ISSN 0956-9979 NOVEMBER 1995

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Winword again.** Following hot on the heels of our report on the first WordMacro virus comes an analysis of a second such virus, Nuclear: turn to p.8.

• **A bluestocking conference.** The *VB* team has just returned from Boston, where one of their most successful conferences ever took place. The full report begins on p.16.

• **Detecting a new way.** *RG Software* has released a new product which claims to detect any and all boot sector viruses. See how the product fared, from p.21.

CONTENTS

EDITORIAL

I could tell you, but then I'd have to kill you

Regular readers of this column will probably have noticed that I have a certain tendency to write about *Microsoft* with what may appear to be excessive frequency. Why should this be? Perhaps I bear some historic grudge against this company? Perhaps I was in line to rule the PC roost until that nice Mr Gates came along? Perhaps I am simply jealous of a man who, even back in 1990, was worth a cool three thousand million dollars? Well, no – none of these are true. Honest.

"The concept of an NDA is anathema to this spirit"

The reason is, as the Chinese curse puts it, we live in interesting times. Not only that, these times are, like it or not, being driven by *Microsoft*. There is a lot happening. *Windows 95* is now with us, bringing with it all its opportunities, and of late we have the intriguing new field of the macro virus opening up, currently centred around *Microsoft Word*. It is this latter which at present occupies my mind, and the minds of many others.

The phenomenon of the macro virus is proving a tricky problem for anti-virus researchers. In principle, detection of such creatures is not a problem even for the conventional scanner. The DOS/*Windows* scanner is running outside the system under which the virus operates (*Microsoft Word*), so any attempts by such viruses at stealth will not work. The viruses are trivial both in terms of their functionality and in terms of their appearance within the binary document files.

So, where does the problem lie? It lies with the information. Specifically, the information required to locate the macros within the document on disk. Without this, speedy and accurate searching for these new viruses is considerably harder; with it, it is possible for the scanner to go straight for the areas of the document in which the macros reside, and find them quickly and reliably.

Obtaining documentation on this subject is not easy. Give it a try if you have a month to spare – phone up your local *Microsoft* office and ask. It's great fun, if you like hold music. To be fair though, the goodies in this area have not been entirely withheld by the folks in Redmond. The format of modern document-types, such as *Word*, are non-trivial to say the least, and what the anti-virus industry wishes to do is not something that could have been anticipated six months ago.

Even after such information is obtained, there is a second problem. This, like so many, is concealed by an acronym – NDA. Non-Disclosure Agreement. Such an agreement is a mechanism by which a company can keep its secrets, whilst still telling people whom they consider have a need to know.

Suppose you are a large software house, and you want to commission my company to write a viewer for the files generated by your new wonder-product, *WidgetDesign*™. At the same time, of course, you don't want any other companies to know what you will have to tell me, otherwise one of them may come up with *WidgetHack*, a cheaper, smaller, more efficient Widget creation tool which is file-for-file compatible with *WidgetDesign*. In this situation, you get me to sign an NDA. This states that I may not discuss the information I am obtaining, or insights gained directly from that information, with anyone outside of our two companies.

This is an interesting concept to the normally voluble members of any programming community. Hackers, and I use the word in the traditional sense without implying negativity, are a talkative lot. They like to discuss what's being done and how to do things, and the anti-virus community is no exception. The concept of an NDA is anathema to this spirit, and to the oft-quoted 'information wants to be free' ethic. Whilst this latter phrase is both over- and mis-used, it would nonetheless be nice to believe that it still has some substance.

The anti-virus community is startling, above most others, for the level of technical cooperation which goes on within it – clearly there are limits, but these are set higher than one might expect. All NDAs can do is to stick oars into this flow of communication. However, as we move into still more interesting times, the problem of NDAs and general lack of information is bound to reappear. It will be with different systems, even different companies, but inevitably it will happen again.

NEWS

Shipping Viruses

This month has seen two more incidents coming to light of computer viruses being mass-shipped on floppy disks.

The first came from *Digital Equipment Corporation*, and was given to delegates at the *DECUS* conference held in Dublin during the second week of September 1995. The disk, which contained white papers concerning *Digital's* product strategy, was discovered also to be carrying the *Microsoft Word* virus Concept [f*or an analysis, see VB, September 1995, p.8*].

Digital has since distributed to their customers both clean copies of the documents and the *Microsoft Scan* tool to remove the Concept virus. They are also offering a Software Hotline on +353 91 754029 (08:00–16:00 UK time).

