

COMPUTER VIRUSES: The Technology and Evolution of an Artificial Life Form MANUSCRIPT SUMMARY

Written by: Karsten Johansson, 1994

NOTE:

This document was written before the advent of Internet worms and trojans. It probably contains more information about the pre-commercial internet virus scene than any other singular source, and thus I have opted to make it available to the Internet as a historical reference. There are a couple of unfinished sections, but maybe if there is enough interest, I may be convinced to finish this and update it to reflect the current state of the malware industry, and update the Artificial Life stuff since so much has happened there since 1994.

Permission is granted to use this information in any legitimate manner as long as (1) my copyright is maintained, (2) you give me credit for all material used, and (3) you send an email to ksaj@penetrationtest.com so I know where and how my research and writing is being used.

There is no copy restriction on this document for reading or distribution, but (4) under no circumstances is sale or profit directly from my work permitted without my implicit authorization. (5) If distributed, this document must remain in its entirety, and shall not be altered from the original PDF file distributed at <http://www.penetrationtest.com>.

Publishers interested in this manuscript or any of my other works may contact me at the same email address.

Summary

At one time, the idea of having a computer in the home would have been met with sympathetic laughter. Within the past ten years, computer science has advanced in great leaps, and made this dream a reality. No longer is the computer considered an alien and inaccessible commodity. It has become such a standard household item that one only has to look about the home to see its profound effects. We have become more and more reliant on this newfound technology and power.

With it has come a new vulnerability. A destructive force, once only speculated about in science fiction books, has now become a painful reality. It has been dubbed the "Computer Virus".

Over a short period of time, the threat has become so great that entire nations are forced to contend with it. Now all computer users must learn how to protect themselves against it. As well, whole sciences have been developed to study this new and highly dangerous technology.

COMPUTER VIRUS: The Technology and Evolution of an Artificial Life Form is an exposé written for everyone who owns or works with computers, detailing all aspects of the computer virus, and similar technologies. Virus scanning, removal, and safeguarding are discussed at length, along with comparison testing between several popular Anti-Virus software packages. (The results of these tests will be shocking to some.) Two branches of science stemming from computer virus technology, synthetic psychology and artificial life, are considered in depth.

Following is a run-down of chapters, with brief descriptions of each.

Chapter 1

Due to high media pressures and sensationalism, users have become divided on the definition of a computer virus. This chapter starts with a non-technical study of a few known viruses and similar programs, to arrive at a list of items characteristic of all programs considered to be computer viruses.

After we have arrived at a working definition, the computer virus is compared to the biological virus. A discussion of the similarities and differences of the two virus forms ensues, using several well-known virus strains and virus incidences as demonstration. It is concluded that they are dissimilar only in habitat.

Chapter 2

This chapter begins with a detailed timeline, starting with Alan Turing in 1931, to the advent of the early hackers, up to the computer virus programmers of today. We will also look at the onset of the scientific studies, namely Artificial Life and Synthetic Psychology.

The first media reports of computer viruses were littered with misunderstanding and fear. To this day, strange stories abound about what certain viruses will do to your system if you don't take certain precautions. A candid look at these "urban tales" will detail how the virus has become one of this century's biggest preoccupations.

Several recent media hoaxes are discussed. Many of the facts reviewed point to the main culprit of the virus epidemic: the anti-virus organizations themselves! Many of the the half-truths, and sometimes right-out lies about computer viruses, are exposed.

Does the anti-virus community really wish the extermination of computer viruses? The results of these studies suggests that they do not.

The authors of these viruses are seldom able to voice their opinions to the general public. Because of this, most of what is read is simple speculation or third party information. I have interviewed many virus writers from ten countries and four continents, and witness their activities in what has been termed "cyberspace". These interviews form the basis of the extension to this chapter.

Surprising answers will be given to the oft-repeated questions: "Who are the guys that write these viruses, and why do they do it?" Not all are the maladjusted prepubescent introverts the news reports would like us to believe.

Chapter 3

Another shocking truth is uncovered in this chapter: Any computer fitted with DOS 5.00 or DOS 6.00 contains an undocumented command very suited, and very able, to remove *any* Master Boot Record virus safely, and without damaging any of the other files on the system. If this command had been documented, the Stoned virus would be non-existent, and most of all, the Michelangelo scare would never have happened!

