Anhang A - Zusätzliche und genaue Angaben zum Verfahren des Virus Test Centers

In diesem Anhang wird das VTC-Verfahren durch zusätzliche, detaillierte Informationen dokumentiert. Diese Angaben ergänzen die Beschreibungen des VTC-Verfahrens aus Kapitel 4. Im einzelnen finden sich folgende Dokumentationen:

Diese detaillierten Dokumentationen stammen aus dem VTC-Testbericht zum Test 2001-10 oder von der Homepage des Virus Test Centers[1]. Dementsprechend - da es sich bei den VTC-Tests um internationale Veröffentlichungen handelt - sind die Angaben in englischer Sprache.

Die in A.1 bis A.4 aufgelisteten Dokumentationen und weitere Informationen zum VTC sowie sämtliche Testberichte[2] sind auf der Homepage des Virus Test Centers verfügbar:

http://agn-www.informatik.uni-hamburg.de/vtc/

[1] A.1 aus [VTC 2001-10a], A5CodNam
A.2 aus [VTC 2001-10a], 4TSTCON.TXT
A.3 findet sich links oben auf [VTC 2002]
A.4 aus [VTC 2001-10a], 5PROTOCO.TXT

[2] ab 1997

A.1 Verwendete Abkürzungen für teilnehmende Softwareprodukte

```
========================
Content of file A5CodNam
  aVTC Test 2001-10:
========================

This file contains the (3-character) code used to identify products
in VTC tests (esp. including those in test "2001-10").

                                                    in VTC test
  ---------------------------------------------------------------
  ALE = Alert (Accura)                          1997-02 ... 1998-02
  ADO = AntiDote                                2001-04
  ANT = AntiVir (H&B EDV)                       1997-02 ... 2001-10
  ANY = Abyware                                 1998-10
  AT5 = Anti-Trojan 5                           2001-04
  AVA/AV3 = AVAST (32)                          1997-02 ... 2001-10
  AVG = Grisoft AntiVirus                       1997-02 ... 2001-10
  AVK = AntiVirus Kit (GData)                   1998-10 ... 2001-10
  AVP = AVP (Platinum)                          1997-02 ... 2001-10
  AVS = AV Scan (H&B EDV)                       1997-02 ... 1997-07
  AVX = AntiVirus eXpert                        2000-08    2001-10
  AW  =                                         1998-02
  CLE = Cleaner                                 2001-04
  CMD = Command Software AV                     2000-04 ... 2001-10
  DRA =                                                     2001-10
  DRW = DrWeb                                   1997-02 ... 2001-10
  DSE = Dr Solomon Emergency AV                 1997-02 ... 2001-10
  ESA = ESafe (Aladdin)                         2000-04
  FPR/FMA = FProt/FmacroW                       1997-02 ... 2001-10
  FPW = FProt FP-WIN                            2001-04
  FSE = F-Secure AntiVirus                      1998-02 ... 2001-10
  FWN = FWin                                    1997-02 ... 1998-10
  HMV = HMVS (Valky/Vrtik, Slowakia)            1998-02 ... 1999-03
  IBM = IBM AntiVirus                           1997-02 ... 1998-02
  IKA = Ikarus AntiVirus                                    2001-10
  INO = Inoculan (CAI)                          1998-02 ... 2001-10
  IRS = IRIS AntiVirus (Iris, Israel)           1997-07 ... 1999-03
  ITM = Integrity Master (Stiller R.)           1997-07 ... 1999-03
  IVB = InVircible (NetZ)                       1997-02,   1998-10
  MKS = MKS-vir (Polonia)                       2000-04
  MR2 = MR2S                                    1999-09,   2001-10
  MCV = Main Channel W2kScan                                2001-10
  NAV = Norton AntiVirus                        1997-02 ... 2001-10
```

