

# **An Open Source, International, Attenuated Computer Virus Vaccine**

July 14, 2001  
Defcon 9  
Las Vegas, Nevada

Dr. Cyrus Peikari

## **Abstract**

The unchecked proliferation of global information networks has left society vulnerable to a digital Armageddon. Computer virus “vaccines” can counter this vulnerability by stabilizing and strengthening information systems. Using analogies from medicine, this paper demonstrates the pressing need for well-designed computer viruses. This paper also proposes the design, implementation, and distribution of an open-source, international, attenuated computer virus vaccine.

## I. Introduction

As the Internet evolves in complexity and interconnectivity, it becomes more than the sum of individual, private networks. Instead, it takes on the characteristics of a single, complex organism. Computer virus outbreaks no longer infect a few thousand computers only. A single virus can now sicken the entire body of the Internet. The Internet can thus be likened to the human body. For example, if each computer in the world represents a structural cell in this body, then security experts and anti-virus solutions might represent the immune system of the body.

In this analogy, it is not enough to immunize individual cells (computers) in the body. Thus, the ideas presented in this paper are designed to benefit the global Internet, rather than an individual computer or network. We will not examine local anti-virus solutions such as virus scanning software. In fact, the global anti-virus solutions described herein may be harmful to individual systems. Using examples from medicine, we will formulate the concept of a global computer virus vaccine that confers immunity by infecting the entire Internet.

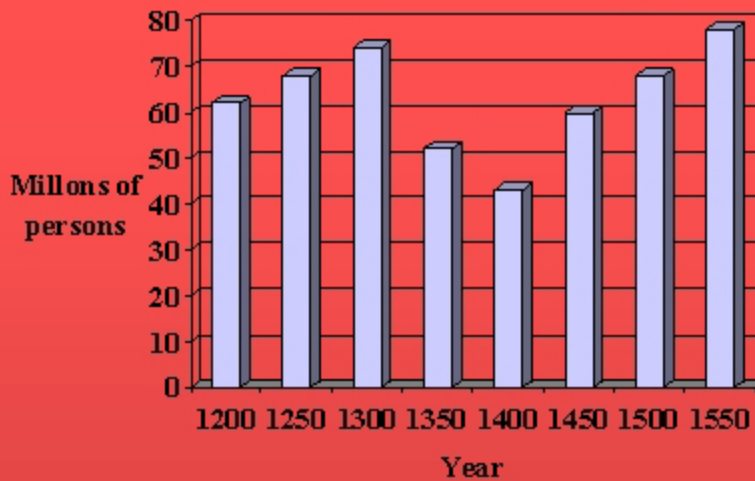
There is a pressing need for such a holistic solution. For instance, an example of the cataclysmic effect of computer viruses occurred when the “I love you” virus was released in May 2000. Within a few days it had spread to and infected several hundred thousand computers. The damage from this one pathogen was estimated at \$15 billion, which at that time made it the most destructive virus to date. In addition to demonstrating the unified susceptibility of the Internet, this virus also showed that current anti-virus solutions were incapable of preventing disaster. In addition, future disasters are likely to be far worse. Thus, new anti-virus solutions are urgently needed in order to stabilize global networks and to protect the body of the world from illness.

## II. Background

The end of civilization could be only as far away as the next virus. History has proven this repeatedly. In the Middle Ages, for example, the Black Plague caused a disaster from which it took Europe centuries to recover. Figure 1 is a graph showing the estimated population of Europe from 1200-1500. As you can see, in the 14th century the population of Europe was abruptly cut in half by bubonic plague.

Fig. 1: Population of Europe

## Population of Europe



The Plague killed both the young and the old and disrupted married life. Entire towns disappeared almost overnight. Large towns were hit especially hard because of overcrowding and because of rats, which carried the plague bacillus. In addition, workers were too preoccupied with burying the dead and with fears of their own death to remain productive. Because employers were decimated, there was no work, and the poor starved to death. As a result, there was massive, widespread insurrection from workers and from peasants across Europe. The government and landowners responded with ferocious repression. Civilization had suddenly stepped backwards the equivalent of one thousand years.

Later, Europeans wiped out another civilization with smallpox. Many think that the Europeans conquered the Native Americans, but this is not true. Smallpox conquered the Americas. Smallpox single-handedly wiped out 95% of the population of Central America and Mexico. Afterwards, the Europeans simply walked into and claimed an empty continent.

