing networks also increase the likelihood that a computer will be

[1] "owned" as expressed in the l33t vernacular of hackers and geeks

infected. Risk generally increases with the number of protocols applied, contacts corresponded with, web sites visited, and application used.

4.4 Behaviors that Mitigate Malware Propagation

Although there is no overwhelming solution to malware at this time, there are behaviors that can mitigate the threat, particularly when widely applied. Even modest prevention actions have been shown to be effective at slowing worm spread [79]. Below are some examples of risk mitigating behaviors that can be taken by individuals. A public health approach would, in part, focus on encouraging such behaviors throughout the population.

4.4.1 Disconnect

Although some infrastructure threats may have repercussions in the physical world, staying off-line is the only certain way to avoid receiving malware or helping to distribute it. This is the only risk mitigating that does not have a hack. A related, but less extreme mitigation technique is to turn off the computer when it is not in use, particularly if it is connected to an "always on" broadband connection.

4.4.2 Use Anti-Virus Software

Virus scanners are an old prevention mechanism but a useful one. The primary weakness of virus scanners is that they can only identify viruses they know about. As a result, their libraries need to be updated frequently in order to continue to protect against emerging threats. Schneier recommends downloading updates at least every two weeks or when a new virus is in the news [76].

4.4.3 Use a Personal Firewall

A network firewall prevents unauthorized access to the network. A personal firewall prevents unauthorized access to a single computer. Most users do not have any need to allow any incoming access to their computers. Blocking this capability helps to prevent malicious access.

4.4.4 Keep Software Current

Most malware obtains control by exploiting vulnerabilities in other software. Software manufacturers try to prevent exploitation by releasing patches to fix known vulnerabilities. Applying patches to software (particularly operating systems and

browsers) when they are released makes a machine impervious to attacks on that vulnerability. Furthermore, some malware can exploit vulnerabilities even in software that is not used. As a result, users should uninstall software that they do not need.

4.4.5 Set Secure Configurations

Most software is defaulted to overly permissive configurations to ensure that a new user is able to do whatever he or she wants. Avoiding user frustration is an admirable goal, but those users then need to restrict the configuration to prevent exploitation of unneeded services. Internet-facing software such as browsers and email clients are most at risk. Schneier offers a number of recommendations for Internet software configurations [76].

5 History and Trends in HIV/AIDS

In this section, I give an overview of HIV/AIDS with a focus on details that are significant to the establishment of the analogy to malware.

5.1 A Brief HIV/AIDS History

HIV (human immunodeficiency virus) is a virus that is spread when infected blood, semen, or vaginal secretions come in contact with the broken skin or mucus membranes of an uninfected person [94]. Additionally, HIV can be passed from an infected mother to her child during pregnancy, delivery, or breast feeding. The virus is fragile and cannot survive at room temperature for more than a few seconds, which is why it does not spread through casual contact [80].

A person may carry HIV without symptoms, or the virus may attack the immune system leaving the body extremely vulnerable to other disease. There is no formal delineation to define when a simple HIV infection has escalated to the point of being labeled advanced HIV disease or AIDS.

It is not known specifically when AIDS began. The earliest known case of HIV was found in a stored blood sample from 1959, but scientists estimate that the first HIV case probably occurred in the 1930s [80]. Numerous cases may have been misdiagnosed many years prior to the beginning of the acknowledged epidemic. The release of a significant CDC report in 1981 is generally considered to be the beginning of AIDS

awareness in the United States [48], despite the fact that the report did not mention a disease by that name but only chronicled unusual cancer and pneumonia cases among young gay men in New York and California.

Singhal and Rogers identify three phases of the epidemic spread of HIV/AIDS: urban beginnings, breaking out of high risk populations, and interiorization [80]. "Urban beginnings" refers to when the virus first emerges within high risk groups—commercial sex workers (CSWs), intravenous drug users, or men who have sex with men (MSMs)—in large cities. Next, the virus breaks out of these high risk populations such as when a husband who has sex with CSWs infects his wife. Finally, because of travel, the virus emerges even in more populated areas, which is referred to as "interiorization." These phases get repeated as infected individuals carry the virus to new geographic locations.

As the disease began to spread in the early 1980s, the main challenge was to determine how the disease was being spread. At that time theories about transmission were uncertain, but the disease seemed to be specific to gay men. However, cases of AIDS began to emerge in non-gays, notably in recipients of blood transfusions, which caused concerns about the blood supply [48].

The epidemic was given the name AIDS, for Acquired Immune Deficiency Syndrome, in English with corresponding names and acronyms in other languages. The use of the term "syndrome" indicates the lack of understanding of the cause of the disease at that time.

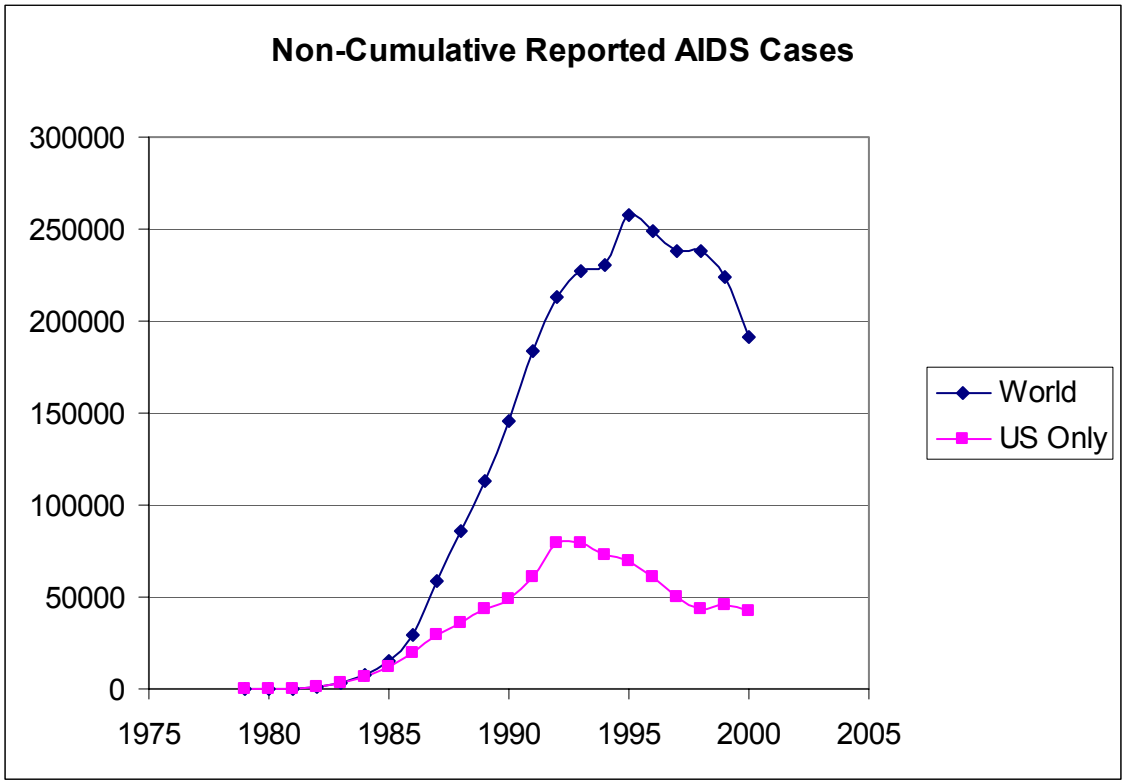
By 1982, AIDS had already been identified in a variety of countries in North America, Europe, and Africa, and it continued to spread [94]. Once the virus now called HIV had been identified, it could be better studied. Scientific and case evidence allowed public health professionals to better identify what did and did not spread HIV. A variety of public awareness campaigns were launched.

Public awareness of AIDS was bolstered by the death or infection of celebrities and likable activists [80]. In the United States (and to a lesser extent elsewhere), the death of

actor Rock Hudson in 1985 helped to increase AIDS awareness, although his sexual status allowed people to still dismiss the disease as a gay issue. Ryan White, a young boy who contracted AIDS from a blood transfusion and who died in 1990, was seen as an innocent victim of the disease. It wasn't until 1991 when Magic Johnson announced his HIV-positive status that the epidemic was given a major heterosexual face. Other countries have their own popular activists such as Nkosi Johnson in South Africa and Ashok Pillai in India.

The HIV/AIDS epidemic continued to grow until the mid-nineties when the trend began to turn around as shown by non-cumulative HIV/AIDS Cases reported to the WHO (see Figure 1). Although the overall trend is in decline, certain regions of Latin America, Asia, and Africa still report increasing numbers of new HIV/AIDS cases each year. In the United States, the number of cases started to decline in 1994, but the trend leveled out in 1998.

Figure 1



The epidemic has been constantly evolving, which has necessitated evolution in the strategies to combat it. For instance, initially HIV was predominantly found in gay men, so women did not seem at risk. Now, women are being infected with HIV at a faster rate than men [80].

5.2 The HIV/AIDS Network Environment

Like malware, HIV/AIDS has been described as propagating in a scale-free network, specifically the network of human sexual interaction [7][26][60]. Arguments against using the scale-free model have been widely criticized [44]. As a result, it is reasonable to assume that the network through which HIV/AIDS spreads exhibits the prime characteristics of a scale-free network: preferential attachment and rapid growth.

As noted by Singhal and Rogers, the epidemic spreads through a small number of centralized nodes [80]. This is the concept of preferential attachment, which indicates that there are a few highly-connected persons who escalate the epidemic by passing the virus on to many partners. Liljeros et al. attribute the preferential attachment in human sexual networks to factors including "increased skill in acquiring new partners as the number of previous partners grows, varying degrees of attractiveness, and the motivation to have many new partners to sustain self-image" [60]. The best opportunity to control an epidemic is to prevent it from infecting those key nodes [80].

The characteristic of rapid growth is evident in the trend of AIDS cases. Rapid growth is possible due to the combination of highly connected persons and those who serve as "bridges" between high-risk groups and the general population. How rapidly the disease can spread within a population was demonstrated to a class of 20 students at the University of New Mexico with an AIDS game. Each student was given a glass of water and a spoon. One glass contained salty water; the other water was fresh. Students would randomly pair off and exchange three spoonfuls of water. Despite the random joining, all the water was salty in six cycles [80].

5.3 Risky Behaviors that Contribute to HIV/AIDS Propagation

Activities that result in an exchange of bodily fluids put persons at risk for contracting the HIV virus. The activities resulting in infection are most frequently sexual (anal sex, vaginal sex, oral sex), medical (blood transfusions), or intravenous drug related (sharing of needles). Although each of these behaviors has inherent risk of infection, the associated risks amplify with frequency of the behavior and failure to use available methods of protection (see subsection 5.4).

Factors contributing to the likelihood that one of the participating parties is infected also increase risk. For example, a person with a single sexual partner is put at greater risk if that person's partner is highly promiscuous. Not learning about one's own or one's partner's HIV status also increases the risk of spreading the infection.

5.4 Behaviors that Mitigate HIV/AIDS Propagation

The most effective way to avoid sexual transmission of HIV/AIDS is to abstain from sex. However, as observed by Kippax and Race, people are more likely to make their activities safe by "modifying and building on them, not by abstaining from or eliminating them" [57].

Limiting sexual partners will lower the risk of spreading HIV. Testing so that individuals are aware of their statuses can also help to prevent propagation, if knowing one's status motivates behavioral alterations.

Condoms help to spread HIV during otherwise risky behaviors by preventing the virus from being able to pass from one body to another. Additionally, a number of anti-HIV topical microbicides, substances which can prevent viral infections, are under development [91]. Vaccination is a preventive mechanism that has been effective for other diseases, but one has not yet been developed for HIV, although much research is being done in this area.

