RVK ROSE SWE Virus Killer - A generic virus remover for COM files
DECOM A generic COM file decryptor
RPCATCH ROSE SWE Poly Virus Catcher - HEURISTIC VIRUS SCANNER

Written and (C)opyright 1992-2005 by ROSE SWE,
Dipl-Ing. Ralph Roth - See ROSEBBS.TXT for full address

1 Index

2 RVK - Synopsis

This is a utility that will step through a polymorph (MtE, NED, DSME, DSCE, ViCE, TPE, SPE, G2, PS_MPC...) decryptor or just an ordinary (unencrypted) virus and decrypts and cleans the virus from the infected file. This process will restore the host program, disable the virus and cut parts out off the virus. RVK then terminates before executing the virus!

3 About RVK

This program is useful if you have an infected file and you want to remove the virus. Just clean it using RVK, then check the resulting file. RVK isolates viral code in an infected program and disables it. From then on it will be safe to use the program again, as the risk of other files being infected or damaged by it will have been securely disabled.

4 About The Cleaning Process

RVK works completely different compared to the 'conventional' cleaners. First of all, it does not recognise any particular virus. However RVK is aware of many tricks used by common viruses. Its disinfection scheme is therefore completely different from known cleaners and it works with almost any (COM) virus. This technique is called heuristic cleaning mode! In that cleaning mode RVK does not need any information about viruses either, but it has the added advantage that it does not even care about the original, uninfected state of a program. This cleaning mode is very effective if your program is infected with an unknown, a polymorphic or with a virus using 80386+ instructions!

Note that this does not imply that the cleaned file is 100% equal to the original one. When RVK uses heuristic cleaning to disinfect the program, the file will never be exactly the same as in its original state. This is not an indication of failure of RVK, nor does it mean the file is still infected in some way. First of all, it is normal that the heuristic cleaned file is still larger than the original one. This is normal because RVK tries to be on the safe side and it will avoid removing too much from the host program. The bytes left at the end of the file are 'dead' code, the instructions will never be executed again, since the 'jump' at the beginning of the program has been removed. The functionality of the cleaned file will nevertheless be the same! For this reason a virus scanner MAY find still the virus in cleaned files - or will now report a new variant of this virus (F-Prot)!

In the heuristic mode, RVK loads the infected file and starts emulating, simulating and tracing the program code to find out which part of the file belongs to the original program and which to the virus. The result is successful if the functionality of the original program is restored, and the functionality of the virus has been reduced to zero. When used, RVK will attempt to follow the execution of the program until the end of the decryptor or if the original entry point is restored by the virus! It will not execute dangerous interrupt calls, and will terminate if one is encountered. Some interrupt calls will be simulated, some emulated, a few will be executed (e.g. "get DOS version" or virus installation check) and some will be removed! It also terminates if DS and ES change, or if a far call is encountered. THIS DOES NOT ABSOLUTELY GUARANTEE SAFETY WHEN RUN! The viruses I have tested RVK on are over 600 COM infectors! One possible time when RVK may go to pass the cleaning process is when the virus does not actually restore the host program - instead trying to go resident or to infect other victims. Please send me any virus that can not be killed with RVK! If possible I will improve RVK to clean this virus too.

5 Multiple Infections and Antidebugging Tricks

It is possible that the infected file is infected with multiple viruses, or multiple instances of the same virus! Some viruses keep on infecting files, and in such case the infected files will keep growing (e. g. Jerusalem). It is very likely that RVK removes only one instance of the virus. In this case, it is necessary to repeat the cleaning process until RVK reports that it can not remove anything any more. Remember that you cannot clean COM files protected with PROTECT or HackStop due to the fact that this code uses antidebugger techniques. You can remove safely encryption added by SCRAMBLE, CRYPTCOM or R-Crypt instead! By the way, RVK can by-pass the most anti-debugger tricks found in existing viruses, packers and scramblers!

6 Decom - Synopsis

This is a simple utility that will step through an polymorph (MtE, TPE, SPE, G2, PS_MPC...) decryptor and decrypt the virus it is attached to, then terminate before executing the virus.

7 About Decom

It is useful if you have a (polymorph) encrypted virus and you want to find out what virus has infected it - just decrypt it using DECOM, then check the resulting file, looking after the decryptor. This is a proto-type version, and is NOT IN ANY WAY GUARANTEED! I had only released this program because to this date nothing else seems to be able to do this (apart from TBCLEAN, which removes the virus!). This will allow anyone who needs to be able to disinfect or to evaluate (polymorph) encrypted viruses. Afterwards you can modify the code to -instead of saving the result to disk- search it for the storage bytes, original SS:SP and CS:IP, or whatever is needed for the disinfection routine. A generic disinfector (RVK) based on DECOM is also available...