How is this possible? Europeans had been building up immunity to typhoid, diphtheria, smallpox, and other plagues. However, Native Americans had lived untouched by these diseases, until the European settlers brought the germs to the New World. With no immunity against the silent killers, natives died of such mild diseases as influenza and the common cold.

By far, the deadliest of the diseases Europeans brought to the Americas was smallpox. Spanish conquistadors spread smallpox throughout Central and South America. The results were devastating. During the century after Columbus arrived in the New World, the Indian population of Central America and Mexico dropped from more than 25 million to just one million people.

Smallpox also nearly wiped out the natives of North America. Everywhere it touched, the disease killed tribes by the thousands. Smallpox killed over half the population of North America. When the time came to defend their lands against the spread of European invaders, many Native American societies found themselves so weakened in numbers that they were unable to defend themselves in war. Again, a single pathogen had destroyed an entire civilization.

We are just now beginning to see pathogens as destructive as smallpox in the digital world. Thanks to early computer viruses, the networked world has already built up some immunity. If it were not for computer viruses, the Internet would be susceptible to total destruction from a single pathogen, just as the Native Americans were.

Biologist built upon this idea of progressive immunization by developing medical vaccines. The early smallpox vaccine conferred immunity from future infections, but it killed one per cent of those who took the vaccine. Thus, at first people were reluctant to take the vaccine, even though it was mathematically proven to make them live longer. In fact, Benjamin Franklin did not give his son the vaccine at that time. His son died of smallpox, and for the rest of his long life Franklin bitterly regretted not immunizing his unfortunate son.

With time, however, the smallpox vaccine became more refined. In fact, it was so incredibly successful that in 1977 smallpox was eradicated from the world. In fact, children today are no longer vaccinated against smallpox, because there is no endemic source left in the world.

Thus, we can see the power of vaccines. In fact, vaccines are so successful that the government now mandates them. Every day the government forces doctors to inject children with attenuated strains of deadly viruses. Historically, some of these vaccines have caused death and disease in children. Nevertheless, because they serve the greater good, society embraces them.

### **III. Arguments for a computer virus vaccine**

As described above, the Internet has become a global, unified organism. As interconnectivity increases, so too does the destructive potential of computer viruses. Examples such as the "I love you" virus demonstrate that existing anti-virus solutions are incapable of preventing massive destruction.

There have already been efforts toward designing digital immune systems, as well as rudimentary attempts at vaccines. For example, researchers at one corporation have designed a system that automatically detects antigens and generates a host-immune response. However, this is a limited attempt to simulate what nature has already given us. The truth is that the Internet has already evolved its own native immune system. In the global body, the "killer-cells" are the automated anti-virus software solutions that are at work every day. The specialized "memory cells" are those network technicians and information security experts that direct the immune response. Thus, we have a world-

embracing immune system in place. What that system now needs is vaccination: not local immunization limited to discrete, private networks, but rather global immunization of the entire world body.

Most anti-virus solutions have been limited in that they work on local systems only. An example of this is scanning for characteristic viral byte signatures in order to recognize pathogens. However, there have not been attempts to stress the entire Internet with attenuated vaccines. Because anti-virus researchers often abhor virus writers, the AV community has been resistant to any concept that includes the release of live, replicating viruses, even if they are beneficial. In fact, a large part of the AV community argues that there can be no such thing as a "good" virus.

However, medical models refute this argument. In medicine, some of the most effective vaccines are those that use "live," attenuated virus samples. Can we imagine ingesting a live sample of a deadly virus, even if it was weakened? Yet most of us have already done so. The poliovirus vaccine required children to swallow a live, attenuated form of the deadly poliovirus. This was not only tolerated; it was embraced. In fact, the government mandated it. Because the government forced us all to swallow this weakened, deadly virus, we were able to successfully eradicate polio. This supports a utilitarian model, which holds that the greatest good for the greatest number of people. It also supports a paternalistic model, which says that the government, like a parent, knows what is best for us. Although this idea makes many cringe, it nevertheless adumbrates the future of government-released computer virus vaccines.

Another medical concept lacking in current digital immune systems is the idea of "herd immunity." Herd immunity means that if you vaccinate a small subset of a population only, then the subset will cross-vaccinate the non-immunized population automatically. For example, doctors know that they do not need to immunize all children with certain childhood vaccines. They know that if they immunize 80 percent of school children, then these 80 percent will infect the 20% that do not have protection. Children are excellent vectors. They transmit viruses by the fecal-oral route (putting their hands in the stool around their own anuses and then touching their classmates' hands and mouths) and by the nasopharyngeal route (wiping mucus from their noses all over their classmates). However, these seemingly unsanitary acts are actually vital for transmitting immunity. Thanks to children spreading their germs, close to 100% of the class will become passively immunized.