Knowledge of these individual behaviors is disseminated, in part, via public health initiatives such as those described in the next section.

6 Public Health Approaches

It has been noted that a socially informed public health approach is more successful than pure epidemiology [57]. In order to discourage the above-described risky behaviors and encourage preventive ones public health organizations use a number of awareness, education, and intervention techniques. Significant examples of these and their notable characteristics are described in this section.

6.1 Some General Public Health Techniques

Whereas an independent doctor is focused primarily on the health of individual patients, public health practitioners look to minimize the impact of disease on the general population. A significant portion of public health efforts are spent on preventive initiatives. Money spent on prevention has been found to save more lives than money spent on treatment [80].

6.1.1 Screening

Testing for infection before symptoms arise, referred to as screening, is a basic public health tool [17]. Screening not only helps to provide individual treatment as early as possible but also to identify and monitor outbreaks of disease. Early recognition is important since, as Singhal and Rogers note, "Waiting on an epidemic is costly" [80].

6.1.2 Partner Notification

Notifying the partners of HIV-positive individuals helps to prevent the further spread of HIV by allowing for early diagnosis of infection and creating opportunity to emphasize safer behaviors. This procedure has the benefit of tracing both new infections (downstream) as well as infection sources (upstream). Many states and some cities require notification as a matter of law.

There are three main strategies for partner notification [17]:

- Provider referral—The clinician notifies partners;
- Patient/Client referral—The infected individual agrees to notify partners; and
- Contract referral—If a partner has not come in for counseling by a certain date, the health department makes contact.

6.1.3 Message Evolution

The HIV/AIDS epidemic has evolved over the years, so programs to fight the epidemic must be able to adapt [80]. The ABC methodology—choosing abstinence, being faithful, and using condoms—or subsets of it were the only HIV/AIDS preventions promoted for a long time. Now, public health officials are working to apply enhanced understanding of sexual networks as well as technological advances in developing vaccines and microbicides that better serve the needs of "newly" at risk populations. Through this advanced public health focus, specific communications methods and messages have evolved for different segments of the population and the needs of the times.

6.1.4 Education

The inclusion of heath and sex education classes in school curricula enables the introduction of public health concepts to young people. This had been an established practice prior to the emergence of HIV/AIDS. The epidemic inspired many schools to modify their health education content to address risky behaviors that help to spread HIV/AIDS. Subsection 6.2.3 describes one program designed to bring the HIV/AIDS message into schools.

6.1.5 Intervention

Using well-structured interventions to replace risky behaviors with more protective ones is particularly useful in the control of the spread of disease. Singhal and Rogers state that one of the significant advantages of interventions is that they have the potential to act upstream of the epidemic [80]. The proactive nature of interventions can reduce HIV prevalence and "relatively risky behaviors" up to 80 percent.

Some specific interventions are described in the next subsection.

6.2 Analysis of Selected HIV/AIDS Public Health Interventions

I reviewed a number of HIV/AIDS public health initiatives. Most of those recorded here are interventions and techniques that have shown significant levels of effectiveness. Others are emergent methodologies that represent newer ways of thinking but have not yet generated evidence to prove their effectiveness. Each of these programs is described below.

6.2.1 Condom Skills Education

Mere knowledge of condoms as protection is insufficient. People need to know how to properly select and use condoms. One CDC approved intervention uses a single 30-minute session to educate heterosexual adults about condom use [16]. The first 15 minutes consist of a presentation showing various condoms, a discussion about the proper use of condoms, and a demonstration of how to put on a condom. This is followed with a 10 to 15 minute question-and-answer session. After the intervention, participants indicate significant reductions in risk behaviors compared to their baselines prior to education.

Notable Characteristic: Proper use/skill building.

6.2.2 Be Proud! Be Responsible!

One successful youth intervention called "Be Proud! Be Responsible" targets African-American male adolescents [16]. The program consists of one five hour session that uses videos, games, and exercises to teach about risky behaviors and the correct use of condoms. The participants report more frequent condom use and fewer sexual partners than the comparative adolescent group.

Notable Characteristics: Proper use/skill building, use of games.

6.2.3 Get Real about AIDS

"Get Real about AIDS" is an intervention designed for incorporation into high school curricula [16]. Teachers from participating schools are trained to present material on general HIV knowledge, specific risks to teens, condom use, and social skills development to prepare students for high-risk situations. Participating students report fewer sexual partners and more frequent condom use than students in non-participating schools[16].

Notable Characteristics: Proper use/skill building, community settings, attention to personal/group risk.

6.2.4 Project RESPECT

Project RESPECT is an inner-city counseling program given at STD clinics [16]. The counseling occurs over four sessions—or two sessions for the abridged version. The sessions include assessing personal risk and discussing condom use attitudes. On the third session of the full-intervention or the second session of the brief-version, HIV test results are received and discussed. Participants indicate significantly higher condom use than comparison group. 30% of fewer participants had new STDs as compared to participants in the comparison group. Adolescents showed higher STD reduction than older participants.

Notable Characteristics: Attention to personal/group risk, awareness of status/available testing, repeated contact.

6.2.5 Cognitive-Behavioral Studies Training Group

The Cognitive-Behavioral Skills Training Group is an intervention geared toward inner-city women [16]. It consists of 4 weekly group sessions of 90 minutes each. The content includes general risk awareness and avoidance but also includes statistics focusing on prevalence in women and the possibility of encountering an infected partner. Role-playing is used to identify ways of discussing condoms and HIV/AIDS concerns with potential sex partners. Skill building is emphasized through condom demonstrations and practice to get the women desensitized to the embarrassment of using condoms. The woman who participated reported significantly greater increases in condom use and greater decreases in frequency of unprotected sex than the control group.

Notable Characteristics: Attention to personal/group risk, proper use/skill building, repeated contact.

6.2.6 Healthy Highways Project

The Healthy Highways Project targeted truck drivers in India [80]. The program struggled until staff members found a message that was meaningful to the truck drivers: "Sex without condoms is like driving without brakes." Keeping healthy for their families at home was used as a motivator. Because the population was not culturally

homogenous, materials were produced in several languages with non-ethnically specific faces and clothing. The program began having an impact but its administration was decentralized after which the program lost momentum and disappeared.

Notable Characteristics: Attention to personal/group risk, community setting.

6.2.7 Video Opportunities for Innovative Condom Education and Safer Sex (VOICES/VOCES)

Video Opportunities for Innovative Condom Education and Safer Sex (VOICES/VOCES) is a video-based intervention to combat HIV/AIDS and other STDs [16]. In a single 60-minute session, participants view a gender- and culturally-specific 20-minute video then interactive discussions reinforce the messages from the video. Participants share problems that they have experienced with condom use and discussed alternatives. Participants had a significantly lower rate of new STD infection than the comparison group.

Notable Characteristic: Attention to personal/group risk, use of real life examples/true stories.

6.2.8 Combined Education and Testing

Another successful intervention pairs HIV testing with education [16]. The education portion consists of a pamphlet and short video describing HIV risks, safer sex practices, and condom use. A counseling session allows for one-on-one discussions with a physician. Participants return two weeks later for their test results and counseling appropriate for the resultant serostatus. Participants in this intervention report fewer occurrences of unprotected sex than those in a control group receiving HIV education without testing.

Notable Characteristics: Awareness of status/available testing.

6.2.9 The Serostatus Approach to Fighting the HIV Epidemic

The Serostatus Approach to Fighting the HIV Epidemic (SAFE) was established by the CDC in 2001 [46]. The goal of SAFE is to focus transmission prevention strategies on

already infected persons, which contrasts with most pre-existing programs that target those "at risk" but not yet infected. The goals of SAFE are as follows:

- Create serostatus knowledge through available testing,
- Increase participation in available programs by linking prevention and care services,
- Ensure a high quality of available care,
- Monitor adherence to therapy regimens, and
- Intervene to encourage individuals to adopt and sustain risk mitigating behaviors through programs designed specifically for the need of sexually-active HIV-positive persons.

Notable Characteristics: Awareness of status/available testing, proper use/skill building, focus on infected persons, repeated contact.

6.2.10 Advancing HIV Prevention: New Strategies for a Changing Epidemic

In the response to the leveling out of HIV infection rates in the United States, the CDC has embarked upon a new strategy called "Advancing HIV Prevention: New Strategies for a Changing Epidemic" [18]. This program focuses on early diagnosis of infection by applying four strategies:

- Include HIV testing in routine health care (particularly for persons identified as being at risk),
- Allow for HIV testing outside of medical settings (such as in correctional facilities or partner counseling services),
- Increase interactions with HIV patients and their partners to increase partner notification and to work on modification of risk behaviors, and
- Decrease perinatal HIV transmission through increased testing of mothers.

The implementation of these approaches is assisted by the availability of new rapid-result HIV tests [17].

Advancing HIV Prevention: combines the work of two decades of fighting HIV/AIDS with new strategies based on proven approaches used to fight other infectious diseases.

In order to meet its goals, the program prompts collaboration between the CDC, other public health organizations, and medical professionals. This program is in its early stages and little is known of its effectiveness.

Notable Characteristics: Awareness of status/available testing, automatic testing, focus on infected persons.

6.2.11 STOP AIDS Program

The STOP AIDS program was a very early intervention founded by gay San Franciscans [80]. Peer focus groups researched current levels of knowledge and then sought to educate the participants. Each session was led by a well-respected, HIV-positive leader. At the end of the sessions, participants were recruited to volunteer. The program was well-designed based on proven sociological theories of small group communication and diffusion of innovation. The use of volunteers kept costs low. The STOP AIDS program made San Francisco one of the first cities in the world where interventions were given credit for a significant decrease in new HIV infections.

Notable Characteristics: Peer leadership, attention to personal/group risk.

6.2.12 Popular Opinion Leader (POL)

In the Popular Opinion Leader (POL) intervention, bartenders are asked to nominate persons who are "popular with others" [16]. These people then become "popular opinion leaders." The first part of the program uses four 90-minute sessions to train the leaders about HIV education and communication strategies. In the second part of the program, each opinion leader has at least 14 conversations about HIV/AIDS risk reduction with peers met in bars. The program is successful at significantly reducing unprotected anal sex amongst the participating population.

Notable Characteristics: Peer leadership, community settings.

6.2.13 Mpowerment Project

The Mpowerment Project is a multi-disciplinary intervention for young gay men [16]. The program uses "fun and interactive" peer-lead activities to draw people into more

formal outreach events. The program content addresses safer sex concerns and skills. The message is reinforced by a targeted media campaign. Participants are found to have significantly reduced their unprotected anal sex activities over members of the comparison community.

Notable Characteristics: Peer leadership, proper use/skill building, community settings, repeated contact.

6.2.14 AIDS Community Demonstration Project

The AIDS Community Demonstration Project recognizes that behavioral change occurs in stages [16]. The program uses stories about successful risk-reduction strategies employed by others in the community in order to remove stigmas about protection techniques. Peer volunteers are trained to perform the intervention, and it is dispatched in general community settings. Findings show that the members of the intervention communities show significantly more condom use than those in comparable communities.

Notable Characteristics: training in stages, use of real life examples/true stories, peer leadership.

6.2.15 Entertainment-Education Strategy (*Twende na Wakati*)

There have been a number of programs that sought to educate through entertainment media. These are more than "very special episodes" of otherwise non-issues based programming. These are entire programs created for the purpose of education and dispelling myths. Examples of this include *Soul City* in South Africa, *Malhacao* in Brazil, and *Twende na Wakati* in Tanzania.