NOD = NOD (eset Software Slowakia)	1998-02 ... 2000-04
NVC/NVN = Norman Virus Control	1998-10 ... 2001-10
PAN = Panda AntiVirus	1998-02
PAV = Power AntiVirus	1997-07 ... 2001-10
PCC = PCCillin (TrendMicro)	1997-07
PCV = PC Vaccine Professional (UK)	1997-02
PER = Peruvian AntiVirus	2001-04
PRO = Protector	2001-04
QHL = QuickHeal	2001-04 ... 2001-10
RAD = RAV/DOS	2001-10
RAV/RA7 = Rumanian AntiVirus	1999-03 ... 2001-10
SCN = NAI VirusScan	1999-02 ... 2001-10
SWP = Sweep = Sophos AntiVirus	1997-02 ... 2000-04
TBA = Thunderbyte AntiVirus	1997-02 ... 1998-10
TSC = TScan (Marx Germany)	1998-02 ... 1999-09
TNT = TNT (Carmel, Israel)	1997-02
UKV = Ultimate Killer Vaccine	2000-04
VBS = Virus Buster (Leprechaun)	1997-02 ... 1998-10
VDS = Perforin (Adv.Res. Group)	1997-07 ... 1998-02
VET (Cybec Australia)	1997-02 ... 1999-03
VHU = Virus Hunter	1997-02
VIT = VirIT Explorer Lite	2000-04
VSA = Virus Safe (Eliashim Israel)	1998-02
VSP = VirScan Plus (Ralph Roth)	1998-10 ... 2001-10
VSW = Virussweep (Quarterdeck USA)	1998-02
VTR =	1997-02
XSC = XScan	1997-02

A.2 Bedingungen für am Test teilnehmende Softwareprodukte

==========
File 4TSTCON.TXT
Conditions for scanners to conform
with VTC test procedure:
==========
Formatted with non-proportional font (Courier)
Remark: Test conditions: NO changes since VTC test "2001-04"

In order to be testable under VTC test conditions, a scanner must conform to the set of conditions listed below. These conditions are the essential basis for processing parallel test batches without manual intervention. Moreover, automatic evaluation of huge scanner log files are performed with awk-scripts. We regard these conditions to be fairly reasonable, not too restrictive, as well as being useful for both users and developers because they allow them to understand and analyse VTC tests more easily.

Several of the scanners in this test did NOT conform to those conditions. Very few even had to be withdrawn from the test, whereas several required "manual support". The task to test such non-conforming scanners is very difficult and time-consuming.

Here is the list of conditions:

A) Common conditions (AA-AB, A1-A9)
F) Conditions for tests against file viruses (F1-F3)
B) Conditions for tests against boot viruses (B0,B1,B1a,B2)
M) Conditions for tests against macro viruses (M1-M2)
W) Conditions for tests against malware (W1)
P) Conditions for testing virus detection in packed files (P1)

A) Common conditions:

AA) Essential parameters or options under which the scanner produces optimum detection results should be available to the tester.

AB) The scanner must perform its detection tasks within reasonable time, compared to similar products.

A1) The scanner must be able to create a report file in a specified directory (at least not on that drive where viruses are located).

A2) The full path of scanned files must be present in the report file. Long paths MUST NOT be abbreviated, e.g. by using "..." instead of several intermediate directory names. Shortening file paths is acceptable when displaying them on the screen, but *not* in the report file.

A3) The scanner must be able to run in "scan-only" mode. If its default mode is to disinfect automatically all viruses found, there must be an option to run it in "scan-only" (i.e., NO disinfection) mode.

A4) The scanner must be able to run unattended - and they must NOT stop on each infected object and request user input. When scanning is completed, the scanner must be able to exit automatically and not wait for additional user intervention (including return keys).

A5) The scanner must be able to run from the command line (DOS versions only), scan a subdirectory tree (not just whole drives) and create a report file with a name and location supplied by the tester.

A6) If the scanner issues an audible alarm each time when it detects a virus, there must be a way to turn the sound off. This is not necessary if the alarm is issued only once - at the end of the scanning, but the alarm should be able to stop on its own, i.e. without requiring user intervention.