This concept of herd immunity can be useful to giant networks such as the Internet. It is not necessary to distribute a vaccine to 100% of systems in order to be successful. For example, the Melissa virus conferred immunity to itself after infection. More importantly, because it spread so successfully, it had a much stronger impact on immunity from a holistic perspective. Melissa caused heightened awareness and thus enhanced the future response of "killer cells" (AV solutions) and "memory cells" (human expertise) of the global immune system. This is a form of herd immunity, because through education the virus strengthened systems that were not even infected.

#### **IV. Characteristics of the Vaccine: Open Source, International, and Attenuated**

Based on lessons learned from medicine, global computer vaccines are inevitable. It would be advantageous if they were designed on an open-source model. This would allow for much better quality control. An open model encourages feedback and testing from researchers and programmers around the world. As we have learned from medicine, vaccines themselves can be damaging. However, with research and testing, they can be perfected. In addition, an open source model permits advanced immunity for critical infrastructure sectors, which can anticipate and test changes in advance.

Who will release the vaccine? By default, it will have to be a government agency. It is illegal to modify a computer system that does not belong to you. The government is the only organization that has the authority to unleash viruses, even in attenuated form. We have already granted this paternalistic power to the government in the form of medical vaccines. In the case of a computer vaccine, a central authority composed of both medical epidemiologists and computer programmers will be responsible. Moreover, it should be an international agency, rather than a regional one. Viruses know no geographical boundaries; a "vaccine" released by one country could be misinterpreted as an act of war when it invades another country that is not prepared for it. Thus, an international computer vaccine will not be practical until there exists an international government with universal authority.

Following the example of some of the most successful medical vaccines, the computer vaccine should be "live." In other words, it requires the power of replication and transmission in order to be effective. However, it should also be attenuated. In this way, it can confer immunity without causing a serious infection. For example, an attenuated Melissa vaccine might have a time-delay and a curtailed number of vectors, allowing for more controlled growth. Similarly, a recent worm that automatically repaired the BIND/named vulnerability on infected machines could be useful if the malicious part of its payload was disabled. Although these are rudimentary examples that are not yet practical, they do suggest possible strategies for future attenuation

#### **V. Arguments in favor of a beneficial virus**

##### 12 requirements of a "good virus":

Over the years antivirus researchers have argued against the plausibility of a beneficial computer virus. For example, in 1997 Vesselin Bontchev published his reasons why a "good" computer virus was impossible. However, in April 1999 the virus author known as Midnyte eloquently confuted these arguments in his famous treatise "Argument for a 'Good' Virus". In this paper, Midnyte, a member of the Ultimate Chaos virus group, proposed a virus that passed Bontchev's 12 barriers to a 'good' virus. The following section does not attempt to reexamine that historic argument. Rather, we will see that an attenuated computer virus vaccine can be beneficial without satisfying those 12 arbitrary points. Although we provide a fresh perspective from medicine, we make no attempt to

justify the virus or to argue its inherent "goodness." Lessons from history and medicine show us that computer vaccines are coming. They are inevitable. This paper is merely attempting to characterize them.

1. Lack of Control: This states that a virus cannot be "good" if it spreads without control. In reality, however, a viral vaccine that confers "herd immunity" should spread without control; this is a desirable trait. For example, doctors use this to their advantage with certain childhood vaccines.

2. Recognition Difficulty: This argues that antivirus software will have trouble distinguishing destructive viruses from beneficial vaccines. However, it is actually desirable for scanners to detect the vaccine. Triggering scanners means that the vaccine has engendered an appropriate immune response.

3. Resource Wasting: This states that viruses are "bad" because they waste resources such as CPU time or bandwidth. However, resource wasting can have a useful result. In medicine, for example, the influenza vaccine is an example of resource wasting. Many patients feel tired and flu-like after receiving a flu shot. This is because the body has to shut down critical pathways and has to mobilize other resources in order to build immunity. However, the overall effect of the vaccine is to strengthen the body against future infection.

4. Bug Containment: This argues that viruses can serve to spread software bugs in a self-replicating way. However, software bugs are ubiquitous. The global computer community is so used to dealing with software bugs that it has become second nature. Thus, just as in the human body, there is a built-in "surveillance immunity" within the Internet. Medical vaccines themselves are not without bugs. In fact, over the years some vaccines such as swine flu have resulted in death or paralysis. However, with proper testing vaccines can be perfected and refined. This is also an argument in favor of an open-source vaccine.