Twende na Wakati is arguably the most effective example entertainment-education [80]. It was a radio soap opera in Tanzania that broadcast twice a week. The show's formula for success included these key factors:

- Conduct formative research to determine how the show will be responded to and to identify the knowledge gaps that need to be corrected;

- Create a values grid of 57 facts to incorporate into storylines;
- Convey topics through positive, negative, and transitional role models; and
- End each episode with a brief (20-30 second) epilogue that gives a summary statement from a credible source.

The research that went into designing the show included 4800 personal interviews and 160 focus groups. A highly experienced creative team worked on the show.

Three types of characters were written into every story. Positive role models were shown as being ultimately rewarded for their good behaviors. Negative role models were punished. Additionally, there were transitional characters whose values changed. A change from bad to good resulted in reward, while a turn for the worse resulted in some sort of punishment. Mkwaju, the name of a negative role model, became part of popular vernacular. When a man boasted of sexual exploits people would say "Don't be a Mkwaju!"

In 1994, 72% of *Twende na Wakati* listeners said that they had adopted AIDS protective behaviors because of the show, which increased to 82% in the second year of broadcast. Research also found that people would discuss issues from the show with their peers.

Notable Characteristics: Use of entertainment, use of real examples/true stories, community settings, repeated contact.

6.3 Other Methods of Prevention

There are some other mitigation techniques worthy of note, although they are not generally accepted public health strategies. I describe some of these here.

6.3.1 Ugandan Model

Since the early 1990s, Uganda has had a 70% decline in HIV/AIDS that is generally attributed to a 60% reduction in "casual" sexual partnerships [85]. Other trends include delay of first sexual activity as well as an increase in condom usage. These trends are distinct from other African countries. Although there is some disagreement about the cause of these trends, there is strong evidence supporting the significant contribution of

social-based learning in Uganda. Personal networks were the main way that people learned about HIV/AIDS and a high majority of people directly knew someone with the disease or who had died from it. This created a "credible communication of alarm" and a "rational fear," which were then supported by formal public health efforts.

Notable Characteristics: Cultural differentiation, peer leadership, community setting, attention to individual/group risk.

6.3.2 Thai Model

Thailand developed a successful HIV control program, although they delayed the start of the program until the disease had a significant presence in the country largely due to an active commercial sex trade [80]. Mechai Viravaidya was a cabinet level official who was asked to lead HIV/AIDS prevention initiatives. Viravaidya's active role led to his being nicknamed the "Condom King" or "Mr. Condom."

The Thai campaign features heavy media coverage, education starting in the first grade, and condom availability. Commercial sex workers are the main target. One campaign called "cops and rubbers" involved police officers distributing condoms in red light districts. These efforts have significantly decreased the rate of new HIV infections.

Notable Characteristics: Strong leadership, government manifest, attention to personal/group risk.

6.3.3 Negotiated Safety

Negotiated safety is a social phenomenon rather than a formal public health strategy. It has been observed as an emergent response to the HIV epidemic amongst sexually-open or serially-monogamous individuals. I describe it here because it demonstrates the type of behavioral modifications that humans are willing make their one initiative.

Negotiated safety is the idea that, rather than choosing monogamy or consistent condom use, HIV-negative partners in an ongoing relationship(s) will cease using condoms with each other contingent on a mutual agreement to safe sex outside the regular

relationship(s). Although the agreement may be to not have sex with other partners, it is not limited to that.

As noted by Kippax and Race, the effectiveness of negotiated safety is yet to be empirically proven; however, it is likely to provide a comparably higher level of safety than total disregard for condom use [57]. The effectiveness in each case will be contingent on partners being aware of their HIV statuses and not betraying the established trust relationships.

Notable Characteristics: Self-adoption, minimizing risk behaviors rather than eliminating them.

6.3.4 Quarantine

Most cultures look at quarantine as a violation of individual rights, but it may be effective at preventing new infections. In Cuba, the government performed massive blood-testing and isolated persons with HIV infections in internment camps called sidatorios, named based on SIDA, the Spanish acronym for AIDS [80]. Cuba now has a relatively low level of HIV infection, which has been inferred to be a possible result of the quarantine.

Notable Characteristics: Minimize contact.

6.3.5 Impact of the Press

As noted above, media coverage played a significant role in Thailand's efforts to control HIV. In the United States, the spread of HIV/AIDS was partially controlled by bringing the issue to the public sphere. In the early days of the outbreak it was difficult for the press to comprehensively cover the disease because much of the terminology necessary to accurately describe how the virus spread was deemed too provocative for publication. The media frenzies surrounding the deaths of Rock Hudson and Ryan White created awareness. As news coverage increased so did public concern [80].

Notable Characteristics: General communication channels.

6.4 Common Elements

Review of the above-described public health approaches reveals a number of common elements:

- Proper Use/Skills Building,
- Attention to Personal/Group Risk,
- Community Setting,
- Repeated Contact,
- Awareness of Status/Available Testing,
- Peer Leadership,
- Use of Real-Life Examples/True Stories,
- Focus on Infected Persons, and
- Use of Games/Entertainment.

Figure 2 shows a summary of which interventions use which elements.

Figure 2

	Condom Skills Education	Be Proud! Be Responsible!	Get Real about AIDS	Project RESPECT	Cognitive-Behavioral Skills Training Group	Healthy Highways Project	VOICES/VOCES	Combined Education and Testing	SAFE	Advancing HIV Prevention	STOP AIDS	Popular Opinion Leader (POL)	Mpowerment Project	AIDS Community Demonstration Project	Entertainment-Education
Proper Use/Skills Building	■	■	■		■				■				■		
Attention to Personal/Group Risk			■	■	■	■	■				■				
Community Settings			■			■						■	■		■
Repeated Contact				■	■				■				■		■
Awareness of Status/Available Testing				■				■	■	■					
Peer Leadership											■	■	■	■	
Use of Real Examples/True Stories							■							■	■
Focus on Infected Persons									■	■					
Use of games/entertainment		■													■

6.4.1 Proper Use/Skills Building

Rather than simply describing risk and ways to mitigate or avoid that risk, a number of interventions go one step beyond to instill in the participants the practical skills to execute risk mitigating strategies. It is known that available condoms will not necessarily be used [80]. Using condoms improperly may create a false sense of security. As a result, some programs teach the proper use of condoms rather than just recommending their use. Other programs use role-playing to provide participants the social skills to avoid or manage risky situations with would be sexual partners. This makes the participants more comfortable with using condoms and discussing safe sex. This comfort level makes them more likely to use preventive behaviors in real life.

6.4.2 Attention to Personal/Group Risk

Instead of repeating generic HIV/AIDS risk awareness information, some programs make a concerted effort to focus on the risks specific to the specific audience of the intervention. This allows the program to focus on the risky behaviors most likely to be faced by the participants.

Focusing on the risk to a specific group is particularly useful if the individuals do not perceive their group to be high risk. By learning about HIV/AIDS prevalence in people like themselves the threat to the participants becomes more concrete. (This relates closely to the characteristics of peer leadership and use of real life examples/true stories.)

6.4.3 Community Setting

Although many of the programs require participants to go somewhere to seek out participation, like to a clinic, others initiate interventions in places that at-risk persons already congregate, such as gay bars or at school. This has the advantage of being able to push the message out even to people who are not self-motivated enough to seek out the information. Bringing the message to where at risk individuals are increases the likelihood that they will hear it.

6.4.4 Repeated Contact

Singhal and Rogers note that repeated contact is usually necessary to change an individual's behavior [80]. As a result, it is beneficial to design programs that interact

with participants during multiple sessions or that repeat messages through multiple channels. Although it may be more difficult to motivate individuals to return on multiple occasions, the repetitive message is more likely to create lasting changes in individual behaviors.

6.4.5 Awareness of Status/Available Testing

A number of the programs emphasize making sure that people know their HIV status and that testing is readily available. Early diagnosis is important not only to treat the infected individual but also to begin that person's behavior modification to prevent the further spread of the disease. By making testing readily available and making people aware of their statuses, necessary actions can be taken sooner rather than later.

6.4.6 Peer Leadership

Some of the programs rely on peer leadership for some or all of the material communication. Peer educators have a perceived credibility to the target audience [80]. Participants are more likely to take messages seriously when they come from someone with whom they can relate rather than an unfamiliar "expert."

An extension of peer leadership is the involvement of a celebrity role model. After Magic Johnson announcing his HIV status, the National AIDS Hotline received four times its normal call volume [80]. The day after the announcement had 19 times the usual call volume with 118,124, and 1.7 million calls were received in the 60 days that followed. Many of these inquiries were from young African-American males asking about how to get an HIV test.

6.4.7 Use of Real-Life Examples/True Stories

Although most programs discuss general statistics and facts, some use very specific examples in order to illustrate either HIV/AIDS risks or how other people have been able to successfully change their behaviors. Much like peer leadership and highlighting personal or group risk, realistic and true examples make risk more understandable than abstract concepts alone.

6.4.8 Focus on Infected Persons

Some programs specifically focus on changing the behaviors of those who are already infected with HIV in order to prevent further spread of the virus. With improvements in anti-retroviral treatments, many HIV positive individuals feel good enough to return to normal life activities, including sex [25]. It is important to not let the treatments make people forget about the virus, and the need to avoid risky behaviors that would spread the virus to others. Similar to the idea of promoting status awareness, programs that focus on infected persons prevent further spread of HIV by encouraging safer behaviors amongst those who are known to be a risk to others.

6.4.9 Use of Games/Entertainment

Using games and entertainment to convey messages of behavioral change can have a similar effect as bringing the message to a community setting. If the media is interesting and enjoyable enough as entertainment it will draw in an audience even if they might otherwise not been motivated to seek education on HIV/AIDS.

6.5 Measures of Success

Before conducting an intervention, the CDC recommends that the program developers compare the characteristics of the proposed program with 20 checklist items [16]. The checklist items highlight common factors of successful interventions in the categories of intervention, implementation, organization, and consumer/participant. All the checklist items are included in Appendix A.

Particularly in their initial implementations, public health interventions are often organized as "field experiments." This means that participants are randomly selected and their behaviors are compared to those of a control group selected from the same population [80]. This creates a basis for comparison to determine the effectiveness of the initiative.

In order to be able to judge the effectiveness of a program after completion, Singhal and Rogers recommend five keys to meaningful evaluation of intervention effectiveness [80]:

- Interventions should be internally and externally evaluated using both quantitative and qualitative methods.
- Communities should provide feedback on their perception of program success levels and recommend criteria for measuring social change.
- Evaluation data should be collected before, during, and after the program.
- Evaluation procedures need to be timely, relevant, and cost-effective per the specific intervention. The authors recommend that 10% of the total budget be focused on evaluation.
- Evaluations should result in direct evidence about the role of communication programs.

Some programs, such as the Advancing HIV Prevention, specify indicators for implementations to monitor or risk losing funding [17].

7 Exploring the Analogy

Malware threatens the continued viability of a general use Internet. Even users who vigilantly protect their own systems are likely to be affected by malware attacks. Existing solutions have been minimally effective causing at least one author to decry the parade of band-aid fixes for viruses and request a new paradigm [72].

Meanwhile, HIV/AIDS continues to spread to many victims regardless of demographic or geographic differences. However, worldwide infection rates are overall on the decline. This is attributable, in part, to many well-organized public health initiatives.