In a separate incident, *PC Magazine* in the UK distributed the Sampo virus on diskettes which were sent out to advertise their 'Editor's Day' at the end of October. This incident is made all the more ironic by the fact that, in the same month, the magazine published a review of anti-virus NLMs. *PC Magazine* has since shipped an alert, along with an anti-virus utility to detect and remove the virus, to recipients of the infected diskette ▮

Big Fish, Little Fish

McAfee Associates has announced the acquisition of two companies in the UK. The integration of *Saber Software* with *McAfee* has heralded plans for the launch of a dozen new products within the next year, and will culminate in a family of enterprise-enabled systems management tools for PC LANs.

Bill Larson, President, CEO, and Chairman of *McAfee*, said: 'The combination of our companies and product lines will create a best-of-breed family of highly integrated point products and suites.'

Following the acquisition of *Saber*, *McAfee* has also announced the purchase of *IPE*, which was until now *McAfee's* exclusive agent in the UK.

Peter Watkins, VP of International Operations at *McAfee*, had this to say of the deal: 'According to a recent report from *IDC*, *McAfee* has a 76% worldwide market share for desktop anti-virus software for our *VirusScan* and *NetShield* products. Now with a secure European base, we will be looking to expand our activities in Europe and establish *McAfee* as the vendor of choice for any user investing in quality network security products.'

IPE's subsidiary, *International Data Security* (*IDS*), will remain independent, and continue to market and sell the entire *McAfee* product range ▮

Prevalence Table - September 1995

Virus	Incidents	(%) Reports
AntiEXE	35	12.4%
Form	31	11.0%
Parity_Boot	26	9.2%
Ripper	19	6.7%
NYB	15	5.3%
Empire.Monkey.B	14	5.0%
Sampo	14	5.0%
AntiCMOS	12	4.3%
Concept	12	4.3%
Junkie	12	4.3%
EXEBug	10	3.5%
Telefonica	7	2.5%
Stoned.Angelina	6	2.2%
Cascade.1701	5	1.8%
Jumper.B	5	1.8%
Natas	5	1.8%
Manzon.1414	4	1.4%
She_Has	4	1.4%
Stoned.NoInt	4	1.4%
Barrotes	3	1.1%
Helloween	3	1.1%
Stoned.Manitoba	3	1.1%
Stoned.Michelangelo	3	1.1%
Stoned.Standard	3	1.1%
Byway	2	0.7%
V-Sign	2	0.7%
Other *	23	8.2%
Total	282	100%

* The Prevalence Table includes one report of each of the following viruses: Boot.437, BootEXE.451, Bye, Empire.Monkey.A, HideNowt.1741, Istanbul, Italian, Jackal, Jimi, Joshi, Leandro, Lixi, Print_Screen_Boot.A, Quicky.1376, Quox, SMEG:Pathogen, Stoned.Kiev, Stoned.NOP, Stop.1045, Tai-pan, Tequila, Urkel, UVscan.

Stop Press

Just as *Virus Bulletin* goes to press, there is more news breaking concerning *Microsoft Word* viruses. The latest such creation was posted to the Usenet newsgroup alt.comp.virus during October 1995, and has been named Colors by researchers. It is non-destructive, the only trigger being to randomise the *Windows* colours. The remaining techniques used by the virus appear to be fairly standard, and it is encrypted (as is Nuclear) using the internal *Word* macro encryption technique ▮

IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 21 October 1995. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

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

Army_Boots

CR: An appending, 411-byte virus, which modifies the contents of AUTOEXEC.BAT. It contains the plaintext strings: 'C:\AUTOEXEC.BAT' and '@ECHO din mamma har paa sig arme stoevlar!'.

```
Army_Boots      B80D F0CD 2181 F90D F074 558C D848 8ED8 33FF 8EC7 803D 5A75
```

CK.777

CN: A prepending, 777-byte, direct infector, infecting three files at a time. It contains the encrypted text: 'The China Syndrome Version 1.00a Written by Crypt Keeper Well, I guess you found the sectors...You got a warning...This program was written in the city of Cincinnati. Non-destructive version -A- l8rd00d'.

```
CK.777          E8AA FFBB 0010 0E07 B44A CD21 0E07 BB00 10E8 D9FF A31C 00BB
```

Crazy_Frog

CER: An appending, encrypted, 1417-byte virus with the text: 'cRaZy fROG, (c)95 by iRASCiBLE'.

```
Crazy_Frog      8B96 6E05 2E8B 8670 052E 3114 2E31 4402 83C6 04E2 F4C3 E440
```