5. Compatibility Problems: This argues that a virus alters host programs, which may then trigger checksum monitors, thus preventing the programs from running. However, an intentionally destructive virus will do this anyway. An attenuated virus can uncover the problems and expose them for repair before they trigger an epidemic. The challenge in designing vaccines is to maximize benefit while minimizing harm.

6. Effectiveness: This argues that using a simulator, which does not have the risks associated with self-replication, can confer the same benefit as a virus. This raises an interesting point from medical immunology. We know from medicine that some of the best vaccines must be "live" in order to be effective. For example, polio was largely eradicated by ingesting a live, attenuated form of the deadly virus. At the time, "dead" simulations of the virus were simply not effective as vaccines. The same can apply to computer virus vaccines. A "live" computer virus, especially an intelligent one that can overcome natural barriers to its growth, could spread more effectively than a non-replicating simulator.

7. Unauthorized Data Modification: This states that a virus modifies data without permission, which is illegal. It also criticizes a virus for being “paternalistic,” which implies that the virus writer knows what is best for the host. By this argument, however, medical vaccines would likewise be “bad”, which is false. Also, in the case of vaccines, society embraces the government’s paternalism.

8. Copyright and ownership problems: This argues that a virus will void a manufacturer’s warranty on the software that is infected. A utilitarian argument (the greatest good for the greatest number) would obviate this barrier. Alternately, an international government could mandate that a vaccine cannot void warranties or ownership.

9. Possible misuse: This argues that an attacker can use a “good” virus as a possible means of transportation to penetrate a system. However, in the case of a vaccine, this is argument is irrelevant. A host should properly detect the vaccine as an unwelcome invasion. This is an important part of the immune response. Thus, a vaccine does not inherently open vulnerabilities, other than its payload. Moreover, a vaccine is attenuated. A real virus would likely be more damaging than a vaccine. The point of a vaccine is to confer immunity without serious infection.

10. Responsibility: This barrier states that creating a class of beneficial viruses such as vaccines “would just provide an excuse to the crowd of irresponsible virus writers to condone their activities.” However, at a Defcon speech in July 2000, Sara Gordon explained that there would always be a cycle of irresponsible virus writers. As virus writers evolve into higher ethical stages, they are continually replaced by a flux of new virus writers at lower ethical stages. Thus, there will always be a group of virus writers who operate at a “low” ethical stage and who feel no need no justification.

11. Negative Common Meaning: This holds that society will never accept the concept of a good virus, because the word “virus” has been loaded with negative meaning. At first, this will be true. Just as with the first smallpox vaccine, there will be massive resistance to early computer vaccines. However, as with their medical counterparts, computer vaccines will eventually be welcomed as they are refined and tested.

12. Trust Problems: This argument states that users will not trust any virus, since viruses cause a loss of control and a feeling of helplessness. This is addressed in the answer to number 11 (Negative Common Meaning) above.

### Are Viruses Inherently Evil?

Although a full debate on the good vs. the evil nature of viruses is irrelevant and is beyond the scope of this paper, we briefly mention the controversy here. For example, in September 2000 Bruce Schneier argued, “Beneficial viruses are a simple solution that’s always wrong. A virus is not “bad” or “good” based on its payload. Viral propagation mechanisms are inherently bad, and giving them beneficial payloads doesn’t help.”

Unfortunately, this dogmatic pronouncement steps out of the realm of science and mathematics and ventures into the gray area of philosophy. In philosophy, no object is inherently *bad*. Rather, an object is only evil in relation to something that it harms. Thus, a destructive computer virus is *evil* in relation to its victims. In contrast, a virus vaccine is *good* in relation to the hosts that it immunizes. In relation to itself, however, the virus is neither good nor bad.

In reality, history and medicine prove that viral propagation mechanisms are often inherently good. The viral cycle has saved hundreds of millions of children from death and disease through the use of vaccines. Antivirus researchers and mathematicians cannot yet understand this, but medical doctors already do.

## **VI. Conclusion**

In summary, computer virus vaccines will someday be needed to stabilize global networks and to prevent the collapse of digital civilization. This paper proposes an open-source, international, attenuated, computer virus vaccine. Based on lessons learned from medicine, such vaccines are not only possible, but are also inevitable.

**DISCLAIMER: REMEMBER THAT YOU NEED PERMISSION TO ALTER SOMEONE ELSE'S SYSTEM, EVEN IF YOU ARE TRYING TO FIX IT.**