It is my goal to explore the nearly quarter of a century of public health strategies used to combat HIV/AIDS in search of lessons learned and best practices that may be applicable to controlling the spread of malware. Because most HIV/AIDS methodologies focus on education, awareness, and behavior modifications, the analogous strategies for malware will mostly be in the same categories. However, there may be concepts that can also be extended to technology solutions.

7.1 Overview of Malware and HIV/AIDS Analogy

In order for solutions to be analogous, the under-lying problems need to have analogous attributes. I see a number of analogous attributes in Malware and HIV/AIDS propagation. A summary of these attributes appears in Figure 3.

Figure 3

Summary of Analogous Attributes

	HIV/AIDS	Malware
Geographic Scope	World Wide	World Wide
Epidemic Enabler	Sexual Revolution	Commercialization of the Internet
Infection Conduit	Bodily Fluids	Computer Code
Spread	Contact	Connection
Accelerant	Frequency of Contact	Frequency of Connection
Impact of behaviors	Certain behaviors increase risk	Certain behaviors increase risk
Basic Risk Behavior	Having sex (vaginal, anal, oral)	Connecting a computer to a network, particularly the Internet
Prophylactic Measures	Condom Topical Micobicide	Virus scanner Personal firewall Software patches Secure configurations
Promiscuity	Having many sexual partners (simultaneously or via serial monogamy)	Having an "always on" high speed Internet connection, opening unexpected email attachments, browsing unfamiliar web sites, using numerous protocols and software
Indirect Promiscuity	Sex with a promiscuous partner	The Internet is inherently promiscuous
Extreme Promiscuity	Having multiple or anonymous sexual partners	Peer-to-Peer (P2P) filesharing
Selection of partners	Almost exclusively by choice	A mixture of choice, randomness, and discrimination
Survivability	Slow destruction of host	Slow or minimal destruction of host
Network	Generally scale-free	Generally scale-free
Genealogy	Virus strains traceable	Code snippets traceable

Both malware and HIV/AIDS are worldwide issues impacting many cultures and demographics. The diversity of at risk groups continues to increase in both cases. As noted by Boase and Wellman, both AIDS and malware spread via contact, usually person-to-person, and frequent contact increases the chance of infection [9]. They both spread by the exchange of infected material (malcode or blood) from an infected host to a susceptible one.

Persons infected with HIV may live to spread the infection for many years, which is why some public health interventions focus on changing the behaviors of those who are

already infected [46]. Similarly, computer viruses are usually designed not to destroy their hosts in order to keep the malcode running [54].

Both of these epidemics have been facilitated by ever evolving threats. For HIV/AIDS there have been shifts in what demographic groups are most at risk. For malware the nature of the attacks themselves is constantly changing. The changing nature of these threats requires dynamic approaches to prevention and defense.

7.2 A Comparative History of Malware and HIV/AIDS

One reason to compare analogous systems is to predict future trends of the system being analyzed [15]. In this case, I hope to learn from the past so that we can improve the future. HIV/AIDS has about a decade of head start on the malware epidemic from which we can learn.

The generally cited start of the AIDS epidemic is the release of a CDC publication on the disease in 1981, although the first officially recorded AIDS infection occurred in 1979 and it is assumed that misdiagnosed cases of AIDS began much earlier. The generally acknowledged first significant malware incident is the release of the Morris Worm in 1988, although some viruses and worms had been developed earlier.

Figure 4 shows a timeline of some prevention and treatment milestones in HIV/AIDS history alongside comparable events in malware history where applicable.

Figure 4

HIV/AIDS Date	HIV/AIDS Milestone	Malware Milestone	Malware Date
1981	CDC report recognized as first awareness of AIDS	Morris/Internet Worm	11/2/88
1983	CDC AIDS Hotline Established	Creation of CERT/CC	1988
1985	First blood test licensed by FDA	Commercial anti-virus software released*	1991
1985	First international conference on AIDS, WHO mobilizes against pandemic	Invitational Workshop on Security Incident Response	1989
10/3/85	First Major Public Impact: Death of Rock Hudson, first celebrity known to have died from AIDS	First Major Public Impact: Distributed Denial-of-Service attacks bring down high profile web sites including Yahoo, eBay, Amazon, and Datek.	Feb 2000
1986	US Surgeon General's Report on AIDS, first US govt. statement on prevention		
1987	AZT approved as first drug treatment of AIDS	Commercial anti-virus software released*	1991
June 1988	First US coordinated HIV/AIDS campaign "Understanding AIDS" is mailed to US households and becomes the most widely read publication in the US		
12/1/1988	First official World AIDS Day (sponsored by WHO)	First Computer Security Day	11/30/1988
1991	Beginning of "red ribbon" AIDS awareness campaign		
1994	US CDC launches campaign featuring condoms		
1994	**First year of trend reversal for Reported U.S. AIDS Cases**		
1995	UNAIDS formed to create a global response		
1996	**First year of trend reversal for Reported World AIDS Cases**		
1996	FDA approves first home HIV test		
1996	First White House AIDS strategy released	National Plan for Information Systems Protection	2000
2003	New CDC Initiative, WHO makes AIDS top priority	New Iniatiative: National Strategy to Secure Cyberspace	2003

*The detect and clean features of anti-virus software make it analogous to both AIDS testing and drug treatment.

The Centers for Disease Control and Prevention (CDC) already existed to address public health issues in the United States prior to the emergence of AIDS. In 1983, the CDC AIDS Hotline was established, creating a dedicated public health resource for AIDS. This is analogous to the formation of the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University to address cyber security issues, specifically malware since the CERT/CC was created shortly after the Morris Worm incident.

The licensing of the first blood test for AIDS in 1985 is analogous to the release of commercial anti-virus programs (one of which being Symantec's Norton Anti-Virus) in 1991. Anti-virus software, because it both identifies and cleans, is also analogous to the approval of AZT to treat AIDS.

The first major AIDS conference was held in 1985, and the first Workshop for Security Incident Response was held in 1989. The first World AIDS Day and first Computer Security Day were held actually held on two consecutive days near the end of 1988. (This Computer Security Day continues along with the NCSA Cyber Security Days described in subsection 8.3.)

Both issues have merited formal strategies released from The White House. The first AIDS Strategy was released in 1996. For malware and other information security issues, the National Plan for Information Systems Protection was released in 2000. It was replaced by the National Strategy to Secure Cyberspace in 2003. I describe the impact of the National Strategy in subsection 8.1.)

A significant milestone in HIV/AIDS history is the death of Rock Hudson in 1985. By being the first public figure known to have died from AIDS, Hudson brought attention and sympathy to the disease. Within the computer science community, the Morris Worm raised awareness, but most of the general public did not know about the Internet at that time and would not start using it for at least another five years. The post World Wide Web event that raised some general awareness about the serious potential malware was

the collection of distributed denial of service attacks that brought down many major web sites in 2000.

Looking at the comparative timeline between significant HIV/AIDS awareness milestones and malware awareness milestones reveals a number of gaps of major events in HIV/AIDS history that to date have no malware equivalents. I characterize the differences in three groups: differences in timing, differences in audience/scope, and missing items.

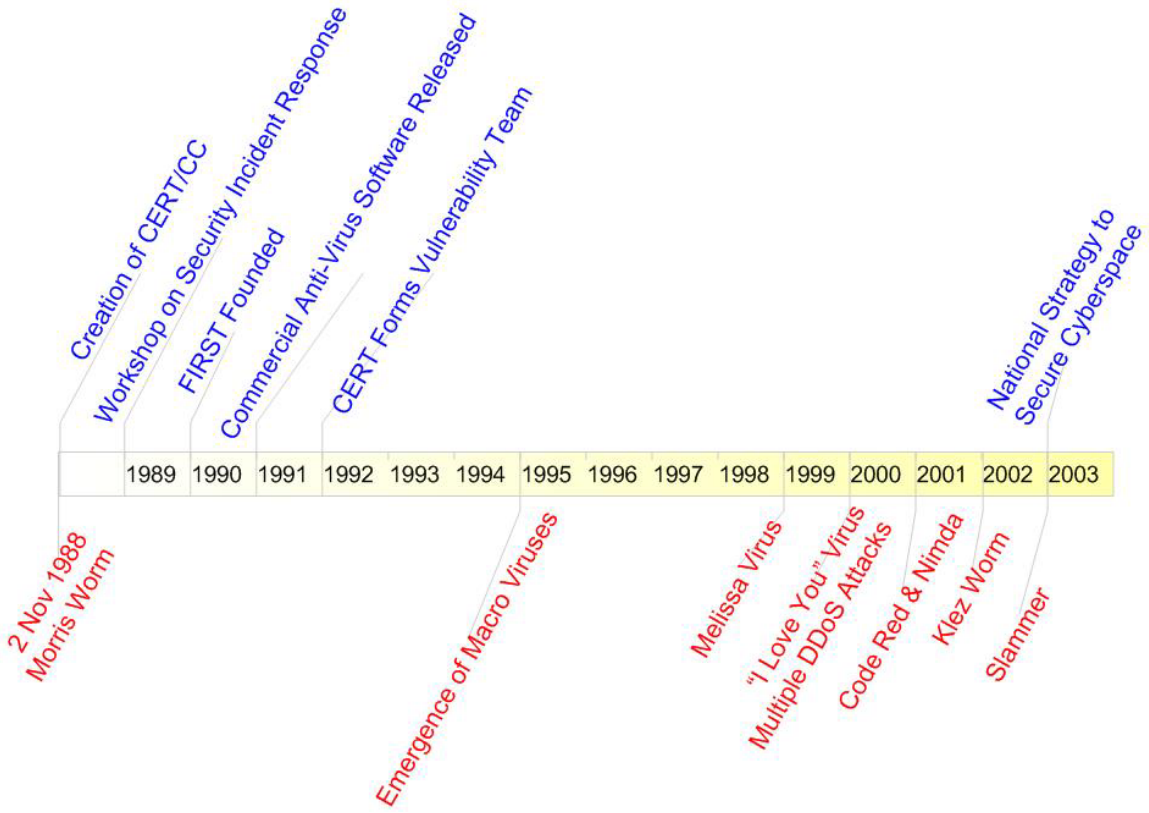
7.2.1 Differences in Timing

What I find most notable when comparing the timelines of HIV/AIDS and malware is that the computer community was quicker with creating a strategic infrastructure to fight malware than the public health community seemed to be to fight AIDS. In the HIV/AIDS side of the timeline, from the acknowledged beginning of the epidemic it took two years to create the CDC hotline; another two years to have a blood test available and have a conference of experts; another two years for the first drug treatment to be approved; and one more year before the first AIDS day to promote awareness. In contrast, the malware timeline achieved equivalents to these milestones within three years of the Morris worm outbreak. In fact, the creation of the CERT/CC and the first Computer Security Day occurred within a month of the outbreak. In the cases of blood test and drug therapy development, part of the lag in response to HIV/AIDS was due to the amount of time required for safety testing and approval. Still, even in the organizational aspects alone, the rapid mobilization to address the malware issue is impressive in contrast to the public health response.

Unfortunately, the momentum seemed to stop at that time as there is a lack of new practical approaches to mitigate malware risks after the release of anti-virus software, whereas the HIV/AIDS timeline depicts constant innovation in the fight against infection. The gap in malware milestones is illustrated in the timeline in Figure 5. Although incremental and theoretical work was being done, no major changes were implemented between 1992 and 2003. This seemingly consistent approach to malware defense is particularly significant since the community at risk for malware dramatically changed in

the mid-nineties as the World Wide Web prompted mass Internet usage. Suddenly, most of the users of the Internet were not computer scientists, yet there was little initiative taken to inform these users of the risks of the network. This demographic change should have sparked new strategies just as HIV/AIDS strategies have change for newly emergent at-risk groups.

