Response to the Proposal for a "C-Virus" database[1]

Morton G. Swimmer

Virus Test Center
Faculty of Computer Science
University of Hamburg
Schlüterstr. 70
D-2000 Hamburg 13
Telephone: +49-40-4123-4162
or: +49-40-4910247 (private)
e-mail: swimmer@fbihh.informatik.uni-hamburg.de

Keywords: computer viruses, classification

Abstract

Dr. Daniel Guinier presented a proposal for a computer virus database in the Fall 1989 edition of **SIGSAC (Volume 7, Number 3)**. In this article a form of virus classification is presented that has been used with some success for nearly two years. Furthermore, future developements in the field of virus classification are outlined.

Introduction

As Dr. Guinier quite rightly pointed out, computer virus classification is needed as an early warning information source. The number of known viruses is growing rapidly. By early 1990 we knew of about 200 viruses, of which over 90 are on IBM-PC's, over 40 on Amiga, at least 25 on Atari, and over 25 on MacIntosh. Extrapolating the developement, by 1994/95 we will have more than 1000 computer viruses!

To deal with this problem, the computer user must have a minimum amount of information to be able to determine whether anomalous behaviour can be attributed to a virus. The computer virus catalog comprises of such information necassary to identify a known virus.

The **Virus Test Center** was started in May 1988, by Klaus Brunnstein. At the time it was one of the first such projects. The goal of the group was to combat the growing problem of computer viruses by gaining insights into their functionality.

The **Computer Virus Catalog** was created by Klaus Brunnstein, who is the publisher, together with the valuable help of D. Ferbrache, C. Fischer, Y. Radai, and F. Skulason. It deliberately does not contain enough detail of virus programming techniques to be of much use for virus programmers, thus following the IFIP decision that strongly advises against the publication of virus code.

VTC Computer Virus Catalog 1.2

The first draft of the Computer Virus Catalog (version 1.0) was created only months after the project was started in May 1988. We felt that a detailed, well structured classification would be of great use, not only to ourselves, but also to other virus researchers. In fact, they responded with comments and suggestions which ultimately resulted in the present version 1.2, by early 1989.

The **Computer Virus Catalog** was intended to describe viruses in enough detail so that a user can positively identify a possible virus attack. The catalog distinguishes between 'System' (boot sector, system files, etc) and 'Program' viruses, as well as giving various other finer details of the virus.

---

1 Parts of this paper are derived from [Brunnstein/Fischer-Hübner/Swimmer 90]

In its current format (version 1.2) the Computer Virus Catalog [Brunnstein 89] contains the following information (a full description is contained in the Appendix):

- General information: name, aliases, strain, when and where detected, general classification.
- Precondition: System and models, operating system and versions.
- Easy identification: eg. texts displayed or stored.
- Infection mechanisms, media affected, triggers.
- Modification of the operating system: eg. interrupts hooked.
- Damage: perminent/transient, triggers, special effects.
- Similarities with other viruses.
- Countermeasures as divided into the 6 catagories:
  - Category 1: Monitoring of files, system vectors or areas
  - Category 2: Alteration detection
  - Category 3: Eradication
  - Category 4: Vaccine
  - Category 5: Hardware methods
  - Category 6: Cryptographic methods (hard/software)
- Tested countermeasures and standard means
- Acknowledgements

As the number of antivirus products grows every day, it quickly became impossible to test all of them. Until now, only our own antiviruses have been mentioned in the catalog. We hope to include the major antivirus packages in the future.

The catalog is available from various archive servers, or by email from either Klaus Brunnstein or myself. Within Germany, one can access the "Infobox", a local Mailbox, where the latest catalog entries are stored. The catalog is updated periodically. Unfortunately we were not granted permission to use mailing lists, or build our own archive server at the university. For this reason we have difficulties distributing the catalog widely and quickly within our own facilities[2].

Further work on computer virus classification

The Virus Test Center is following a number of possibilities to enhance the catalog and classification in general.

We hope to bring out a new and more precise version of the present catalog soon. This version will most likely be more system specific, to allow for infection mechanisms native only to a certain types of machine platforms. It will attempt to become more precise, so as to avoid misinterpretations.

At the same time we will develope a machine readable version of the catalog. This will result in easier access to the data in the catalog. As the number of viruses grow, this will become vital to the functioning of such a database. One possible means of distributing the information would be to use the existing electronic mail services. The body of the mail would be an entry, which would be automatically processed. This could be expanded into a global distributed text database.

A lot of thought is being put into the possibility of creating a virus description language, that we have preemtively dubbed "**Threat Description Language for Viruses**" (**TDL/V**). This could make up part of the a priori rules used by a virus detection system. Such a system could possibly detect viruses not yet in the knowledge base, using only behaviour patterns of know viruses.

---

2 As Cohen said: "...I would like to thank all those who stood in my way. I just want them to know that I haven't forgotten them." (sic) [Cohen 86]

Conclusion

The Computer Virus Catalog was created to maintain a high standard in the classification of computer viruses. For a long time we were alone in using this format, but there were not that many viruses about. In the mean time we have been swamped by viruses and have not been able to keep up with the classification of them. In this situation we are grateful for people who have helped us by handing in catalog entries for viruses. Possibly a large distributed computer virus catalog would encourage more virus researchers to classify their findings, so that less work is repeated by researchers around the world. For this to be a success we will need ideas from the community, which is why I can only encourage discussion of this topic in any forum.

I wish you a virus free future!

