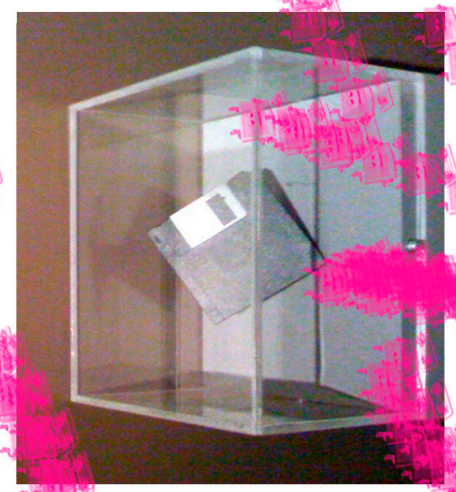


INTRODUCTION

This text is the outcome - and to a certain extend the documentation - of a series of performance lectures. Held between 2014-15 the lectures focused on a variety of computer viruses.
At the center was a certain interest focused on early examples of these viruses, surrounded by an experiment on how to think, speak about and display viruses. (WORK!)
Unsatisfied by the image and video documentation of these lectures, I decided to translate the lectures into this text and developed the objects on which it is stored.

ACKNOWLEDGEMENTS

A number have helped and support me on the lectures and this text.
Just to thank a few:
Karoline Achilles, Hans Bernhard, Post Brothers, danoct1, Sebastian Dürer, Frederic Ehlers, Ann-Charlotte Günzel, Neck Hood, Nina Kuttler, Hunter Longe, Leon Lothschütz, Christian Philipp Müller, Jero van Nieuwkoop, Neuer Saarbrücker Kunstverein, Johanna Schaffer, Daniel Stubenvoll

Imprint

Text: Fritz Laszlo Weber

Graphic Design: Fritz Laszlo Weber

Additional graphics: Karoline Achilles

Last updated: 03/08/16

fritz-weber.de/acab

On November 2 1988 Robert Tappan Morris started his newest program. At this point the Internet was still a young, rapidly growing network.

Morris was studying information technology at a US-American university. He wanted to find out more about the back—then unknown size of the Internet, using a self-replicating program he designed and developed. His goal was to figure out how many agents, machines and hubs had merged and consolidated so far.

The program had a simple structure. Once activated on an initial computer, it headed for other computers in its local subnet, its close environment. Upon arrival at new computers, the program raised a central count, left a marker, that indicated that the computer has been taken into account, and then moved on to the next computer and the next environments.
Two days later the internet was tottering. Computers, servers and entire subnets were paralysed and not responding anymore. Network administrators began to take computers offline as preventive measures in order to escape the virtual threat.
A threat, a danger, a risk, that was also echoed extensively in international media.

Morris' program circulated fast and the subnets it migrated through were smaller then expected. A programming failure by Morris caused situation where computers could be marked multiple times, actually endlessly. Computers couldn't perform their previously assigned tasks anymore and became inoperable.

When Robert Morris became aware of the unintended effects the program had, he tried to send instructions to various system administrators.

Instructions on how to block the program which by then has already been named Morris Worm.
But so many copies of the program, so many worms, were already circulating, that the message got stuck in jammed routes and hubs. The worm had rescued itself from its author.

In turn, the author was convicted a few months later as one of the first persons under the recently passed Computer Fraud and Abuse Act.[1] He was sentenced to three years of probation, community service and a monetary fine for the damage his program has caused.
Though the damage in this case was not caused by data loss or destroyed hardware, but was calculated from the caused loss of computing time at universities, companies, governmental organisations and military units.
The Morris Worm and his comrades slowly gained a new visibility on the radars of transforming network societies and information economies.
The replicating, autonomous, transforming and migrating programs became the spectres of the network societies, subsumed under the term computer viruses.

The biological virus as the name-giver for these new agent and actants[2] comes along with a variety of misleading translations, wrong assumptions and analogies from its source.
Viruses are understood as an unpredictable, invisible risk for every body. They are understood as especially viral — and therefore dangerous - the higher the density of relations in the networks are and it is hence fought with hygiene and order.
Following this logic, every computer unit is seen as a sole body in a temporary community of independent bodies. The individual

body must be kept unsullied and its accesses and entries must be tightly closed in case of doubt. Hence the network is understood primarily as a collection of loose, temporal connections. It is not seen as an entire, unsteady and rambling body incorporating other bodies and subjects in various constellations and relations.[3]
The network does not begin or end at the point of contact between the network adapter and the data cable or wifi signal. The network is part of the computers, once they are connected. It flows through all processing units, memories and wires. Its design works like an electricity circuit that needs to get closed in order to be conductive. In the process of connecting, all elements—computers, cables, hubs, users, scripts... —of this network flux establish protocols of exchange and correspond through common languages, they fuse, intertwine or interlock.

The Morris Worm was not the first bastard to challenge the understanding of programs and computer networks. And in the years after this occurrence, a scene around various programmers and developers formed developing programs that did not acknowledge the common understanding of the network, the dominant and imported rules and its arbitrary borders.