Figure 5



7.2.2 Differences in Audience/Scope

Public health initiatives frequently include education and training for medical professionals, but the focus, as the term public health implies, tends to be on getting the message to the public. In the computer security realm most efforts seem to be targeted at computer professionals, not untrained computer users. This is particularly true prior to the World Wide Web, but only recently have there been large initiatives which target the untrained home user. Some of these are described in section 8.

7.2.3 Missing Items

Determining which items from HIV/AIDS prevention strategies have no equivalent in historical anti-malware initiatives depends on how the analogies are drawn. Below are some items from the HIV/AIDS timeline that appear to have no equivalents in computer security strategy. These may serve as inspiration for potential opportunities for malware risk awareness strategies.

Comprehensive Information Distribution

In June 1988, the first coordinated US HIV/AIDS campaign kicked off by sending a publication called "Understanding AIDS" to all US Households. It became the most widely read publication in the US at that time [49]. This scope of this initiative also demonstrates that the issue was a serious priority.

Infuse with Popular Culture

In 1991, the "red ribbon" AIDS awareness campaign began. Among the wearers of the red ribbons were many celebrities, who would even wear their ribbons to high-profile events such as awards shows. This combined the issue with popular culture and carried awareness to the public through general entertainment channels. Although malware concepts periodically arise in movies and television programs, there has not been a clear, pervasive warning that has been widely recognized like the red ribbon campaign.

Campaign featuring Specific Action

US HIV/AIDS cases began to decrease in 1994. This is shortly after the first CDC campaign to feature condoms. Although a number of factors likely contributed to the decline in new infections, the fact that the public was given clear advisement for risk avoidance was a likely contributor. Knowing that there is a threat will have little effect if people do not know how they should change their behaviors. Recently there have been an increasing number of television advertisements emphasizing virus protections, but the AOL/NCSA survey results [4] indicate that even users who have virus protection software will not necessary use it effectively. Additionally, there are other protective behaviors required to avoid current malware threats.

7.3 Analogous Networks of Malware and HIV/AIDS

As mentioned in sections 4 and 5, both AIDS and malware propagate in scale free networks. This means that the patterns of connectivity are similar. The same vulnerabilities to epidemic spread apply.

Additionally, the AIDS and malware epidemics both escalated during unprecedented cultures of growth in their respective networks. For AIDS, it was the sexual revolution of the seventies, and for malware, it was the internetworking boom of the nineties [15]. Such interconnected environments set the stages for mass infection.

7.4 Analogous Risky Behaviors of Malware and HIV/AIDS

Having sex puts a person at risk of contracting HIV/AIDS. Connecting a computer to the Internet puts that computer at risk of becoming a malware host. Without these contacts, both the person and the computer could have a reasonable expectation of safety. However, many individuals choose not to abstain from these practices.

Promiscuity elevates risk in both cases. Having sex with multiple partners either repeatedly or through serial monogamy increases a persons risk of HIV/AIDS infection. Each additional partner increases the chance of infection. Similarly, a computer that interacts with many other computers is more likely to be infected with malware. A computer can connect with another computer in a variety of ways. One popular connection is by browsing a web page that puts the browsing computer at risk for malicious scripts (small programs) running and infecting the system.

Participating in a peer-to-peer (P2P) filesharing network connects a machine to a multitude of unfamiliar and possibly malware-infected computers, which makes this risky behavior most analogous to a sexual network of indiscriminate partner swapping. Staniford et al. give detailed descriptions of the risk of malware propagation in such networks [84].

Although monogamy decreases the risk of HIV/AIDS, a monogamous person whose partner is promiscuous is put at greater risk by connecting them indirectly with numerous

partners. This is true, too, of malware, but the risk is difficult to avoid. The Internet is an inherently promiscuous partner. By placing a computer on-line, other computers can infect it even if no user action is taken to connect with those other machines. A computer on the Internet can become infected with malware even if the user has done nothing but turn it on.

Preventive measures (described in the next subsection) can mitigate the risks of these behaviors, but only if they are used. As a result, not using available protections constitutes another type of risky behavior. In malware, this type of risky behavior frequently occurs amongst people who have not been infected with malware for a while. As observed by Wang and Wang, users are more likely to be vigilant after a previous infection, but this period of vigilance is temporary [90]. Similar behavior is observed among asymptomatic HIV patients [46].

7.5 Analogous Preventive Behaviors of Malware and HIV/AIDS

Both HIV/AIDS and malware infections can be avoided by abstaining from the behaviors that spread them. For HIV/AIDS this would mean not having sex; for malware this would mean not connecting the computer to the Internet. Williams notes that bodies are at risk because of exposure to things in the environment just like a system that would be safe as a stand-alone is vulnerable once connected to the Internet [95]. Many people do not consider abstinence, from sex or the Internet, to be a reasonable option. Still, there are behaviors that can be employed to prevent infection.

Limiting contact will limit risk. For HIV/AIDS being faithful and having a faithful partner will decrease risk. For malware, some ways that contact can be limited include not opening email from strangers, not opening unexpected attachments, and blocking web sites from running scripts unless the purpose is known and trusted. Unfortunately, if a computer has an "always on" Internet connection, it is at risk of contact regardless of how much or how little activity the user initiates. Turning off the computer when not in use prevents extraneous network contacts.

For both HIV/AIDS and malware, using barrier-method prophylactics decreases the risk contact. For HIV/AIDS, this generally means using a condom. For malware, prophylactic measures require a number of steps, some of which are specific to particular activities. Using anti-virus software and keeping it up to date helps to identify malicious code to either prevent or repair a possible infection. Using a firewall prevents unauthorized access to the computer. Adjusting browser and email program settings to prevent programs from launching without user permission will also prevent malware infection.

7.6 Analogical Analysis of Public Health Approaches

Studying the common elements of successful HIV/AIDS public health interventions may provide clues for how to structure malware risk intervention programs. Of course, translating the public health programs to cyber security must be done with care to assure that the characteristics that made the original intervention successful are not lost in the transposition. As the CDC recommends when modifying previously effective HIV/AIDS interventions for use in new environments, "the important thing is to achieve a balance between adapting the intervention to suit local needs and maintaining the core elements and key characteristics that made the original intervention successful" [16].

Below, I describe how the previously mentioned common elements (from section 6) may translate to malware, including some examples of their use.

7.6.1 Proper Use/Skills Building

Frequently, malware awareness efforts take the form of publicizing recent attacks and emphasizing the importance of anti-virus software. Although this sort of awareness serves as a good base or reminder, efforts must be made to ensure that Internet users know how to properly use and update their anti-virus software. Furthermore, risk-mitigating behaviors and net smarts need to be instilled rather than allowing people to believe that anti-virus is enough.

7.6.2 Attention to Personal/Group Risk

Risk tends to be more meaningful when it is personal. Educating persons about malware will have greater impact if people learn about the types of risk that are most applicable to

them as individuals or as specific groups. Malware risk could be personalized on a number of factors including operating system run, other software used, frequency of use, and purpose of use.

7.6.3 Community Setting

Inviting people to education sessions can only be effective if they actually get there. Injecting education into places that the audience already goes can be beneficial because it may reach people who would not be motivated to go out of their way to get the information. Going to an Internet audience need not involve going to a physical place. Conveying risk awareness material through commonly used applications or commonly visited sites could help to inform a wide audience who may not realize that they are at risk. Still, the impact of true person-to-person conveyance should not be totally dismissed as described in subsection 7.6.12.

7.6.4 Repeated Contact

A one time workshop or tutorial will introduce malware topics, but to encourage users to adopt and maintain behavioral changes there needs to be repetition. This is especially important with malware since the threats are ever changing. As with the previous topic, this contact need not be face-to-face. Email updates or pop-up messages can serve as reminders, but enough motivation needs to have already been instilled in the users so they will want to read the messages.

7.6.5 Awareness of Status/Available Testing

Initially, it may seem that malware efforts have focused largely on the awareness of status and available testing because of the emphasis on virus scanners. This is true. However, the importance of knowing one's HIV status is to prevent further spread of the virus. In the malware world, worms can propagate so quickly that they will have already spread significantly if the infection is discovered after the fact. Therefore, anti-virus software can stop the further spread of known malcode, but it will not be effective for the initial attack if it is propagating rapidly.

However, if we look at the analogy as HIV/AIDS weakening the immune system to make the body vulnerable to other infections, then this approach should equate to awareness

and testing of system vulnerabilities not malware infections. Vulnerabilities in this case would be outdated or unpatched versions of software and overly permissive configuration settings. Network administrators use tools to examine for vulnerable hosts on their networks, but there is little emphasis on performing these checks on home computers that are not under administrative control.

7.6.6 Peer Leadership

Some messages are more effective when they come from respected peers rather than an unknown "expert." Peer-based messages are also more likely to use language that is clear to the target audience. Peer leadership could be used to promote malware risk awareness through formal or informal channels. Formal channels might include peer-lead information sessions or discussion groups. Informal channels could include sending informational emails, posting information on a personal web site or blog, or including awareness information as an email signature.

7.6.7 Use of Real-Life Examples/True Stories

Rather than teaching about malware risk through general descriptions and statistics, telling stories to which the audience can relate will allow them to better understand the potential impact of malware in their lives. This is similar to the idea of focusing on personal/group risk. An individual user may not be able to relate to news stories about major ecommerce sites being brought down by an attack, but he may respond to hearing how his neighbor's bank records were compromised.

7.6.8 Focus on Infected Persons

At this time, persons infected with HIV remain infected for the rest of their lives; however, most malware infections can be cleaned from infected computers. As a result, a malware program focused on infected hosts would likely just involve using anti-virus software and other processes required to return the host to an uninfected state. Still, using infection to trigger intervention for behavioral change does have a potential application to malware.

The users of computers that have been infected, particularly those that have been repeatedly infected, are good candidates for risk awareness and behavior modification

education. Anti-virus logs could be one source of information about frequency of infection. This information could be used to send informative emails or invite people to risk intervention sessions. Additionally, interactive training could be incorporated into the anti-virus software, possibly something that runs while a scan or clean-up is being performed.

7.6.9 Use of Games/Entertainment

Computers are already a popular platform for game-playing. Malware awareness could be incorporated into educational video games, particularly when targeting younger demographics. Computer security issues are periodically showing up in the plotlines of television programs and movies, but an educational value seems incidental. It would be interesting to see the impact of an entire program, equivalent to *Twende na Wakati*, designed specifically to convey computer security messages, such as a *Cyber CSI*. The key, as noted by Singhal and Rogers, is to use a high quality creative team so that the resultant feel is that of entertainment rather than education, while still delivering the necessary message [80].

7.6.10 Measures of Success

The public health community creates considerable emphasis on monitoring and measuring the successes of enacted programs. The computer security community emphasizes testing in systems development, but the need to quantify the impact of education and outreach initiative may be less apparent. In order to determine which initiatives, if any, are successful at modifying user behaviors, there needs to be a predetermined set of measurements for comparison. In this way, time and money will not be wasted on repeating ineffectual programs.

7.6.11 Additional Public Health Concepts

The concept of screening has had some equivalent in combating malware in the periodic use of scanning at network perimeters, email servers, or ISPs. Partner notification can have application when malware propagation is traceable; nodes that may have been infected can be identified and hopefully cleaned before too much further damage occurs. Because many children now start using computers from a very young age, the

incorporation of computer security concepts into school curricula could have an impact for instilling base knowledge and awareness.

The concept of message evolution has particular application to malware. Because malware continues to evolve, the threat environment is constantly changing. Behaviors that may have been considered fine a year ago may suddenly become high-risk. Users need to be aware of the most current information.