When used, DECOM will attempt to follow the execution of the program until the end of the decryptor. It will not execute dangerous INT calls, and will terminate them if one is encountered. It also terminates if DS and ES change, or if a far call or something else is encountered that will cause the lost of control over the programs execution. **THIS DOES NOT ABSOLUTELY GUARANTEE SAFETY WHEN RUN!** While I have not encountered an polymorph encrypted file that it did not safely decrypt, it is quite possible to program such. The ‚true‘ polymorph viruses I have tested DECOM on are:

- Alive:SPE
- Argyle
- Bosnia:TPE.1_2
- Byway (Dir-2.TheHndV)
- CoffeShop:MtE.0_90
- CoffeShop:TPE.1_0
- CoffeShop:TPE.1_3
- Connie:DSME
- Crazy_Chemist:SPE
- Dedicated.A:MtE.0_90
- Dedicated.B:MtE.0_90
- Dedicated.CryptLab:MtE.0_90
- Demo:DSCE
- Demo:DSME
- Demo:GCE
- Demo:PME
- Demo:SPE
- Demo:TPE.1_4
- EbbelWoi.QUX
- Encroacher.A:MtE.0_90
- Encroacher.B:MtE.0_90
- Fear:MtE.0_90
- Flip.2153.A
- Flip.2153.B
- Flip.2153.D
- Flip.2153.E
- Flip.2343
- Flip.2365
- GOL-Wanted
- Gotcha.Pogue:MtE.0_90
- Groove:MtE.0_90
- Insufficient.A:MtE.0_90

- Insufficient.B:MtE.0_90
- Insufficient.C:MtE.0_90
- King:SPE
- Lame:DAME.0_91
- Lame:HPE.0_90
- Lame:HPE.0_91
- Little:TPE.1_3
- Ludwig.A:MtE.0_90
- Ludwig.B:MtE.0_90
- Ludwig.C:MtE.0_90
- Natas.4730
- Natas.4738
- Natas.4744
- Natas.4746
- Natas.4748
- Natas.4988
- N8fall (the 4xxx versions, as well „Won't last", 57xx versions) - com files only...
- One_Half.3744 (fails sometimes)
- One_Half.3755 (fails sometimes)
- Ontario.1024
- PC_Weevil:MtE.0_90
- Phoenix.1226
- Phoenix.2000
- Phoenix.Evil
- Phoenix.Phoenix.A
- Phoenix.Phoenix.B
- Phoenix.Proud
- SMEG:Pathogen (too complex for DECOM!)
- SMEG:Trivial (too complex for DECOM!)
- Teacher:DSME
- Tester:NED.1_00
- Testfiles:TPE.1_0
- Testfiles:TPE.1_4
- Tremor (COM-Variant)
- Trigger:DAME.0_90
- Uruguay Family
- V2P6
- V2PX.1260
- WordSwap.1503

As well as a collection of my own MtE & TPE test files (15000!) and over 400 different encrypted viruses (Cascade, G2, PS-MPC, ANNI-VCS, IVP, VCL, etc.). One possibility when DECOM is not able to decrypt the code is:

- the decryptor does not actually encrypt the code
- the code is not encrypted in any way
- anti-emulator code is found
- the decryptor uses anti-debugging tricks, which DECOM is not yet aware of
- if there are „do nothing" loops like sometimes found in the TPE 1.3/1.4 viruses. In this case use RVK!

This generally results in DECOM printing that it can not safely decrypt it. If you got the hands on such a file please send me it in order to improve DECOM.

8 RPCatch

I am the author of a German virus scanner called VirScan Plus, which is able to detect more than 35000 viruses. The most time I spend to add detection of polymorph viruses to VirScan Plus. For this reason I have written RPCatch, a generic heuristic scanner for encrypted viruses. Later, when RPCatch is stable, the routines will be incorporated into VirScan Plus. RPCatch has a buildin 80386 dissassembler as well as an code emulator and a heuristic detection engine to catch all those polymorph encrypted viruses.

8.1 RPCatch - Usage

Invoking RPCatch with no parameters will result in a recursively scan of the current directory. You can invoke RPCatch additionally with a drive statement with will result in a recursive scan from the root directory of the specific drive.

8.2 Parameters

```
        /? -?           a short help
        drive:          drive to be scanned

    E.g.:       rpcatch c:
```

8.3 Detection ratio

RPCatch detects about 100% of all Tremor, TPE, MtE and DSME encrypted viruses. Furthermore RPCatch detects allmost all simple encrypted viruses such as VCL, PS_MPC, IVP, BW or G2. In generally spoken, RPCatch detects about 90% of all encrypted viruses I have in my collection (and that's a big amount :). To be honest, RPCatch will also detect all encryted programs with are protected by programs like CryptCom, Scramble or Protect.

9 A Little Warning

This package is a prototype version, and is NOT IN ANY WAY GUARANTIED! I am only releasing this program because to this date nothing else seems to be able to do this (apart from TBCLEAN which is disbanded meanwhile). This will allow anyone to be able to disinfect COM files. As an advantage RVK is not limited to 8086 code, it will even clean viruses which will use 80586+ instructions (remember: you CAN NOT CLEAN 386 code on a 286 machine)! Send me ANY virus that could not be cleaned by using RVK!