Similar to the graffiti culture that emerged a decade earlier in New York, existing territorial devisions were rejected, spaces reclaimed and occupied, and therefore authorities were constantly outsmarted and hacked.[4]
The graffiti piece as a circulating, public message in a network of tubes and stations. The virus as a circulating, public message in a network of cables and memories. The design and execution of the messages played a key roll to the respective reading community, as well as ideas of authorship and implicit or explicit political positing.

In turn, these messages were continuously labeled as vandalistic, hostile attacks by authorities, creating the perception of a never-ending plague. The computer viruses were thus located in a speech and thought matrix between health/disease (viruses) and peace/violence (trojans).
This grid is particularly cemented by commercial anti-virus software producers,who draw themselves through their public presentation, language and appearance as the good-willing opponent of the virus. Thereby creating an industry, that advertises the notion of digital security, reliability and well-being.

In the court ruling[5] of the Morris case the judges seemed to struggle with criminalizing terminology when describing Morris' actions and his program. They are particularly careful with the formative and now dominating terms and notions:

> *Morris released into INTERNET, a national computer network, a computer program known as a "worm"[1] that spread and multiplied, eventually causing computers at various educational institutions and military sites to "crash" or cease functioning. (...)*
> *[1] In the colorful argot of computers, a "worm" is a program that travels from one computer to another but does not attach itself to the operating system of the computer it "infects." It differs from a "virus," which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer.*

A decade after the Morris Worm, and many computer generations later, another important virus appeared on the screens of the globalized network society.
Shortly before the millennium, fears of a worldwide system crash were circulating as a lot of old computer models weren't capable of performing the time switch from 1999 to

2000. In the end the big crash of system-relevant machines during New Years Eve stayed absent, but actually six months later a love letter led to a global chain of trouble.

Starting from the Philippines on the morning of May 4 2000, copies of an email were quickly spreading westwards with the beginning workday. The email consisted of a short confession of affection by the sender and an attached love letter.
By opening the love letter attachment a script within the attachment was activated. The script started overwriting various files and finally started sending out love letters to every contact in the address book.

The love letter email later named I Love You Virus did not really make use of technical security gaps, but rather benefitted from the users curiosity.
And it spread remarkably fast in networks, that are designed to place people within fixed, stratified positions and relations.
On the afternoon of May 5 the CIA, the pentagon, the British Parliament and a variety of international cooperations had to shut down their email servers after they could not get hold of the love letter trouble.
The love letters between colleagues, bosses and interns from all branches and departments were double clicked with great interest and after ten days the virus had reached millions of inboxes and computers. The viral potential of the I Love You Virus was increased significantly by a massive flow of media and press reports. Fuelled by fear and panic and affirmed by anti-virus software vendors these reports spread as fast as the virus itself.
By now viruses caused not only a loss of computing time or data, but also created nervous markets and collapsing stock prices.
A computer virus replicated itself into other systems.

In the - again very simple - source code of the I Love You Virus, one could find this remarkable note:

> *barok ...i hate go to school suck->by:spyder @Copyright (c) 2000 GRAMMERSoft Group->Manila,Phils.*

The GRAMMERSoft Group was known among students for selling copied exam files from hacked computers of their professors at the AMA Computer University in Manilla. And as many other hackers, crackers and virus authors, the author had attached a signature, a tag to their piece. Especially in the light of the initial purpose of the virus, there is a certain irony that the author left a copyright remark attached to this self autonomous, replicating—i.e. copying—program. Through the GRAMMERSoft Group an investigators came across the thesis proposal of Onel de Guzman.

The IT student had proposed the design for a program, that would collect internet access passwords from privileged users and redistribute it to users who could not effort the back then still pricey internet access charges. The prototype for this program was the I Love You Virus. It was released premature and its actions were, similar to the Morris Worm again, only partially anticipated by the author. In the end, the virus had nested itself into 50 million computers and the calculated economy damage was an estimated 25 billion US-Dollars.

But authorities couldn't press for charges, as there were no laws in action that would criminalize Guzman's intentions or his programs behavior, yet.

Neither Guzman, nor anti-virus developers could stop the virus immediately, but through the vast circulation in the media the general public became aware of the virus and thereby the curiosity and naivety of the users, the basis of the viruses' success, came to an end.

Computer viruses exist and spread in a very fragile network constellation of computer models, software versions, webbed relations and knowledge accumulations. They come to life through these very constellations and end with certain constellation transitions.

At the same time viruses are not necessarily a single entity or identity, but alter themselves, enabled by polymorphic designs, or get altered, appropriated and transformed by other authors.
In the story of the I Love You Virus, months after its initial spread and lifetime, various viruses used successfully the same principles and even the same source code, often only varying on the teasing and promising message.

The I Love You Virus and its variations, like all other viruses, got their names not from its programmer or author, but through the discoverers, explorers and investigators. So in contrast to usual, author-based naming practices, as common in many cultures, here procedures became established that relate to the discovery and naming of new species, formations or places in various sciences. And similar to the naming procedures for celestial bodies or insects, regulations were put in place by the anti viruses community for naming and categorizing.