7.6.12 Person-to-Person Interaction

Almost all of the public health strategies previously described involve some sort of person-to-person interaction. People communicate directly with other people. In the computer security industry there is a temptation to create awareness through technology channels, such as informative web sites, emails, and tutorials. These will frequently not be as effective as direct interpersonal attention.

Harvard University launched an initiative to better protect student computers from viruses [24]. The program consisted of an online and offline publicity campaign and door-to-door distribution of a customized anti-virus suite. The representatives conducting the door-to-door visits were not to install the software; they only explained the importance of the software and distributed the CDs. If a student was not in his or her room, a disk was left with a note summarizing the spiel that would have been given in person. About a third of the estimated computer population began using the custom tools, but it was observed that those who had personal visits were more likely to be compliant than those who received a disk with a note.

7.7 Limitations of the Analogy

Although the similarities between HIV/AIDS propagation and malware propagation create a basis for useful comparison, there are a number of differences between these threats that limit the analogy. Some disanalogous attributes are summarized in

Figure 6.

Figure 6

Summary of Disanalogous Attributes

	HIV/AIDS	Malware
Threat	One disease	Many threats
Propagation Speed	Must wait for human action	Often faster than human action
Method of Attack	Creates a vulnerability that is exploited by other attackers	Various: creates a vulnerability or exploits an existing one
Default Trust Level	Usually start with a low level of trust and defenses get dropped over time	Usually start with highly trusting configuration and need to add defenses
Level of Intimacy	Contact is truly direct	Connections are brokered through routers and hubs.
Social Stigma	High	Low
Fear Factor	High	Low
Fatality	Host cannot be cured (at this time)	Host can be cleaned or rebuilt

One obvious difference between the two sides of this analogy is that the threat of HIV/AIDS is a single disease whereas malware is a combination of many threats with new ones being constantly created. As a result, expertise in preventing malware propagation requires a more general view than for preventing the spread of AIDS. However, in this paper HIV/AIDS has served only as an example of how public health professionals intervene to minimize risky behaviors in the general population. The varied messages about the numerous ways of contracting HIV, when looked at as general strategies, can still be applied to the various risky behaviors associated with malware.

Propagation speed is another major difference between HIV/AIDS and malware. Sexual transmission of HIV/AIDS inherently requires the time it takes to have sex. HIV/AIDS cannot spread more quickly than humans can act. On the other hand, depending on its method of propagation malware, most notably the Slammer worm, has been shown to be capable of hundreds of thousands of computers very quickly. Predictions of a "Warhol Worm" that can infect all susceptible nodes in fifteen minutes, only emphasize the assumption that malware propagation will continue to increase in speed, and that speed is already much quicker than human reaction. As a result, humans cannot be expected to stop a malware outbreak in progress, but they may be able to prevent the outbreak with prior action.

The nature of the HIV/AIDS attack can also be seen as different from that of most malware. HIV/AIDS attacks the immune system then another disease takes advantage of the weakness created [95]. Traditional malware exploits existing vulnerabilities, which would make it more analogous to opportunistic infections rather than HIV/AIDS itself. However, some malware, such as remote access Trojans and back doors, do create new vulnerabilities in the infected system. This level of granularity, however, is of little impact to the intent of user interventions.

With both HIV/AIDS and malware, vulnerability occurs from contact with a contagious partner. As a result, connections need to be made with trust that the person or computer being connected with is not contagious. People tend to have a low level of trust when they meet new people, then they lower barriers to allow greater amounts of trust over time (or because of other influence such as drugs or alcohol). In contrast, computers have a high default trust level because they were originally designed for a single, non-networked user [81]. Barriers, if desired, must be added on top of the inherently open architecture. This is a key underlying technological issue that enables malware propagation and mission fulfillment, but this weakness can be mitigated by decreasing the inherent level of trust that users embody through their behaviors.

Another difference is that the contact that spreads HIV/AIDS is direct. There are no intermediaries to infection. Network-propagated malware rarely spreads directly from infector to infectee; instead, the malicious code must be passed between a number of hubs and routers. In some ways, this is analogous to asymptomatic HIV carriers; however, since the program never executes on those machines they cannot be truly considered infected. Although this difference may be significant for designing technical solutions for malware, it is negligible when focusing on user behaviors as I have done here.

Lastly, human disease, particularly HIV/AIDS, carries a social stigma and a threat of death that are generally much more concrete concepts to most people than the potential

impact of malware. Still, explaining examples of malware capabilities to users may still serve as a motivating factor.

8 Some Recent, Notable Anti-Malware Initiatives

There have been some recent actives in the cyber security arena that focus on the human element. None of these are specifically anti-malware solutions, but that topic is a component of the general cyber security focus of these programs.

8.1 National Strategy to Secure Cyberspace

The National Plan for Information Systems Protection released in 2000 took a broad view of the need to protect our nation's critical infrastructure and did not address the role of individual users [65]. In contrast, the National Strategy to Secure Cyberspace, released in February 2003, clearly acknowledges the impact that even home users can have on the network as a whole if their computers are compromised and used to attack critical systems [66]. Priority three of the strategy calls for the creation of "A National Cyberspace Security Awareness and Training Program." This section emphasizes the need to empower everyone to secure their portions of cyberspace. Various levels of education and awareness programs are described, with much of the responsibility falling on the Department of Homeland Security.

8.2 DHS National Cyber Security Division

The National Cyber Security Division (NCSD) of the Department of Homeland Security was created, in part, to address the goals of the National Strategy to Secure Cyberspace. One major initiative has been the launch of a National Cyber Alert System to keep users informed of current online security hazards. The site got more than one million hits on the first day, and in less than a week, a quarter of a million people had subscribed for updates. Amit Yoran, the director of NCSD at the time, called it the "broadest distribution site for cyber security information in the world" [69].

8.3 National Cyber Security Alliance

The National Cyber Security Alliance is a public-private partnership that helps to fulfill the National Strategy mandate. The alliance maintains the staysafeonline.info web site that publishes security information, including a list of "Top 10 Cyber Security Tips" and

a self-guided security aptitude test [67]. The Alliance also sponsors National Cyber Security Day, held since 2002. These days are promoted semi-annually, every April and October to correspond with daylight savings time adjustments [45]. October 2004 was the first National Cyber Security Awareness Month, featuring awareness efforts targeting different groups each week [67].

Unfortunately, National Cyber Security Day has been criticized for being under-promoted, particularly for the general public [75]. This is likely due to the fact that the event is primarily promoted in technology and security industry publications and on the web sites of partners and participants. Coverage of these events in the popular press is generally limited to the technology section.

8.4 Carnegie Mellon CyLab Education, Training, and Outreach

CyLab at Carnegie Mellon University is also becoming active in cyber security education, training, and outreach. One driving initiative is to design a program to make 10 million citizens "cyberaware." This initiative is starting with 20,000 Pittsburgh households, in part through adding security elements to another computer education initiative in the Pittsburgh school system [87].

CyLab is also creating a "MySecureCyberspace" portal to deliver customized computer security curricula to its users [23]. They are also developing a K-12 cyber security curriculum and a "Digital Fluency" program for college freshmen.

CyLab is also looking to convey cyber security messages through entertainment. An exhibit is being designed for a hands-on science museum and an educational game is under development [87]. Additionally, CyLab presents Cyber Security Journalism awards recognizing media excellence on this topic.

9 Conclusion

User behavior can play a significant role in preventing massive malware outbreaks. Users need to understand the differences between risky behaviors and preventive behaviors in order to help mitigate malware propagation. Unfortunately, the computer

security industry has largely ignored the human aspect of prevention. Recent efforts in this area are largely ignored or unproven.

In contrast, the public health discipline combines science with human behavioral interventions in order to control epidemics, such as HIV/AIDS. These techniques include screening, partner notification, message evolution, education, and intervention. The industry also takes care to scientifically measure the impact of its initiatives in order to improve on weak programs and recreate successful ones. As a result, there is a great deal of understanding about what makes an effective intervention.

The intervention expertise of the public health industry should be applied to the development and implementation of initiatives to modify computer user behavior in an effort to control the spread of malware. Some elements that should be applied in such initiatives include:

- Proper Use/Skills Building,
- Attention to Personal/Group Risk,
- Community Setting,
- Repeated Contact,
- Awareness of Status/Available Testing,
- Peer Leadership,
- Use of Real-Life Examples/True Stories,
- Focus on Infected Persons, and
- Use of Games/Entertainment.

Additionally, the interventions should use field experiment methodology and quantitative monitoring to determine which programs are effective.

Much like the threat of biological illness, it is unlikely that the threat of malware will ever go away completely, but by combining responsible user behavior with technological advances malware can be kept to manageable levels. This is important for the continued viability of the Internet or any network may replace it.

Coordinating such initiatives requires centralized direction and oversight. This brings back the idea of the Cyber CDC [84]. A CCDC would not need to implement all the solutions itself but could serve to provide guidance to other implementation groups. For example, the medical CDC published a guide of HIV/AIDS interventions with proven results and distributed so that the programs described could be repeated by interested organizations [16]. Such actions create a centralized authority while maintaining the flexibility of autonomous implementation groups.

Despite all this, I am not intending to suggest that technological innovation is not important in the fight against malware. It most certainly is. Unfortunately, it is unlikely that any technological solution could completely eliminate the problem of malicious software. As one security consultant observed, "Once you build a better mousetrap, hackers build better mice" [43].

Although new technological protocols and tools may be able to mitigate malware propagation and damage, there will always be risk associated if we continue to support an environment of interconnectivity and interoperability, which at this point people are unlikely to want to give up. As a result, systems will continue to have the need to grant permissions to programs, even if they are locked down by default. If permissions can be granted at all it is likely that malware authors will find a way to obtain the desired permissions for their programs. If the new technologies are less inherently vulnerable there will be a greater need to use social engineering strategies to trick users into granting permissions to malicious software. The human factor will remain a key enabling or mitigating force.

One area in which technological innovation could help to support behavioral interventions would be in providing easy to use comprehensive tools for user protection. Currently there are many risky behaviors to avoid and preventive behaviors to adopt in order to try to keep a computer free of malware. Even security expert Bruce Schneier admits to not always following his own advice for keeping his computer protections up to

date [76]. Technological improvements that simplify the message of recommended actions would be immensely helpful for both education and compliance.

10 Recommendations for Future Work

Below are some suggestions for further work that extends this analysis but was beyond the scope of this paper.

10.1 Survey Malware Threat Perceptions

The AOL/NCSA survey was insightful as far as demonstrating the level of user vigilance, or lack thereof, in protecting personal computers. In addition to this, it would be useful to determine how general computer users perceive the capabilities of malware. That is, from what do they think they are trying to protect themselves? In the AOL/NCSA survey, 6% of the people stated that they knew their computers were infected [4]. If there the threat associated with malware is perceived to be low, individuals may not be compelled to take action even when they know their machine is infected. If such apathy becomes prevalent, there is little hope for the stability of the Internet.

10.2 Evaluate and Hone of Current Initiatives

Particularly since the release of the National Strategy to Secure Cyberspace, there has been some activity with the apparent goal of creating cyber security awareness, which often includes malware risk awareness, in the public sphere. Conceptually, many of these programs seem to be based on good ideas. Unfortunately, anecdotal evidence seems to indicate that the message is not getting out to where it needs to be.

Recommended is a comprehensive survey to determine the level of public knowledge about current awareness campaigns and web resources. For example, the National Cyber Alert System boasts many web site hits and subscribers, but if those are all technology professionals, the message would not seem to be making it to where it is needed most.

