Exhibit 19

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

November 1991 ISSN 0956-9979

VIRUS BULLETIN

THE AUTHORITATIVE INTERNATIONAL PUBLICATION
ON COMPUTER VIRUS PREVENTION,
RECOGNITION AND REMOVAL

Editor: **Edward Wilding**

Technical Editor: **Fridrik Skulason**

Editorial Advisors: **Jim Bates**, Bates Associates, UK, **Phil Crewe**, Fingerprint, UK, **David Ferbrache**, Defence Research Agency, UK, **Ray Glath**, RG Software Inc., USA, **Hans Gliss**, Datenschutz Berater, West Germany, **Ross M. Greenberg**, Software Concepts Design, USA, **Dr. Harold Joseph Highland**, Compulit Microcomputer Security Evaluation Laboratory, USA, **Dr. Jan Hruska**, Sophos, UK, **Dr. Keith Jackson**, Walsham Contracts, UK, **Owen Keane**, Barrister, UK, **John Laws**, Defence Research Agency, UK, **David T. Lindsay**, Digital Equipment Corporation, UK, **Yisrael Radai**, Hebrew University of Jerusalem, Israel, **Martin Samociuk**, Network Security Management, UK, **John Sherwood**, Sherwood Associates, UK, **Prof. Eugene Spafford**, Purdue University, USA, **Dr. Peter Tippett**, Certus International Corporation, USA, **Dr. Ken Wong**, PA Consulting Group, UK, **Ken van Wyk**, CERT, USA.

CONTENTS

VIRUS BULLETIN ©1991 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139.
/90/$0.00+2.50 This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Case 3:17-cv-05659-WHA Document 126-23 Filed 06/28/18 Page 3 of 4

KNOWN IBM PC VIRUSES (UPDATE)

Updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 20th October 1991. Hexadecimal patterns may be used to detect the presence of the virus with a disk utility program, or preferably a dedicated virus scanner.

Type Codes

C = COM files E = EXE files D = Infects DOS Boot Sector (logical sector 0 on disk)
M = Infects Master Boot Sector (Track 0, Head 0, Sector 1) N = Not memory-resident after infection
R = Memory-resident after infection P = Companion virus L = Link virus

864 - CN: This virus adds 864 bytes in front of the files it infects. Awaiting analysis.

```
864             B04D B449 B742 473A 2575 153A 7D01 7510 3A45 0275 0BC6 4502
```

1876 - CER: This 1876-byte virus is probably of Polish origin. Awaiting analysis.

```
1876            8EC0 33FF 33C0 B9FF 7FFC F2AE 26F6 05FF 75F8 83C7 038B D72E
```

Best Wishes-970 - CER: This virus is detected by the search pattern for the Attention virus, but not by the pattern for the Best Wishes-1024 virus. This variant is not able to infect .EXE files properly.

Black Wizard - EN: A variant of the 'Old Yankee' virus and detected by the pattern for that virus. This variant is 2051 bytes long and plays a different tune than the original virus, but is otherwise similar.

Bulgarian 123 - CN: A simple 123-byte virus from Bulgaria, which does nothing but replicate. It may infect the same file repeatedly.

```
Bulgarian 123   B103 8D54 F4B4 40CD 21B4 3ECD 21B4 4FCD 2173 AFBB 0001 FFE3
```

Copmpl - CER. This is a 1111 (COM) or 1114 (EXE) byte Polish variant of the Akuku virus. The name is derived from the following text, which can be found inside the virus 'Sorry, I'm copmpletly dead' (sic). The only effect of the virus is to play a tune.

```
Copmpl          80E6 0F8A D680 FA00 7407 80FA 0B76 06B2 02B4 0ECD 218C C88E
```

Copyright - CN: A 1193-byte virus from East Europe, which contains a fake Award BIOS copyright message. Awaiting analysis.

```
Copyright       AB4A 75F2 E2EA 33C0 CD16 B800 06B7 0733 C9B6 18B2 4FCD 10E9
```

DIR-II - LCER: A 1024-byte 'link' virus from Bulgaria. 'Infects' all COM and EXE files in each directory on a single pass. If the virus is resident, 'infected' COM and EXE files can be disinfected by renaming their extensions. (*VB*, Nov 1991).

```
DIR II          BC00 06FF 06EB 0431 C98E D9C5 06C1 0005 2100 1E50 B430 E824
```

DM-400 - CR: This 400-byte virus does not seem to do anything but replicate. It contains the text '(C)1990 DM'.

```
DM-400          80FC 4B74 3380 FC56 7419 FE04 80FC 3D74 12FE 0480 FC3E 751C
```

Europe '92 - CR: This 421-byte virus activates if the year is set to 1992, when it displays the message: 'Europe/92 4EVER!'

```
Europe '92      B450 CD21 8CD8 488E D8C6 0600 005A 891E 0100 8916 0300 53B8
```

Fake-VirX - CN: A 233-byte virus from Finland which activates on any Friday the 13th, when it displays the message 'VirX 3/90'.

```
Fake-VirX       408B D5B9 0600 CD21 B801 575A 59CD 21B4 3ECD 21B8 0001 FFE0
```