A7) The only limit of the size of the report file that the scanner creates must be the amount of free disk space.

A8) The scanner must be able to test objects on netdrives and obey the given user rights (i.e. read only, access denied).

A9) The scanner must not move any file which it regards as infected to another drive or a specified directory.

F) Conditions for tests against file viruses:

F1) The report file must contain the directory path and the file name of the suspious or infected file.

F2) The scanner must be able to scan files with extensions defined by the tester, or it must at least be able to scan files with extensions COM, EXE, SYS, BAT and CMD.

F3) The scanner must be able to run without problems on a huge directory tree - it should not be a problem to handle around 30,000 directories containing 100,000 files.

Remark: these conditions apply also to tests of special file viruses, such as of selected Polymprphic and VKit viruses.

B) Conditions for tests against boot viruses:

B0) The scanner must be able to scan under SIMBOOT.

B1) It should be possible to scan multiple diskettes without leaving the scanner. The scanner should prompt the tester to change the diskettes. It must request ONE AND THE SAME input from the tester between two diskettes, regardless of whether a virus is found or not. If the scanner does not have the option to scan multiple diskettes, it must have the option to append the results of the scanning procedure to an existing report.

B1a) If the scanner doesn't work with Simboot, it must be able to scan the images directly.

B2) The report file generated when scanning multiple diskettes must contain information about all scanned diskettes - not only about the infected ones, and not only about the last one.

M) Conditions for tests against macro viruses:

M1) The scanner must be able to scan macro viruses.

M2) The report file must contain the directory path, the file name of the suspious or infected file.

W) Conditions for tests against malware:

W1) The scanner must be able to scan for any file including non-self replicating malware such as trojan horses, virus droppers, first generation viruses, (network) worms, hostile applets etc.

P) Conditions for testing virus detection in packed files:

P1) The scanner must be able to scan for viruses in files compressed with ZIP, ARJ, LHA and RAR.

Added in Test "2001-02": WinRAR and CAB.

Q) Conditions for other classes of viruses:

In test "2000-08": testbed for script viruses (VBS, JS, mIRC) added.
Same conditions as for macro viruses apply.

In test "2001-04": testbed for exotic viruses (OS/2, Linux, Java) added.
Same conditions as for macro viruses apply.

A.3 Grundsätze zum Arbeiten mit bösartiger Software

==========
VTC Code of Conduct
==========
(Status: June 2001)

This code adresses those members of staff and students working in projects at Virus Test Center of Faculty for Informatics at Hamburg university. This code is relevant for any research or other work related with viruses and other forms of malicious code.

The purpose of this code is to protect persons inside and outside VTC laboratories as well as all technical equipment, esp. including hardware, operating and network systems, databases, test environments and application software. Moreover, this code shall inhibit (as far as possible) any side-effect of research and work with malicious code on any other person or technical equipment outside VTC.

This code also applies to students working in courses and exercises concerned with teaching, learning and training methods of Reverse Engineering. In these projects, additional requirements regarding the protection of Intellectual Property of systems or products in question apply (not listed in VTC CoC).

Rules:

R.01) Be always aware that work with viruses and other forms of malicious code bares a significant risk. Be therefore always prepared for recovery actions.

R.02) Always do your best to properly separate your working environment (hardware, systems and system software, network, application programs, databases, tools) from all other environments which is not needed to pursue your goal.

R.03) Follow VTC rules for separation of networks and use related techniques (local hubs and switches to connect relevant clients and servers, and to effectively disconnect any other component). Never run any experiment with viruses or other forms of malicious code with ANY connection to ANY other local or global

network (Internet).

R.04) Always work with best possible care. Always document any relevant step or procedure, to support analysis of failed experiments.

R.05) Any form of acquisition of viruses or other forms of malicious software for experimental purposes (e.g. via Internet) is only permissible for actions related to VTCs mission. This esp. includes analysis of emerging malicious threats as well as developments of methods, tools and and software to counteract related threats.