For intervention-type initiatives, such as some of the work being done by CyLab, disciplined follow-up and evaluation should be done to determine the effectiveness of the content and delivery method. Some questions to answer:

- Do the participants show greater security knowledge than their non-participating peers?
- Do the participants retain that knowledge after the program ends?
- Do the participants avoid risky behaviors based on that knowledge?
- Do the participants continue to avoid risky behaviors after the program ends?
- And particularly significant for this work: does a general cyber security focus result in behavioral changes that can mitigate malware propagation?

Once these questions are understood, successful strategies can be extended and less successful ones can be honed to yield better results.

10.3 Determine the Impact of Media Messages

Messages about malware are conveyed through journalism, advertising, and even, periodically, in the plots of movies and television shows. These messages tend to be memorable for information security professionals, but are they noticed by the general public? Are the issues accurately understood by non-computer professionals? Do computer users avoid risky behaviors and adopt protective ones as a result of these messages? Understanding these questions can help to form more effective messages in the future.

10.4 Develop Malware Interventions Using a Public Health Basis

In this paper, I have identified some traits of public health interventions that seem to have useful applications for combating malware. New malware interventions could be designed and implemented using attributes inspired by HIV/AIDS interventions. Because public health initiatives emphasize quantitative evaluation, the malware initiative should have measurements of success designed into it, which would allow for a clear determination of whether the program is meeting its goals.

Also helpful for designing such interventions would be determining which of the intervention characteristics are most effective. There was no clear indication in the literature read for this paper.

10.5 Produce a "Cyber CSI" or Equivalent Television Show

Twende na Wakati and other international programs have shown that well-made and well-focused entertainment can also successfully educate its audience. As described in subsection 7.6.9, an equivalent television series could be used to inform the public about cyber security issues. I can guarantee at least one loyal viewer.

11 Bibliography

[1] Adams, A. and M.A. Sasse. "Users Are Not the Enemy." *Communications of the ACM* vol. 42, no. 12 (Dec. 1999): 41-46.

[2] Albert, Reka, Hawong Jeong and Albert-Laszlo Barabasi. "Error and attack tolerance of complex networks." *Nature*, 27 July 2000: 378-82.

[3] Anagnostakis, Kostas G., Michael B. Greenwald, Sotiris Ioannidis, Angelos D. Keromytis, and Dekai Li. "A cooperative immunization system for an untrusting internet." In *Proceedings of the 11th International Conference on Networks (ICON), 2003*. http://www1.cs.columbia.edu/~angelos/Papers/icon03-worm.pdf.

[4] AOL/NCSA Online Safety Study, October 2004. http://www.staysafeonline.info/news/safety_study_v04.pdf

[5] Avolio, Frederick M. "Putting It Together." *netWorker*, April/May 1998, 15-22.

[6] Barabasi, Albert-Laszlo and Reka Albert. "Emergence of Scaling in Random Networks." *Science*, 15 October 1999, 509-12.

[7] Barabasi, Albert-Laszlo. *Linked*. New York: Penguin Group, 2003.

[8] Berghel, Hal. "Malware Month." *Communications of the ACM* 46, no. 12 (December 2003): 15-9.

[9] Boase, Jeffrey and Barry Wellman. "A Plague of Viruses: Biological, Computer and Marketing." 21 September 2001. http://www.chass.utoronto.ca/~wellman/publications/viruspaper/version.PDF.

[10] Braithwaite, Kisha and Veronica G. Thomas. "HIV/AIDS knowledge, attitudes, and risk-behaviors among African-American and Caribbean college women." *International Journal for the Advancement of Counselling* 23 (2001): 115-29.

[11] Bridwell, Larry. "ICSA Labs 9th Annual Computer Virus Prevalence Survey." ICSA Labs, A Division of True Secure Corporation, 2004. http://www.trusecure.com/cgi-bin/download.cgi ?ESCD=w0169&file=wp_vps2003_report.pdf.

[12] Briesemeister, Linda, Patrick Lincoln, and Phillip Porras. "Epidemic Profiles and Defense of Scale-Free Networks." In *Proceedings of the 2003 ACM Workshop on Rapid Malcode, SESSION: Defensive Technology, Held in Washington, D.C.*, 67-75. New York: ACM Press, 2003.

[13] Broersma, Matthew. "Slammer: The First 'Warhol' Worm?" ZDNet UK. 03 February 2003. http://news.zdnet.co.uk/business/0,39020645,2129785,00.htm.

[14] Brunet-Jailly, J. "AIDS and Health Strategy Options: the Case of Cote d'Ivoire." 1998. http://www.worldbank.org/aids-econ/arv/brunet/bj-eng-a4.pdf.

[15] Buttram, Randy. "The Biological Analogy and the Future of Information Security." GIAC Security Essentials Certification Practical Assignment 1515, Version 1.2f, 20 February 2002. http://www.giac.org/practical/ Randy_Buttram_GSEC.doc.

[16] CDC. HIV/AIDS Prevention Research Synthesis Project. *Compendium of HIV Prevention Interventions with Evidence of Effectiveness*. November 1999, Revised. Atlanta, Ga.: Centers for Disease Control and Prevention, 1999.

[17] CDC. "Advancing HIV Prevention: Interim Technical Guidance for Selected Interventions." Centers for Disease Controls and Prevention, 19 May 2003. http://www.cdc.gov/hiv/partners/Interim-Guidance.htm

[18] CDC. "Advancing HIV Prevention: New Strategies for a Changing Epidemic – United States, 2003." Centers for Disease Controls and Prevention, *Morbidity and Mortality Weekly Report* 52, no. 15 (18 April 2003): 329-332. http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5215a1.htm.

[19] CDC "What is HIV?" National Center for HIV, STD, and TB Prevention, Divisions of HIV/AIDS Prevention, Frequently Asked Questions. 15 December 2003.

[20] CERT. Computer Emergency Response Team/Coordination Center. http://www.cert.org.

[21] CERT. "Attack Trends." The CERT Coordination Center, 20 February 2002. http://www.cert.org/archive/pdf/attack_trends.pdf.

[22] CERT. "Incidents Reported." *CERT/CC Statistics 1988-2004*, 19 October 2004. http://www.cert.org/stats/cert_stats.html.

[23] Carnegie Mellon CyLab. 2004. http://www.cylab.cmu.edu/.

[24] Davis, Kevin. "Saving Users From Themselves: Creating an Effective Student-Oriented Anti-Virus Intervention." In *Proceedings of the 29th annual ACM SIGUCCS conference on User Services Held in Portland, OR,* 27-32. New York: ACM Press, 2001.

[25] Del Rio, Carlos. "New Challenges in HIV Care: Prevention Among HIV-Infected Patients." *Topics in HIV Medicine* 11, no. 4 (July/August 2003): 140-4.

[26] Dezso, Zoltan and Albert-Laszlo Barabasi. "Halting viruses in scale-free networks." *Physical Review* E 65, art. No 055103 (2002).

[27] Edwards, Donna M., Ross D. Shachter, and Douglas K. Owens. "A Dynamic HIV-Transmission Model for Evaluating the Costs and Benefits of Vaccine Programs." *Interfaces* 28, Issue 3 (March 1998): 144-166.

[28] Electricnews.net. "The End of the Internet is Nigh." *The Register*, 28 September 2004. http://www.theregister.co.uk/2004/09/28/internet_end_nigh/.

[29] Emm, David. "Traditional Antivirus Solutions - Are They Effective Against Today's Threats?" Viruslist.com, 17 October 2004. http://www.viruslist.com/en/viruses/analysis?pubid=153595662.

[30] Emm, David. "Antivirus Updating - Why It's More Important Than Ever Before." Viruslist.com, 17 October 2004. http://www.viruslist.com/en/viruses/analysis?pubid=153596013.

[31] Eng, Thomas R. and William T. Butler, ed. "Chapter 4: Prevention of STDs." In *The Hidden Epidemic*, 118-74. Washington, D.C.: National Academic Press, 1997.

[32] FIRST. "Annual FIRST Conference." *Forum of Incident Response and Security Teams*. http://www.first.org/conference/.

[33] Forrest, Stephanie, Steven A. Hofmeyr, and Anil Somayaji. "Computer Immunology." *Communications of the ACM* 40, issue 10 (October 1997): 88-96.

[34] Fowler, Dennis. "Attack of the Killer Virus." *netWorker* 7, issue 4 (December 2003): 16-22.

[35] F-Secure. *Data Security Summary for 2003.* 18 December 2003. http://www.f-secure.com/2003/

[36] Garetto, Michele, Weibo Gong, and Don Towsley. "Modeling Malware Spreading Dynamics." In *Proceedings of INFOCOM*, April 2003. www.telematics.polito.it/garetto/papers/virus2003.pdf.

[37] Ghosh, Anup K. and Jeffrey M. Voas. "Inoculating Software for Survivability." *Communications of the ACM* 42, issue 7 (July 1999), 38-44. New York: ACM Press, 1999.

[38] Gordon, Sarah and Richard Ford. "Real World Anti-Virus Product Reviews and Evaluations – The Current State of Affairs." In *Proceeding of the 19th NIST-NCSC National Information Systems Security Conference Held 22-25 October*

1996, vol. 2, 526-38. http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper019/final.PDF.

[39] Gordon, Sarah. "What is Wild?" In *Proceedings of the 20th NIST-NCSC National Information Systems Security Conference Held in Baltimore, MD October 1997*, 177-90. http://csrc.nist.gov/nissc/1997/proceedings/177.pdf.

[40] Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. "2004 CSI/FBI Computer Crime and Security Survey." Computer Security Institute, 2004. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[41] Gorman, Sean P., Rajendra G. Kulkarni, Laurie A. Schintler, and Roger R. Stough. "A Predator Prey Approach to The Network Structure of Cyberspace." In *Proceedings of the Winter International Symposium on Information Communication Technologies Held in Cancun, MX*, 1-6. Dublin: Trinity College, 2004.

[42] Graham-Rowe, Duncan. "Computer Antivirus Strategies in Crisis." *NewScientist.com*, 3 September 2003. http://www.newscientist.com/news/news.jsp?id=ns99994119.

[43] Grimes, Brad. "The Right Ways to Protect Your Net." *PC World*, September 2001. http://www.pcworld.com/howto/article/0,aid,56423,00.asp.

[44] Handcock, Mark S., James Holland Jones, and Martina Morris. "On 'Sexual contacts and epidemic thresholds,' models and inference for Sexual partnership distributions." 27 May 2003. http://www.csss.washington.edu/Papers/wp31.pdf.

[45] ITSecurity.com "National Cyber Security Alliance Gains Momentum as Home Users, Businesses and Academia 'Spring Forward.'" 2 April 2004. http://www.itsecurity.com/tecsnews/apr2004/apr16.htm

[46] Janssen, Robert S., David R. Holtgrave, Ronald O. Valdiserri, Melissa Shephard, Helene D. Gayle, and Kevin M. De Cock. "The Serostatus Approach to Fighting

the HIV Epidemic: Prevention Strategies for Infected Individuals." *American Journal of Public Health* 91, no. 7 (July 2001): 1019-24.

[47] Jeong, H., Z. Na, and A.-L. Barabsi. "Measuring preferential attachment for evolving networks." *Europhysics Letters* 61, no. 4 (2003): 567-72.

[48] Kanabus, Annabel and Jenni Fredriksson. "The History of AIDS 1981-1986." AVERT, 2 September 2004 (last update). http://www.avert.org/his81_86.htm.