Methods of securing your data from damage caused by viruses or trojan horse programs are discussed in depth. The reader is taught how to get through a virus attack with minimum damage and wasted time. A Lesson in "Safe Hex" shows how no system needs to be vulnerable. A full section on data recovery is added to aid those who are unfortunate enough to have been attacked.

An easy-to-follow guide to various proprietary anti-virus techniques is outlined to allow the reader to draw educated conclusions as to the usefulness of such software. Certain techniques work better than others, while some techniques offer you nothing but the most basic of protection, and are virtually useless.

There are several functions that can be added to DOS and the BIOS that will completely eliminate the computer virus threat. Examples are given, and several questions are raised as to why none of these ideas have been implemented before. An effective anti-virus system modification is listed for the reader to install on their own system.

Results of an in depth study of various anti-virus products are impartially related. Through these results one can see the hard-sell tactics at work. Other tests and observations show the deficiencies of some of the many virus scanning products, and lead one to wonder if their producers really do know anything at all about the viruses they purport to scan for!

Chapter 4

The new catch-phrase in the computer industry is Artificial Life, and one half of this chapter is devoted to this. Artificial Life is the simulation of life-like properties through an inanimate medium. Studied is the complex emergent behaviour that forms from a few basic rules. Certain questions like "At what point can an object be considered alive?" arise and are discussed. Sources are borrowed from various biological texts to answer the very important question: What is life? Through it we can determine why science would want to attempt the creation of living matter out of non-living matter.

The book then delves into the obscure, but very powerful study known as Synthetic Psychology. This science is so closely related to Artificial Life that it is often difficult to tell the difference. Because of the very nature of Synthetic Psychology, great care must be taken to avoid retaliation from your experiments! As this is a very subdued science, many people are generally surprised when they read about the studies involved.

We then speculate about the future of these sciences, of computer viruses, and of the computing public. Following well established guidelines, we are able to show that computer viruses are very much alive, and may have legitimate uses in the scientific field.

Chapter 5

This, and the next chapter, are for the avid computer addict interested in hands-on experience with computer viruses. Part of the reason for the virus epidemic and the accompanying fear is the shroud of secrecy hanging obtrusively over every corner: the ignorance instilled upon all computer users.

As an example, all media venues warned us to avoid using our computers on March 6th, 1992 because of the Michelangelo virus. On this day the virus would format random areas of your computer's boot disk. This is one example of a Manipulation Task. The limits of possible damage are discussed here in a frank manner. It will become obvious, though, that with proper precautions, even the worst of manipulation tasks is not as severe as the press would lead you to assume.

This section also discusses many other technical feats, such as virus encryption, reproduction, anti-debugging and stealth techniques, and much more.

Chapter 6

This chapter contains the source code to several computer virus specimens. Special precautions have been taken so that none of the viruses pose any threat of getting out in the wild. Most of the viruses are scannable by the major anti-virus products. Two dangerous viruses are written with 386 assembly language. Execution on an XT or 286 computer will result in a system crash. This is to avoid any malicious use of the virus code.

The computer programmer will often be surprised to see that there is no magic happening within the virus code. Once these programs are well understood, it is obvious that most of the computer virus stories are media generated for hype and power.

In all cases, the code is extremely well documented to allow even non-programmers to understand to some degree what is happening.

The virus samples given are:

[DOS 7]	Prepending .COM virus with extreme Anti-Hack routines
[Lezbo]	Appending .COM/.EXE/.OVL stealth virus
[Michelangelo]	The infamous Boot Sector/MBR virus
[SYS Inf]	Rare .SYS file appending infector
[Little Mess]	Extremely Rare Telix script companion virus
[Proto 3]	Polymorphic appending .COM virus

Appendix A

Virus Writer's Code of Ethics

The Constitution of Worldwide Virus Writers - Initial Release - February 12, 1992

Appendix B

Debug Scripts

This appendix holds the debug scripts for every executable file listed in the book, plus instructions on how to use them to derive working copies of the files they mirror.

Appendix C

Dictionary of Computer Virus, Artificial Life, Synthetic Psychology, and Related Terms

Appendix D

Bibliography and Suggested Reading

*

This book is the most comprehensive, in depth look at the computer virus to date. As it holds no product affiliation, facts are clear and precise, and without bias.

Contact:

Author
Karsten Johansson
PC Scavenger
90 Cambridge Avenue
Toronto, Ontario
M4K 2L4

Agent
Ian Young
TMW Communications
2484 Gerrard St. East
Scarborough, Ontario
M1N 1W7