Gergana - CN: Four variants of the Gergana virus, which are longer than the original with improved error handling.

```
Gergana-222     BF80 FFB9 3000 F3A4 E9C6 FD5E 81C6 0001 BF00 01B9 DE00 F3A4
Gergana-300     BF80 FFB9 3000 F3A4 E985 FD5E 81C6 0001 BF00 01B9 2C01 F3A4
Gergana-450     BF80 FFB9 3000 F3A4 E97E FD5E 81C6 0001 BF00 01B9 C201 F3A4
Gergana-512     BA00 FAB4 3FCD 21C3 B900 02B4 40CD 21C3 B801 572E 8B0E 5001
```

Gosia - CR: A 466-byte virus from Poland. It contains the text 'I ♥ Gosia'. ♥ is the ASCII character (03))

```
Gosia           0275 10AC 268A 2547 3AC4 7405 80CC 203A C4E2 EE9F 03F9 8B1D
```

Gotcha - CER: Two related viruses from East Europe, 879 and 881 bytes long. They contain the text string: 'GOTCHA!'.

```
Gotcha          9C3D DADA 7428 80FC 3D74 0A3D 006C 7405 80FC 4B75 1306 1E50
```

Hero-394 - ER: Related to the 506-byte Hero virus, but does not damage the files it infects. Awaiting analysis.

```
Hero-394        B98A 0133 C0BF 0002 0305 83C7 02E2 F929 069C 03B8 0042 33C9
```

Hungarian-482 - CR: This 482-byte virus from Hungary activates on November 7th. If an infected program is run on that date it will display the string 'Format ...' and proceed to format the hard disk.

```
Hungarian-482   5603 F7AC 0AC0 740A D0E8 B40E B307 CD10 EBF1 B901 00BA 8000
```

VIRUS BULLETIN ©1991 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139.
/90/$0.00+2.50 This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Case 3:17-cv-05659-WHA Document 126-23 Filed 06/28/18 Page 4 of 4

Guidelines

From the user's point of view, it makes good sense to use a number of different anti-virus packages in order that they may each confirm the findings of the other. One of the major reasons for such an approach is to limit the problems posed by false positive indications. Unfortunately, the careless or self-centred approach of many vendors means that their packages may actually *cause* false positives in other packages.

To avoid the confusion and inconvenience caused by false positives there are certain guidelines:

- Use several scanners from dissimilar sources. The more search data that is available the better - this increases the likelihood of detecting genuine infections while providing a means to diagnose suspected false alarms. No single virus-scanner can provide 100 percent protection!
- Always run scanning and integrity checks on a freshly booted system. Boot from power off between subsequent checks.
- Remember that false positives can result from scanning with anti-virus software from dissimilar sources. Either remove such software from the disk under inspection or ignore any warnings limited solely to it.
- It would be highly unusual to find just a single occurrence of a parasitic (program infecting) virus on a working hard disk. Once a virus is invoked its main purpose is to spread, so you would expect to find several occurrences within a working environment. Floppy disks on the other hand, could quite easily contain just a single infection.
- Avoid the use of integrity checking programs which add *modifications* to actual file profiles. These are often advertised as providing a checking system which will travel with the file but they are worse than useless when used in conjunction with other integrity checking software that completes a reliable check.
- When a virus infection has been indicated, you should attempt to verify its existence via other methods (integrity checks versus scanning methods etc.). These include checking along possible infection paths and testing with other software.

You should also remember to check with the vendor of the package - if there are any false positive problems, they are likely to know about them and be able to put your mind at rest. In any case they should be informed so that they can make efforts to correct the problem (assuming it is a problem they *can* address).

Finally, if a package continues to produce an unacceptable number of false positive indications it should be discarded. The whole point of anti-virus software is to save time and worry - not generate it!

PRODUCT REVIEW

Mark Hamilton

Virus Buster

Virus Buster is an Australian package from *Leprechaun Software International*. The package consists of a 320-page perfect-bound paperback manual, two 360 Kbyte and one 720 Kbyte diskettes in video-cassette type packaging.

The software consists of three main programs, *BUSTER*, *WATCHDOG* and *DOCTOR* and a number of complementary files, three of which are simply included to install the package on a hard disk or floppies. The installation process scans memory and the destination disk before copying and installing the constituent parts of the package.

Installation

The package refused to install onto the hard disk of my Apricot 486, but it installed without any problem to the hard drive of my Compaq DeskPro 386/16. An inauspicious start to the review.

Alternatively, you can simply copy the 22 files into a sub-directory, and using the instructions in the documentation, configure the software to suit your preferences.

Buster

BUSTER is a checksumming program which detect changes in files. The first time it is run, it creates an encrypted data file, BUSTER37.DAT, which contains details of the file's path name, date, size, header and checksum. This information is used by *BUSTER* for subsequent checks. By default, *BUSTER*, checks all the normal executable file types, but you are able to add to or remove from the list of these to suit your personal preferences.

When *BUSTER* is re-run, any changes to the recorded details to any of the files (or disk's system area) are reported in a pop-up window. You can add details of any new program; change *BUSTER's* record for a file; rename the file; wipe the file; or, generically restore the file to its former self. *BUSTER* is intelligent enough to know whether it can restore a particular change successfully and disables this option if it can't.

On my Compaq Deskpro *BUSTER* completed its checks on 419 executable files (14 Mbytes) in just 2 minutes, which works out at 118 Kbytes per second. It took less than one second longer to create its database initially.

Like all generic checkers, it tripped-up over self-modifying programs - such as some of the shareware text editors which

VIRUS BULLETIN ©1991 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139.
/90/$0.00+2.50 This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.