DigPar

CR: A polymorphic virus, about 1000 bytes long, which contains the text: 'The Digitised Parasite: Australian Parasite [AIH]' and 'Weiners XOR machine 1.0 (c) Australian Parasite [AIH] June 1994'. The pattern below detects the virus in memory only.

```
DigPar          B43F B903 00BA B503 CD21 89D6 81C2 9856 3914 746E B802 4233
```

Ebola

ER: A polymorphic, 3000-byte virus which often causes system crashes. It contains the text: 'Ebola virus 1.2! Extremly stealthmutating system! Technical infos: No way to detectFucked heuristicsGreets go to allvirus detelopinggroups in Brno ! Czech republic94'. It is not likely that we will see this virus spread widely. The template below detects it in memory.

```
Ebola           9C3D 004B 746A 80FC 4074 8D3D E4F7 7447 3D2F C974 4A80 FC4E
```

ExeHeader.265

ER: A stealth, 265-byte virus which inserts its code into EXE headers. The virus hooks Int 13h and infects files when they are read. It contains the text: '[Dying_Oath] by Retro'.

```
ExeHeader.265   8B07 354D 5A74 1126 803F EB75 4426 817F 5CB4 0D74 2EE9 3900
```

H8

CR: A prepending, 1773-byte virus with stealth capabilities. It contains the plaintext strings: '[H8YourNMES]' and 'xtf-ndivskavcommand'.

```
H8              B4FF CD21 C706 0601 EB01 0BC0 7507 EB01 80B4 FECD 21E8 4003
```

Horsa

CN: An appending, 1185-byte direct infector which uses direct disk access (Int 25h/Int 26h).

```
Horsa           AA1E E800 0058 2D12 0033 D2B9 1000 F7F1 0BD2 7403 E98B 038C
```

Kela

CER: An appending, stealth, 2018-byte virus. All infected files have their time stamps set to 62 seconds.

```
Kela            B8FF FFCD 210E 1F8E C0BF 0001 8BF5 B9E8 03F3 A61F 0775 03E9
```

Lady Death

CER: A polymorphic, appending virus, approximately 2744 bytes long, containing the text: 'Lady Death: Dark Fiber [NuKE]' and 'Stainless Steel Armadillo'. The virus corrupts EXE and some COM files. The template below detects it in memory.

```
Lady Death      39F0 5E75 263D DF2E 7504 B864 9FCF 569C 50BE 4A0A FC2E AC2A
```

Leda

CR: An appending, 820-byte virus with the following encrypted text (displayed from 6–11 November): 'Masz wirusa LEDA (BDv3.0), (c) BD 27.V.1994', 'PS Dzieki dla autora wirusa FLOOR 1153'.

```
Leda            B8BD 57CD 2181 FB14 BD74 22B8 2135 CD21 895C 678C 4469 832E
```

Manzon

CER: A polymorphic, appending virus, circa 1400 bytes long, which contains the text: 'MANZON (c)'. The template given detects it in memory.

```
Manzon          3DBA DC75 0590 908B D0CF FAFC 80FC 3E74 183D 004B 7403 E95E
```

Merci

CO: An overwriting, 308-byte virus with the encrypted text: '.COM *.C* CHKLIST.MS ANTI-VIR.DAT'. When the virus infects a file it displays this message: 'Merci virus infected: <filename>'.

```
Merci           E803 00EB 3990 BE3E 018B FEB9 F600 AC32 0639 01AA E2F8 C3E8
```

Mirage.1331

CER: A 1331-byte virus with stealth capabilities. It appends itself to EXE files, but prepends itself to COM files. The virus contains the plaintext strings: 'Mirage' and '\COMMAND.COM'. The time stamp of all infected files is set to 62 seconds.

```
Mirage.1331     80FC  FA75  4B5F  5F3C  0374  15BF  0001  5751  BE33  06B9  CCF9  F3A4
```

Monica.885

CR: An appending, encrypted, 885-byte virus which contains a dangerous payload. The virus sets and activates the CMOS password with the option to verify it at both CMOS setup and PC bootup. The new password is set to 'MONICA'.

```
Monica.885      B929  0381  EE38  03E8  0100  155F  2E8A  052E  3004  46E2  FA58  5F59
```

Multiplex.815

CN: An appending, 815-byte, direct infector containing the plaintext strings: 'MULTiPLEX (c) 1994 Metal Militia\ Immortal Riot, Sweden', 'Somewhere, somehow, always :)*.com', 'IRUSES', 'ImRio'.

```
Multiplex.815   E800  0058  2D0A  01E8  9502  E814  03E8  2402  B447  B200  568D  9CED
```