10 Legal Terms and Disclaimer

RVK+DECOM basically has no legal guarantee and warranty because I do not want to get sued over it, and should be used "as is". Here is the official disclaimer:

RVK+DECOM ("program") will **ALTER** and **DESTROY** executable files and may have or cause **compatibility problems** with them (that is why YOU should keep a backup file, in case of incompatibility with a particular file) in certain circumstances. Under no circumstances may Ralph Roth ("author") be held liable or accountable for any damage to system files, executable files, data files, or any other system or data damage due to use or misuse of his program. The author also may not be held accountable for loss of profits or for any other damages incurred by the use or misuse of his program. The author has forewarned any users that damage to files may occur with use or misuse of his program, and in executing the program, the user fully understands these risks and this disclaimer.

Greetings (and virus free time)
Ralph Roth

You can obtain the newest DECOM & RVK version from (please add some money for disc and shipping!) - see ROSE_BBS.TXT

11 RVK+DECOM - History

Version 0.01-0.05

Now RVK prompts you only for a filename _IF_ the virus has been safely decrypted or disabled! This means although, that you can now overwrite the old file at your own risk. RVK no emulates a lot of MS-DOS calls to handle many more viruses! "Anti Debugger Code Handling" improved!

Version 0.10

RVK can now be invoked via command line else you will be prompted for a source file! RVK now truncates (most of) the virus-body, therefore check the resulting file carefully!

Version 0.11

Added more code checking in order to clean the Annihilator Stealth viruses. RVK displays now information about the cleaned file. Some (dangerous) instructions are now additionally overwritten with NOP's, therefore check your cleaned files carefully!

Version 0.13

Added more anti-debugging tricks checking. Tested with over 50 new viruses.

Version 0.20 (March 95)

Added a software emulator that is able to emulate INT calls and most anti debugger tricks without loosing control over the program! RVK can now handle almost all files, except some special anti debugging code. Furthermore the handling of infected files is now safer, more reliable and more successful than ever before!

Version 0.21 (April 95)

My FAX number has changed! Little code enhancements to clean more viruses!

Version 0.22 (June 95)

The program is now able to by-pass some IN/OUT commands. The package now includes an alpha version of the heuristic scanner "RPCATCH".

Version 0.23 (December 95)

Fixed some orthographical errors in RVK.COM.

Version 0.24 (February 96)

The code emulator can now handle the POP SS/POPF antidebugger trick. Credits goes to L. Vrtik & J. Valky for pointing out this trick, as well as supplying me sample code.

Version 1.20 (March 96)

Added the handling of 386++ commands. For this reason you will need at least a 386 SX to run the program! Changed the version number to 1.20 (now the same as DECOM). The code emulator can now handle another antidebugger trick. Credits goes to L. Vrtik & J. Valky for pointing out this trick, as well as supplying me sample code. Excluded the RPCatch program from the package.

Version 1.21 (March 96)

The code emulator can now handle another antidebugger trick. Credits goes to L. Vrtik & J. Valky for pointing out this trick, as well as supplying me sample code. Added the "TBClean Bug" from VLAD #6 to the emulator, as well as another antidebugger trick found in the GOL-Wanted virus, which hinder RVK to clean infected files. Credits goes for this goes to Martin Roesler.

Version 1.22 (April 96)

The code emulator can now handle GS: and FS: segment override anti debugging tricks. Credits goes to L. Vrtik & J. Valky for pointing out this trick, as well as supplying me sample code. Added the handling of protected mode debugging tricks, using the CR and DR registers.

Version 1.23 (July 96)

The code emulator can now handle the PUSHFD/POPFD anti debugging trick and other 32 bit anti debugger tricks. Credits goes to Rand0m^X-Adi for pointing out this trick.

Version 1.24 (December 96)

Minor small bug fixes. Fixed some typos in the DOC. Added an interrupt 3 emulator. Added code to handle anti-emulator code found in the Grief.3584 and ANNI-VCS viruses. Now the program displays the last IP Counter, the AX value and the opcode of the latest instruction if the emulating process failed. This is useful to find out why and where the emulations process has been interfered.

Version 1.25 (10 August 1997) and version 1.26 (15 February 1998)

Minor code and documentation changes. Version 1.25 was released on the VIRUS.GER CD-ROM (published by VHM). The Cicatrix cumulative update January 1998 contains this version along with tons of viruses. To avoid speculations if this is version was hacked or infected this new version is released instead!

Version 1.29 (April 2002)

Merged the documents into one big PDF file. Some small fixes on the source code.

Version 1.30 (May 2003)

Enhanced the documentation. Some small fixes on the source code.

Please excuse my English; it is not my native language!

ALL IMPROVEMENTS ARE WELCOME!