R.06) It is the privilege and duty of VTC management to properly maintain a collection of viruses on different platforms as well as of other forms of malicious software.

R.07) Viruses and other forms of malicious codes may NEVER be transferred (in ANY form, whether executable or not) to anybody outside your project except with explicit agreement of VTC management.

R.08) Generally, transfer of viruses and malicious code or essential technical information about viruses and malicious code is only permissible to a given expert with known or assured professional knowledge, when s/he convincingly argues that s/he needs that specific code to pursue her/his work in helping to protect others from viral or malicious risks, and provided that there is sufficient (positive) evidence that the related expert is trustworthy.

R.09) Never work with any person on viruses or malicious code when you can NOT be sure that s/he qualifies for such work (see R.08).

R.10) Never work with authors of viruses or malicious code (it is permissible to interrogate such authors if this doesnot help them in pursuing their malevolent work).

R.11) Never work with persons eXchanging viruses or malicious code (VXers).

R.12) Always try to inform the public about risks arising from writing and disseminating viruses and any other forms of malicious code.

Violations of Rules, Sanctions:

It is the duty of VTC management to analyse any disregard

or violation of these rules. Any related analysis shall not only collect and assess any relevant aspect but also give any person a fair chance for presenting her/his views. Sanctions shall be adequate, and they may range from warning to exclusion from VTC work.

A.4 Testumgebung

```
========================
File 5PROTOCO.TXT
AV Product Test Protocol:
========================
Formatted with non-proportional font (Courier)


This document specifies the test procedures applied to test the
precision of detection as well as the reliability of detection of
PC-based boot, file and macro viruses. Moreover, test procedures
for determining detection of packed viral objects and non-viral
malware are also described. Where relevant, details concerning
differences against previous VTC tests (esp.2000-04/08) are given.


1) Hardware and System Software used:
-------------------------------------
Test "2001-10" installation differs from last test (2001-04) essentially
in updated testbeds (which were frozen on April 30, 2001), and that it
tests macro and script viruses/malware only.

Again, the detection of viral code in packed (file and macro) objects
was tested for the set of In-the-Wild viruses, including 6 popular
packers (ZIP, LHA, ARJ, RAR, WinRAR, CAB). Moreover, a set of non-malicious
objects was used to determine the ability to avoid false-positive warnings,
and a special (file/macro) malware database was included to determine the
degree to which trojan horses are detected.

As in test "2001-10", 5 platforms (DOS, W-98, W-NT, W-2000, Linux) were used.

The databases of macro and script virus and malware were stored on a
Windows NT 4.0 SP5 server:

   Win-NT Server (1) has the following hardware:
      Pentium 200 MHz, 64 MB RAM, 2 GB hard disk (boot)
                       2*4,3 GB data/reports,
                       2*9,1 GB virus database (mirror)
            3 network cards: 2*100 MBit/sec, 1*10 MBit/sec
      Protected against electrical faults (USV: APC 420 VA)
      Operating system: Windows NT Server 4.0 SP 6

   Network:       1* 10 MBit/sec BNC for 20 DOS clients
            1*100 MBit/sec via 2 cascaded switches
```

for all other clients with 10 MBit/sec cards
1*100 MBit/sec via 100 MBit/sec hub for all other clients

Additionally, 25 clients (15 MS-DOS, 9 for Windows platforms: Win-98, Win-NT and W-2k, and 1 Linux) were used for the test. DOS-Clients work on MS-DOS 6.22. Hard disks are only used for the boot process. All W32 client works under English version. Win-NT clients work under Windows NT 4.0 Workstation with SP 5, English version. All clients are connected to the server using Microsoft NetBUI.