[49] Kanabus, Annabel and Jenni Fredriksson. "The History of AIDS 1987-1992." AVERT, 2 September 2004 (last update). http://www.avert.org/his87_92.htm.

[50] Kanabus, Annabel and Jenni Fredriksson. "The History of AIDS 1993-1997." AVERT, 2 September 2004 (last update). http://www.avert.org/his93_97.htm.

[51] Kanabus, Annabel and Jenni Fredriksson. "The History of AIDS 1998-2002." AVERT, 2 September 2004 (last update). http://www.avert.org/his98_99.htm.

[52] Kanabus, Annabel and Jenni Fredriksson-Bass. "The History of AIDS 2003 Onwards." AVERT, 2 September 2004 (last update). http://www.avert.org/aidshistory.htm.

[53] Kephart, Jeffrey O. "A biologically inspired immune system for computers." *In Artificial Life IV: Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems*, edited by R. A. Brooks and P. Maes, 130-9. Cambridge: MIT Press, 1994.

[54] Kephart, Jeffrey O., Sorkin, Gregory B., Chess, David M. and White, Steve R. "Fighting Computer Viruses: Biological Metaphors Offer Insights into Many Aspects of Computer Viruses and Can Inspire Defenses Against Them." *Scientific American*, November, 1997. http://www.sciam.com/1197issue/1197kephart.html.

[55] Keromytis, Angelos D., Janak Parekh, Philip N. Gross, Gail Kaiser, Vishal Misra, Jason Nieh, Dan Rubenstein, and Sal Stolfo. "A Holistic Approach to Service

Survivability." In *Proceedings of the ACM Survivable and Self-Regenerative Systems Workshop, October 2003*. http://www1.cs.columbia.edu/~angelos/Papers/saber.pdf.

[56] Kienzle, Darrell M.and Matthew C. Elder. "Recent Worms: A Survey and Trends." In *Proceedings of the 2003 ACM Workshop on Rapid Malcode, SESSION: Internet Worms: Past, Present, and Future Held in Washington, DC,* 1-10. New York: ACM Press, 2003.

[57] Kippax, Susan and Kane Race. "Sustaining Safe Practice: Twenty Years On." *Social Science & Medicine* 57, no. 1 (2003): 1-12.

[58] Krebs, Brian. "A Short History of Computer Viruses and Attacks." Washingtonpost.com, 14 February 2003. http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26.html.

[59] Leveille, Jasmin. "Epidemic Spreading in Technological Networks." *HP Technical Reports*, HPL-2002-287 (23 October 2002). http://www.hpl.hp.com/techreports/2002/HPL-2002-287.html

[60] Liljeros, F and C R. Edling, L A.N. Amaral, H E. Stanley, and Y Aberg. "The Web of Human Sexual Contacts." *Nature* 411 (2001), 907-8.

[61] Martin, Kelly. "The Polluted Internet." *The Register*, 27 August 2004. http://www.theregister.co.uk/2004/08/27/polluted_internet/

[62] Moore, David, Colleen Shannon, Geoffrey M. Voelker, and Stefan Savage, "Internet Quarantine: Requirements for Containing Self Propagating Code", in *Proceedings of the IEEE Infocom Conference Held in San Francisco, CA April 2003*. http://www.cs.ucsd.edu/~savage/papers/Infocom03.pdf

[63] Moskowitz, Judith Tedlie, Diane Binson, and Joseph A. Catania. "The Association Between Magic Johnson's HIV Serostatus Disclosure and Condom Use in At-Risk Respondents." *Journal of Sex Research,* Spring 1997. http://findarticles.com/p/articles/mi_m2372/is_n2_v34/ai_19551965.

[64] Mundie, Dave. CERT/CC. Personal email, 2 December 2004.

[65] The National Plan for Information Systems Protection. 2000. http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf.

[66] The National Strategy to Secure Cyberspace. February 2003. http://www.whitehouse.gov/pcipb/.

[67] National Cyber Security Alliance. 2004. http://www.staysafeonline.info/.

[68] Neubauer, Bruce J. and James D. Harris. "Protection of computer systems from computer viruses: ethical and practical issues." *Journal for Computing in Small Colleges* 18, no. 1 (2002): 270-9

[69] Newell, Adrienne. "Is Cyberspace Getting Safer?" PC World, 11 February 2004. http://www.pcworld.com/news/article/0,aid,114749,00.asp

[70] Owens, Douglas K., Donna M. Edwards, and Ross D. Shachter. "Population Effects of Preventive and Therapeutic HIV Vaccines in Early- and Late-Stage Epidemics." http://www-smi.stanford.edu/pubs/SMI_Reports/SMI-97-0674.pdf.

[71] Pastor-Satorras, Romualdo and Alessandro Vespignani, "Epidemic spreading in scale-free networks." *Physical Review Letters* 86, no. 14 (2 April 2001): 3200-3.

[72] Ranum, Marcus J. "Believing in Myths." *Communications of the ACM*. 47, no. 1 (January 2004): 144.

[73] Reuters. "Windows Besieged by Hackers." *Cnn.com*, 20 September 2004. http://money.cnn.com/2004/09/20/technology/symantec_msft.reut/?cnn=yes.

[74] Reynolds, J.K. "RFC1135: Helminthiasis of the Internet."*Internet RFCs*, 1989.

[75] Roberts, Paul. "National Cyber Security Day is a Well-Kept Secret." *InfoWorld*, 5 April 2004. http://www.infoworld.com/article/04/04/05/ HNnationalcybersecurityday_1.html.

[76] Schneier, Bruce. "Safe Personal Computing." *Crypto-Gram Newsletter,* 15 May 2001. http://www.schneier.com/crypto-gram-0105.html#8.

[77] Schneier, Bruce. "Virus Wars." *Crypto-Gram Newsletter,* 15 April 2004.

[78] Schneier, Bruce. "Clever Virus Attack." Crypto-Gram Newsletter, 15 November 2004.

[79] Sidiroglou, Stelios and Angelos D. Keromytis. "A Network Worm Vaccine Architecture." In *Proceedings of the IEEE Workshop on Enterprise Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security,* June 2003. http://www1.cs.columbia.edu/~angelos/Papers/worm-vaccine.pdf.

[80] Singhal, Arvind and Everett M. Rogers. *Combating AIDS: Communication Strategies in Action.* California: Sage Publications, 2003.

[81] Spafford, Eugene H. "Computer Viruses as Artificial Life." *Artificial Life* 1, issue 3 (Spring 1994): 249-265.

[82] Spafford, Eugene H. "A Failure to Learn from the Past." In *Proceedings of the 19th Annual Computer Security Applications Conference,* December 2003. http://www.acsac.org/2003/papers/classic-spafford.pdf.

[83] Stamp, Mark. "Risks of Monoculture." *Communications of the ACM* 47, issue 3 (March 2004),120. New York: ACM Press, 2004.

[84] Staniford, Stuart, Vern Paxson, and Nicholas Weaver. "How to 0wn the Internet in Your Spare Time." In *Proceedings of the 11th USENIX Security Symposium,*149-67. Berkeley: USENIX Association, 2002.

[85] Stoneburner, Rand L. and Daniel Low-Beer. "Population-Level HIV Declines and Behavioral Risk Avoidance in Uganda." *Science,* 30 April 2004: 714-18.

[86] Teo, Lawrence, Gail-Joon Ahn, and Yuliang Zheng. "Dynamic and Risk-Aware Network Access Management." In *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, SESSION: Dynamic Access Control, Held in Como, Italy*, 217-30. New York: ACM Press, 2003.

[87] Tsamitis, Dena. Carnegie Mellon CyLab, personal interviews, 9 March 2004 and 28 October 2004.

[88] Wang, Chenxi, John C. Knight, and Matthew C. Elder. "On computer viral infection and the effect of immunization." In *Proceedings of the ACSAC Held in New Orleans, LA 2000*, 246-56. http://www.cs.virginia.edu/~jck/publications/acsac.2000.pdf.

[89] Wang, Yang, Deepayan Chakrabarti, Chenxi Wang, Christos Faloutsos. "Epidemic Spreading in Real Networks: An Eigenvalue Viewpoint." 2003. http://www.db.cs.cmu.edu/Pubs/Lib/srds2003spreadingNetwork/deepay_spreadingNetwork.pdf.

[90] Wang, Yang and Chenxi Wang. "Modeling the Effects of Timing Parameters on Viral Propagation." In *Proceedings of the 2003 ACM workshop on Rapid Malcode Held in Washington, D.C.,* 61-6. New York: ACM Press, 2003.

[91] Watanabe, Myrna E. "Topical Control of HIV Transmission Possible." *The Scientist* 16, Issue 22 (11 November 2002): 34.

[92] Weaver, Nicholas, Vern Paxson, Stuart Staniford, and Robert Cunningham. "A Taxonomy of Computer Worms." In *Proceedings of the 2003 ACM workshop on Rapid Malcode*, Washinton, D.C 2003, 11-8 New York: ACM Press, 2003. http://www.cs.berkeley.edu/~nweaver/papers/taxonomy.pdf.

[93] White, Steve R. "Virus Bulletin 2010: A Retrospective." IBM Thomas J. Watson Research Center, 20 September 2000. http://researchweb.watson.ibm.com/antivirus/SciPapers/Retrospective.htm.

[94] WHO. *UNAIDS/WHO Global HIV/AIDS Online Database*. http://www.who.int/GlobalAtlas/DataQuery/.

[95] Williams, Jeff. "Just Sick About Security." In *Proceedings of the 1996 Workshop on New Security Paradigms Held in Lake Arrowhead, CA*, 139-46. New York: ACM Press, 1996.

[96] Williams, Mary B., David Ermann, and Glaudio Gutierrez. "Cautionary tales and the impact of computers on society." *ACM SIGCAS Computers and Society* 19, Issue 3 (September 1989): 23-31.

[97] Williamson, Matthew M. and Jasmin Leveille. "An epidemiological model of virus spread and cleanup." Information Infrastructure Laboratory, HP Laboratories Bristol. 27 February 2003. http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf.

Appendix A: CDC Intervention Checklist

When evaluating an intervention strategy, the CDC recommends evaluating characteristics of the intervention against the checklist elements below [16]. For each item, a specific example should be cited to show how the intervention meets that goal. Additionally, each item should be ranked as high, medium, or low to reflect the level to which the intervention achieves that goal. These evaluations can then be used to identify weak points in existing intervention strategies.

A. Intervention Items
   1. The intervention has a clearly defined audience.
   2. The intervention has clearly defined goals and objectives.
   3. The intervention is based on sound behavioral and social science theory.
   4. The intervention is focused on reducing specific risk behaviors.
   5. The intervention provides opportunities to practice relevant skills.

B. Implementation Items
   1. There is a realistic schedule for implementation.
   2. Staff are adequately trained for sensitivity to the target population.
   3. Staff are adequately trained to deliver the core elements of the intervention.
   4. Core elements of the intervention are clearly defined and maintained in the delivery.
   5. Staff uses a variety of teaching methods, strategies, and modalities to convey information, personalize the training, and repeat essential prevention messages.

C. Organization Items
   1. There is administrative support for the intervention at the highest levels.
   2. There are sufficient resources for the current implementation.
   3. There are sufficient resources for sustainability.
   4. Decision-makers are flexible and open to program changes.
   5. Intervention is embedded in a broader context that is relevant to the target population.

D. Consumer/Participant Items

1. The intervention meets specified priorities and needs defined by the community.
2. For the target population selected, the intervention is culturally competent.
3. For the target population selected, the intervention is developmentally appropriate.
4. For the target population selected, the intervention is gender specific.
5. The intervention as implemented is acceptable to the participants.