NRLG.755

CR: An appending, stealth, encrypted, 755-byte virus; the shortest member of the NRLG family. It contains the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. - 800 LIMO 1-800-972-7117'.

```
NRLG.755        F303  8DBE  3301  BA01  00F6  15FF  05F6  1547  47EB  0590  B44C  CD21
```

NRLG.824

CR: An appending, encrypted, 824-byte virus with stealth capabilities. It contains the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. -AZRAEL800 JEWELRY 1-800-346-7231'.

```
NRLG.824        BA01  0080  35E5  FF05  8135  E41B  FF05  F715  802D  4F80  35AC  812D
```

NRLG.853

CR: An appending, stealth, encrypted, 853-byte virus containing the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. - 800 SEAFOOD 1-800-472-0542'.

```
NRLG.853        5504  8DBE  3301  BA01  00F6  15FF  05F6  1547  47EB  0590  B44C  CD21
```

NRLG.865

CR: An appending, stealth, encrypted, 865-byte virus with the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. - 800 ROOMS 1-800-442-6633'.

```
NRLG.865        6104  8DBE  6001  BA01  0081  354C  C581  2D95  CB80  2DA6  812D  98DB
```

NRLG.872

CR: An appending, encrypted, 872-byte virus which occasionally crashes the system. It contains the text: 'Nemesis 1995 Gooberish'.

```
NRLG.872        6804  8DBE  4701  BA01  00F7  15F7  1581  3575  BE80  35D8  802D  E880
```

NRLG.901

CR: An appending encrypted, 901-byte virus with stealth capabilities, which contains the text: '[NuKE] N.R.L.G AZRAEL' and 'Created by MuTaTiOn INTERRUPT! This Could Have Formatted Your Hard Disk! See +++rus Goobers! 1994'.

```
NRLG.901        8504  8DBE  5F01  BA01  0081  2D6D  1281  35FB  4CF7  1580  3501  8135
```

NRLG.985

CR: An appending, stealth, encrypted, 985-byte virus, which contains the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. - 800 DRUGS 1-800-872-1626'.

```
NRLG.985        D904  8DBE  3301  BA01  00F6  15FF  05F6  1547  47EB  0590  B44C  CD21
```

NRLG.1007

CR: An appending, stealth, encrypted, 1007-byte virus. It contains the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. - 800 NANNY 1-800-443-4411'.

```
NRLG.1007       EF04  8DBE  3301  BA01  00F6  15FF  05F6  1547  47EB  0590  B44C  CD21
```

NRLG.1009

CR: An appending, stealth, encrypted, 1009-byte virus. It contains the text: '[MuTaTiOn INTERRUPT] 1994 - Thanks to N.R.L.G. - 800 FLOWER 1-800-878-1073'.

```
NRLG.1009       F104  8DBE  3301  BA01  00F6  15FF  05F6  1547  47EB  0590  B44C  CD21
```

NRLG.1038

CR: An appending, encrypted, 1038-byte virus with stealth capabilities. It contains the text: '[NuKE] N.R.L.G. AZRAELi!'.

```
NRLG.1038       0E05  8DBE  5901  BA01  0080  3578  802D  95F7  15FE  0581  053E  3DF7
```

Oxan

CR: A simple, appending, 710-byte virus. On every twelfth day of February (12 February) it displays the text: 'Happy birthday Oxan !'. On any other afternoon, during the first 20 minutes of each hour, it displays the current version of DOS using the message: 'MS-DOS Version <current DOS version>'.

```
Oxan            FB9C  3D00  4B75  03E8  0B00  9DFA  2EFF  2E11  00EB  4011  0050  5351
```

OpalSoft

CN: An appending, 683-byte, direct fast infector. It contains the plaintext string: '*.COM OpalSoft 10.3.1994 v1.1 C:\'.

```
OpalSoft        C706  3C02  3412  CD19  B980  00BB  0000  8B87  8000  2E89  8129  FE43
```

V.720

ER: An appending, 720-byte virus which marks all infected files with a time stamp of 62 seconds.

```
V.720           B8FF  FFCD  213D  0001  740B  545A  3BD4  7505  33F6  E825  0058  0510
```

XERAM

CEN: An appending, encrypted, 1663-byte, direct, fast infector containing the text: 'N-XERAM'. It deletes the files \CHKLIST.MS, \SCANVAL.VAL, and \NCDTREE\NAV_._NO. The payload, which triggers on any Friday the 13th, includes overwriting 255 sectors on a hard disk if the country code is France, US, Japan, Taiwan or Germany.

```
XERAM           B904  0333  F6A1  3E01  3104  4646  81FE  2E01  7504  81C6  7800  4975
```

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.