Generally, clients were flexibly allocated to optimize scanning processes. As the test is performed in a university lab, with no additional funding from elsewhere (we also do NOT request AV producers to pay any fee for our tests!), our hardware may not be regarded "the best possible":

DOS Clients (15) have the following hardware:

15* Intel 80486 DX2 50 MHz, 16 MB RAM, 270 MB hard disk, 10 MBit/sec
switched to 5 monitors over switchboard
software: MS-DOS version 6.22

Windows Clients (9) have the following hardware:

2*Pentium 133 MHz, 64 MB RAM, 2 GB hard disk, 10 MBit/sec
Pentium 90 MHz, 32 MB RAM, 1 GB hard disk, 100 MBit/sec
Pentium-II 350 MHz, 64 MB RAM, 2 GB hard disk, 100 MBit/sec
Pentium 233 MMX MHz, 64 MB RAM, 2 GB hard disk, 100 MBit/sec
Pentium-II 233 MHz, 64 MB RAM, 4 GB hard disk, 100 MBit/sec
Pentium-II 350 MHz, 64 MB RAM, 4 GB hard disk, 100 MBit/sec
Pentium MMX 233 MHz 196 MB RAM, 4 GB hard disk, 100 MBit/sec
Pentium III 128 MB RAM, 4 GB hard disk, 100 MBit/sec

Linux Client (1) has the following hardware:

Pentium 166 MHz 64 MB RAM, 100 MBit/Sec
System: Linux (SuSe) Professional 7.0

BTW: any donation of related hardware will be warmly welcomed by VTC test team.

Specially developed software supporting semi-automatic execution of test scans and evaluation of protocols consist of batch programs and scripts (PERL and AWK). Some UNIX programs like AWK, GAWK, JOIN etc have also been applied.

2) The Databases of Macro and Script viruses:

An overview of entries in the VTC virus databases (status: April 30, 2001) is given in Appendix 3: "A3TSTBED.zip" and A4TSTDIR.txt. TESTBED.VTC contains the following entries (in ZIPped form):

1) In-The-Wild Testbeds:

ITW-MACR.VTC content of ITW macro virus testbed
ITW-SCRI.VTC content of ITW script virus testbed
PAC-FILE.VTC content of packed ITW file virus testbed
PAC-MACR.VTC content of packed ITW macro virus testbed
FP-MACR.VTC content of Macro virus FalsePositive Testbed

2) Zoo (=full collection) Testbeds:

ZOO-MACR.VTC content of full macro virus testbed
ZOO-SCRI.VTC content of full script virus testbed
MAL-MACR.VTC content of macro malware testbed
MAL-SCRI.VTC content of script malware testbed

These entries (which also indicate the multiplicity of infected objects in the resp. directory) also conform with related entries in scanner evaluation protocols.

The macro virus database is organised according to the CARO macro naming convention. Related testbeds contain macro viruses known at end-April 2001 (see VTCs List of Known Macro Viruses). For each macro virus, different goat documents were stored to test consistent identification and reliable detection.

Contents of the macro virus database:

6,762 different macro viruses
21,667 files infected each with exactly ONE macro virus
143 different macro viruses reported "In-The-Wild"
1,308 files infected with exactly ONE ITW-virus
80 ITW macro viruses in 672 infected objects, packed with one of 6 packers (ZIP,LHA,ARJ,RAR,WINRAR,CAB)
329 totally non-malicious/non-viral objects in 26 different directories for fp-test

With fast deployment of script (esp. VBS) viruses, a special testbed for script viruses was developped (the content of which is reflected in VTCs List of Known Script Viruses).

Contents of the scriptvirus database:
---

588 different script viruses
1,079 files infected each with exactly ONE script virus
19 different script viruses reported "In-The-Wild"
110 files infected with exactly ONE ITW-virus

2B) Additional Macro Malware Database:

Concerning non-viral macro malware, this is well documented (see VTCs "List of Known Macro Malware" which summarizes both viral and non-viral macro malware). This testbed included:

426 specimen of macro malware in 683 different directories.

2C) Additional Script Malware Database:

Concerning non-viral script malware, this is well documented (see VTCs "List of Known Script Malware" which summarizes both viral and non-viral script malware). This testbed - which is used for the first time - included:

22 specimen of macro malware in 30 different directories.