Literature

[Brunnstein 89]
Klaus Brunnstein: "Zur Klassifikation von Computer-Viren: Der 'Computer Virus Catalog'", Proceedings of the 19th GI's (German Computer Science Association) Annual Conference

[Brunnstein/Fischer-Hübner/Swimmer 90]
Klaus Brunnstein, Simone Fischer-Hübner, Morton Swimmer: "Classification of Computer Anomalies", Draft Paper for the National Computer Security Conference 1990 in Washington D.C.

[Cohen 86]
Fred B. Cohen: "Computer Viruses", doctorate dissertation, University of Southern California, December 1986.

[Fischer-Hübner/Brunnstein 89]
Simone Fischer-Hübner, Klaus Brunnstein: "Das Virus Test Centrum an der Universität Hamburg", Proceedings of the 19th GI's (German Computer Science Association) Annual Conference

[Swimmer 90]
Morton Swimmer: "PC-Viren, Würmer, und Trojanische Pferde", Hamburger Computer Tage, January 1990.

[Weiner 90]
Michael Weiner: "Notes on a 'Virus Description Language'", March 1990

Appendix

```
----- Computer Virus Catalog 1.2: "Virusname" (Date of Entry) --------

Entry..............: "Virusname" (=Name of virus)
Alias(es)..........: Alternate Name(s)
Virus Strain.......: "Family" (if any) to which this virus belongs
Virus detected when.: Date of first appearance
              where.: Where was Virus produced or first detected
                      (both entries only if well-known)
Classification.....: System Virus (BootSector, Command.Com, BAT V.)
                      Link or Program Virus (Overwriting/Extending V.)
                      Resident, Direct Action
Length of Virus....: 1.Length (Byte) on storage medium
                      2.Length (Byte) in RAM

-------------------- Preconditions ---------------------------------

Operating System(s).: e.g. AMIGA-DOS, ATARI-TOS, MacOS, MS-DOS,
                           UNIX, VMS, MVS, VM
Version/Release.....: Special Version of OS (e.g. UNIX System V,
                      UNIX BSD, VMS etc) if needed, and Release
                      (e.g. MS-DOS 3.2, UNIX BSD 4.2)
Computer model(s)...: The Computer models (e.g. ROM BIOS versions)
                      on which the Virus runs.

--------------------\ Attributes ----------------------------------

Easy Identification.: if applicable: Typical texts, either messages
                      (e.g. screen), or texts in Virus body (readable
                      with HexDump-facilities), Volume Labels etc.
                      by which viruses may easily identified
Type of infection...: Self-Identification methods;
                      Executable File infection(.COM,.EXE):overwriting,
                      extending; resident; (RAM/File) Direct Action;
                      WCS infection (e.g. CMOS at initialisation setup);
                      System infection: RAM-Resident, Reset-Resident,
                      Bootblock/Bootsectors, Command.Com, BAT, Device
                      Handlers/Libraries etc;
                      Infection of unlinked Object Files;
                      Source Code Infection.
Infection Trigger...: e.g. time/date, other events, random, reset (CTRL+
                      ALT+DEL), operations such as: DIR, execution of
                      specific program (.COM/.EXE).
Storage media affected: Infection of (particular) diskettes, hard disks,
                      DiskPacks, etc.
Interrupts hooked...: Interrupts used and changed by this virus.
Damage.............: Permanent Damage: e.g. overwriting bootblock,
                      repeated restart/format, zeroing of sectors,
                      Bad Sectors in FAT etc;
                      Transient Damage: e.g. screen buffer manipulation,
                      audio effects, blinking LEDs;
                      Transient/Permanent Damage: viruses which (under
                      specified conditions) produce parmanent damage
                      while "normally" producing transient damage.
Damage Trigger.....: e.g. time/date, value of infection counter, other
                      events, random, reset, operations.
Particularities.....: special effects e.g. process velocity slowed-down
Similarities........: dis/similarities to other viruses ( either from
```

same "family" (=strain) or different viruses);
names of related viruses.

---------- Agents ----------

Countermeasures.....: *Names of tested products of Category 1-5:*
Category 1: .1 Monitoring Files: program which monitors (attempted) changes in files
.2 Monitoring System Vectors: program which monitors changes in vectors (e.g. resident, interrupt vectors)
.3 Monitoring System Areas: program which monitors System Areas such as BootSectors/Blocks.
Category 2: Alteration Detection: a program which detects changes in given files
Category 3: Eradication: a program which erases a specific virus code from files or from RAM (if resident)
Category 4: Vaccine: a program which alters files (on permanent storage) or RAM resident programs such that viruses regard them as already infected
Category 5: Hardware Methods: methods to detect or prevent alteration or infection of files, vectors or system areas.
Category 6: Cryptographic Methods (Hard/Software): methods keeping programs on storage in encrypted form, and decrypting them before execution.
Countermeasures successful: *Names of those countermeasures (of given category) which, without (or with known "small") restrictions or side effects, were "successful" to detect, identify, inactivate or erase the given virus or exclude infection by it.*
Standard means......: *Means in the respective System which may be used to identify/destroy this virus.*

---------- Acknowledgement ----------

Location.....: *e.g. Virus Test Center, University Hamburg, FRG*
Classification by...: *Author(s) of Reverse-Engineering Document*
Documentation by....: *Author(s) of this Catalog Entry;*
Translator of Non-English document (if applicable)
Date.....: *Production/last Update of this Catalog Entry (this information also in the 1st line)*
Information Source..: *Information used for Documentation (only in cases where Reverse-Analysis was not possible).*

----------End of "*Virusname*"-Virus----------