Whereas graffiti culture was male dominated, the community of virus authors was further defined by people with access to the respective technology–i.e. economically and academically privileged.
Onel de Guzman and Robert Tappan Morris had, beside their access to knowledge, technological equipment and networks, gained first experiences with computers long before their studies. Morris father was a computer scientist himself, among others for the NSA.
Looking at the pseudonyms of computer vi-

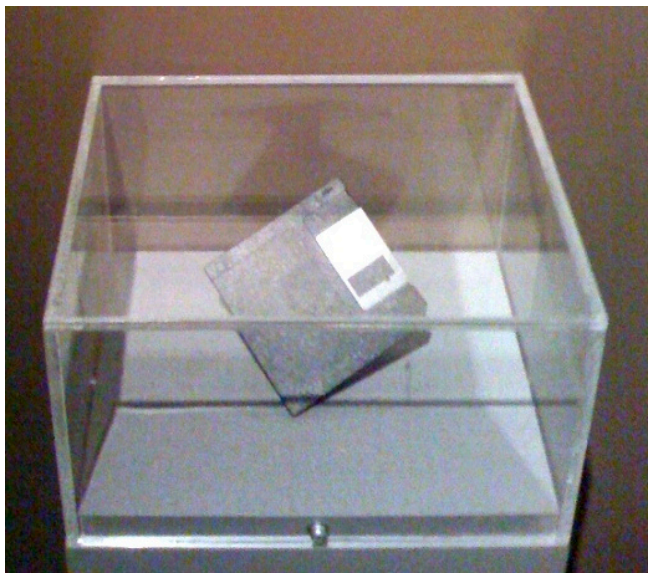
rus authors, most names can be understood as male connoted, sometimes referring to martial warriors, thereby contributing to a militarized understanding of viruses.

And until today there is no public known female virus author yet. This is presumably also due to the numbers of female IT students decreasing significantly in the late 80s in western countries. Whereas programming was a mostly female assigned task in the early stages of the computer age, female agents slowly got replaced with an increasing importance of the information technology sector. A bit more with every computer generation. First, knowledge and education was relocated, due to a rising complexity, to academic institutions with little access for women back then. Next the job of the programmer was reshaped as a stereotypical male one. And by the 80s, when women had fought for and gained better access to academia, home computing experience had become a unspoken precondition for studying IT. Home computers, though, were advertised as and shown in the pattern of a dad/son activity. So due to this constellations a massive drop in the numbers of female IT students was measured in the US, reaching its low point in the mid 90s. The same years, when the technological conditions were exciting for viruses. The internet had just began to grow out of its military-scientific roots, and especially the home computers contributed to a large part to this development. At the same, the internet had not reached its current importance for maintaining order in western state systems, global economies, and markets. These constellations opened up new spaces for various hacks and experiments, among them the computer viruses. The continuous development of software security led to a shrinking number of exploits, the so called security gaps that enable programs to travel and migrate between computers and

networks. These exploits became a rare and coveted good, with new markets emerging around them. People started selling exploits to make a living and others invested reasonable amounts to collect and make use of them. And so slowly the political, experimental, rebellious, and entertaining viruses vanished from the networks. What was left, were the viruses utilized for spam distribution, fraud, industrial espionage, and state intelligence services. They became the dominant model in this commodified environment.

But before this turn, a 90's exemplar of a virus spread via floppy disk, or rather via the personal networks, in which they were exchanged. The virus entered the back then common MS-DOS systems, a command line operating system without any special graphical user interface. The virus activates itself during a booting routine every now and then, starting to write slowly TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO TECHNO
TECHNO all over the screen, while a monotonous, repetitive techno song was played via the computers sound unit.[6] The users could only watch the performance helplessly until the screen was filled and the song was over. If they try to enter any key before, the text performance would pause and the virus would command the user: Don't touch the keyboard!. After the performance the computer reboots itself leaving not a single trace of its previous state of exception behind, until the next random time it would activate during startup.

Today the Morris Worm is exhibited at the Computer History Museum in Silicon Valley. Its source code is stored on a floppy disk locked away inside a vitrine. It’s a bit like in a zoo.



---

1. See case of Aaron Swartz to understand the full impact of this law in the next decades.
2. The broad range of programs that is categorized as viruses is equipped with various forms of functions, capabilities, intelligence and agencies. Hence computer viruses as category are not only either agents or actants.
3. There are various concepts and ideas trying to describe form(s) of computer and digital networks and the various relations within them. Since the form of the internet is constantly changing due to technological development and power shifts, and since this text is covering a fairly broad time span, I do not necessarily stick with one particularly, but rather emphasise the categorical misconception in the understanding of networks preached by anti-virus industry.
4. The Artistic Construction of a Counter-Culture, Rashaun Esposito, 2005
5. UNITED STATES of America vs. Robert Tappan MORRIS, United States Court of Appeals, Second Circuit, 1991.
6. TECHNO TECHNO TECHNO