2C) Additional test for False Positive Detection:

In order to test the ability of scanners to avoid "false positive" alarms on non-malicious non-viral objects (files and macros), 2 sets of "clean" objects were mixed into the resp. viral databases.

Clean files collected from several CD-ROMs were used for tests:

664 non-malicious non-viral objects (*.exe, *.com etc)
were stored in 27 different directories.

The list of CD-ROMs used for false positive testing is listed in appendix 3 (A3TSTBED.ZIP).

Concerning testing for false positive alarms on macro viruses, a set of
329 non-malicious non-viral objects (*.doc, *.dot, *.xls)
were stored in 26 different directories.

Remark: concerning copyright of related CD-ROMS, we use selected active content to help protecting the copyright holder for wrong allegations

concerning false alarms. We never use the code actively but only for assurance that scanners dont falsely alarm on these samples.

6.) Testing scanners on standard database of Macro Viruses:

All AV scanners are tested against two large macro-related database. The main database contains all "zoo" and ITW macro viruses, both in uncompressed and compressed forms; mixed into this database, there are also specific directories containing non-viral macro objects for false-positive detection. The second (smaller) database contains all non-viral macro malware (trojans, droppers, intendeds etc). All malware included in those databases matches the contents of the VTC Macro Virus List, which is published regularly (previously: monthly, now at the end of each quarter) For details, see http://agn-www.informatik.uni-hamburg.de/vtc.

The malware database contains also some file viruses which are being created ("dropped") by macro viruses. We decided to test them in the context of the macro malware test because they only appear in the context of macro malware.

The directory structure of the virus database reflects the CARO naming scheme for macro viruses with all samples of one variant stored in one subdirectory. Starting from the root directory of the database, the first level contains directories describing the host software (Word, Word97, Excel, Excel97, Lotus123, AmiPro). The second level contains subdirectories with the names of the families of the viruses and the next level hosts subdirectories of all variants of that family, in which the viruses can be found. Optionally (only in malware database), we have another subdirectory called "FILE" which contains the file viruses mentioned above.

The number of samples for each virus varies between one and 78 samples (for Concept.A), although the average is 2-3 infected objects each. Our results are split into two sections: "detection of viruses" and "detection of files", where "detection of viruses" has two sub-sections: "unreliable detection" and "unreliable identification".

(An index of the malware databases is available in a3tstbed.zip)

After each scanner is run, all report files are preprocessed by those AWK scripts already mentioned in the desciption of file virus test.

7.) Testing scanners on standard database of Script Viruses:

The test is equivalent to the macro virus test except that the testbed

is bases on script viruses the status of which is regularly published
by VTC in the "List of Known Script Malware" (LoKSM) (see VTC website).
Presently, the script virus testbed adresses the following platforms:

VBS, JS, IRC, mIRC et al.

8.) Creating the final summary of the results:

(Text essentially same as in previous test: 2000-08 / 2001-04).

The final evaluations for all tests are similar. Only one report of
file and macro viruses tests is used to get the total number of files
in the directory. As for boot viruses, the configuration file from
Simboot is used (if there was no specific need for manual operation).
Three new files result from these processes. New files contain the
directory name and the total number of files in this directory. Each
preprocessed report is joined with the new file. One AWK-scripts
evaluates the result of the joining.

The results are listed as follows:
- The number of viruses (+malware) detected: it is not necessary
  that all examples of the virus are detected.
- The number of viruses with unreliable (=inconsistent)
  identification: all variants of a viruses are detected
  but at least one sample is identified with a different name.
- The number of viruses with unreliable detection: here, not all
  samples of a virus are detected but at least one.

The files containing the preprocessed information mentioned above are
huge, although they are reduced to contain essentially the virus names.
For all tested scanners (latest version), they are included in a
separate archive (Scan-Res) for anonymous ftp.