

# Autoimmune computer virus

October 2005

Alberto Cammozzo  
mmzz -at- stat.unipd.it

# Autoimmune biological virus

«The immune system is a complicated network of cells and cell components (called molecules) that normally work to defend the body and eliminate infections caused by bacteria, viruses, and other invading microbes

If a person has an autoimmune disease, the immune system mistakenly attacks self, targeting the cells, tissues, and organs of a person's own body.»

NIH Publication No. 98-427 *Understanding Autoimmune Diseases* - May 1998  
<http://www.niaid.nih.gov/publications/autoimmune/autoimmune.htm>

# Antivirus aware computer viruses

«Many viruses are able to recognize certain anti-virus software, and respond differently to such software than to programs designed for other purposes.

Some viruses go after the databases stored by anti-virus products.

Some viruses simply go after anti-virus products, trying to erase them.»

David Stang – *Fighting Computer Virus Infection through Auto-Immune Responses - Applying Principles of Life to Anti-Virus Technology*  
<http://vx.netlux.org/lib/ads01.html>

# Autoimmune computer viruses (AICV) are not new

«Biological immune disorders in which host defenses turn against the host and actually cause damage are known as **autoimmune diseases**. Computer autoimmune disorders parallel their biological counterparts. Recently, a warning (defense mechanism used by computer users) turned out to be a not-so-harmless hoax. The hoax warning stated that certain files were infected by a computer virus. Heeding the warning, unsuspecting computer users removed the affected utility files from their computers' operating systems .»

Trudy M. Wassenaar and Martin J. Blaser – *Contagion on the Internet* – Letter to Emerging Infectious Diseases Journal , **March 2002** - National Center for Infectious Diseases

<http://www.cdc.gov/ncidod/EID/vol8no3/01-0286.htm>

# How an antivirus works

- Each **antivirus firm** has its own *antivirus database file*:
  - containing viruses definitions or *fingerprints*,
  - updated when needed (e.g. new virus comes up).
- **Antivirus client** downloads frequently the updated *database file* from the antivirus' producer web/ftp *servers*. **Antivirus engine** runs on client's PC/server with the updated definitions of viruses from the new *database file*. **Antivirus client** will remove or quarantine files which *fingerprint* is in the updated *database file*.
- In **corporate** context there usually are *intermediate servers*.

# Threats exploiting the antivirus itself

- We already have malware that interferes with antivirus systems, preventing detection.
- What happens if the *virus database file itself* can be corrupted?
  - Misleading effect on antivirus's behaviour.
  - Making the antivirus itself damage the system it is intended to protect.

# Possible actions from an AICV

- Deletion of non-viral files from the file-system, **adding** their fingerprint in the *database file* file.
  - e.g. an antivirus treating as infected files beginning with string '**MZ**' will delete all .EXE files.
- Allowing viruses to spread, **removing** their fingerprint from *database file*:
  - prevents detection of viruses that otherwise would be detected.
  - enables a perfect virus time-bomb: the virus silently floods the net, undetected, activating itself at a given time.

# What AV producers should do

- Technical:
  - Having the *database file* digitally signed (not encrypted) and keys properly managed.
- Make us know:
  - how virus database files are digitally signed, so that anyone can verify them,
  - how virus database files and keys are managed, to check them.
  - please, show us the **source code**.



# What we can do

- Avoiding the dangers of **software monocultures**:
  - Push **BITdiversity**: Biodiversity applied to IT environment: don't stick to a single O.S.
  - Beware of antivirus monopoly.
- Rethink **redundancy**:
  - OS redundancy: push multiple different operating systems on the key servers and clients. If the virus attacks one OS, the other will likely be safe. Traditional redundancy will fail.
  - Avir Redundancy: having multiple simultaneous antivirus systems with different signature files.
- Keep the **data** safe.
  - be prepared to access to your data from a different OS.
  - avoid proprietary data formats as hell.

END