Macro viruses: problems and defences

Dr. Jan Hruska

Part # tr00031m/980313

Abstract

The macro virus problem is escalating rapidly and one virus alone (Winword/Concept) now accounts for about 15% of all infections. New macro viruses are continuing to appear. This paper describes some problems in the detection and eradication of macro viruses, as well as outlining virus defence options.

Introduction

Over 9500 viruses currently exist which are capable of replicating under DOS. Most of these are parasitic viruses (aka file or program viruses) accounting for 89.5% of the total, about 5% are pure boot sector viruses, 5% are multipartite viruses (infecting both boot sectors and programs) and only 0.5% of viruses are macro viruses. Parasitic viruses are responsible for only 5% of all infections, multipartite viruses for 10%, macro viruses for 18% and boot sector viruses for a massive 67%. The most commonly encountered virus is Winword/Concept, responsible for 15% of all infections reported to Sophos* between January and June 1996. The second most common virus is Form, responsible for 11% of infections over the same period.

There are no excuses...

... for getting infected by a pure boot sector virus. Since the early 1990s most manufacturers have been shipping PCs which allow the user to switch the default boot sequence from *floppy drive followed by hard drive* to *hard drive followed by floppy drive.* This makes the PC immune to boot sector viruses. Two thirds of all virus infections today could be prevented by this simple operation which takes less than a minute to complete, but the high percentage of boot sector virus infections today is evidence that this technique continues to be ignored.

* Virus statistics are based on viruses reported to Sophos. An incident is logged as one unit regardless of whether the virus was intercepted before causing an infection or whether it infected one PC or 1000 PCs. Other anti-virus vendors report similar percentages.

A program which would set the safe boot sequence automatically (for example from a login script) is technically possible, but the way of storing the sequence information in the CMOS is not standard and depends on the BIOS manufacturer. This makes an automated approach difficult. New operating systems (Windows 95, Windows NT and OS/2) complicate things further by prohibiting direct port access. The easiest solution is still to visit each PC physically.

If the manufacturers have provided the ability to set the boot sequence, why is the default sequence not the reverse of the current one? A good logical explanation does not seem to exist.

Virus problem

Since boot sector viruses are easily preventable, anybody who does not disable booting from floppy disk deserves no sympathy and his eventual cries for help will be ignored. Macro, multipartite and parasitic viruses remain a problem even on properly configured PCs. However, multi-partite viruses cannot spread by booting from an infected floppy disk on PCs protected in this way against boot sector viruses, while their ability to spread via COM and EXE files is severely limited by the way Windows 3.1 works([1]). Parasitic viruses are similarly decimated by Windows 3.1, so, providing that boot viruses gradually disappear as users become wiser and new operating systems become widely used, macro viruses are likely to become the prevalent virus type.

Furthermore, macro viruses work on any platform which runs the host application, which means that there are simply more machines available for infection. A Microsoft Word macro virus will probably function correctly in Windows 3.X, Windows 95, Windows NT and the Macintosh. (One interesting hurdle in the path of macro viruses is the many different language versions of Word, making it difficult, but not impossible, to write an international Word macro virus.)

Microsoft Office 97 brings with it several advantages to the budding virus writer. Instead of Word Basic

© 1997 Sophos Plc, The Pentagon, Abingdon, OX14 3YP, England. Tel (+44) 1235 559933, Fax (+44) 1235 559935, Email technical@sophos.com, http://www.sophos.com/. 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.

(which is not compatible with other Office applications), Office 97 will offer Visual Basic for Applications version 5 (VBA5). All Office 97 applications will be able to execute the same code, which seems like a juicy fruit which Microsoft is offering to the virus writers. Backward compatibility will also be provided, with existing macros being automatically translated from Word Basic to VBA5. This, unfortunately, means that a largish number of viruses in VBA5 will appear at the time of the Office 97 launch, since the current Word viruses translated to VBA5 stand a good chance of working.

Since the first macro virus appeared in the wild in July 1995, the speed of its spread and the scale of infections have probably surprised even the gloomiest doom merchant. Organisations with tens of thousands of infected documents are not uncommon and the problem is further fuelled by active large-scale virus dissemination centres: organisations which refuse to implement anti-virus measures and clean infected files 'since it is only Concept'. Needless to say, this approach is profoundly wrong and may be illegal in some countries.

Two virus defence options

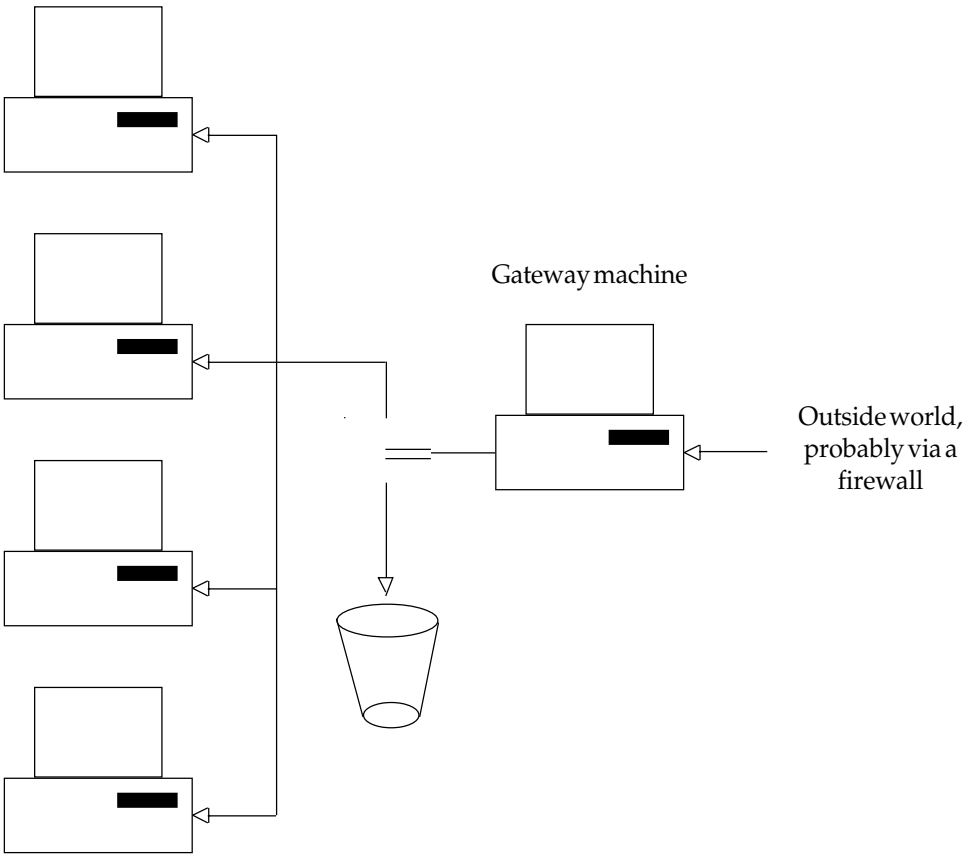
If the major virus problem in the future is going to be macro viruses and humanity refuses to stop exchanging documents, or switch from Microsoft Word to another text processor, what are the effective solutions to the problem?

Standard anti-virus software which can be used to check disks or files has only a limited use in an environment where there are so many easy and quick ways of introducing potentially infected objects into a company.

Two main techniques of virus protection in such environments are used: virus-checking gateways and on-access virus scanning.

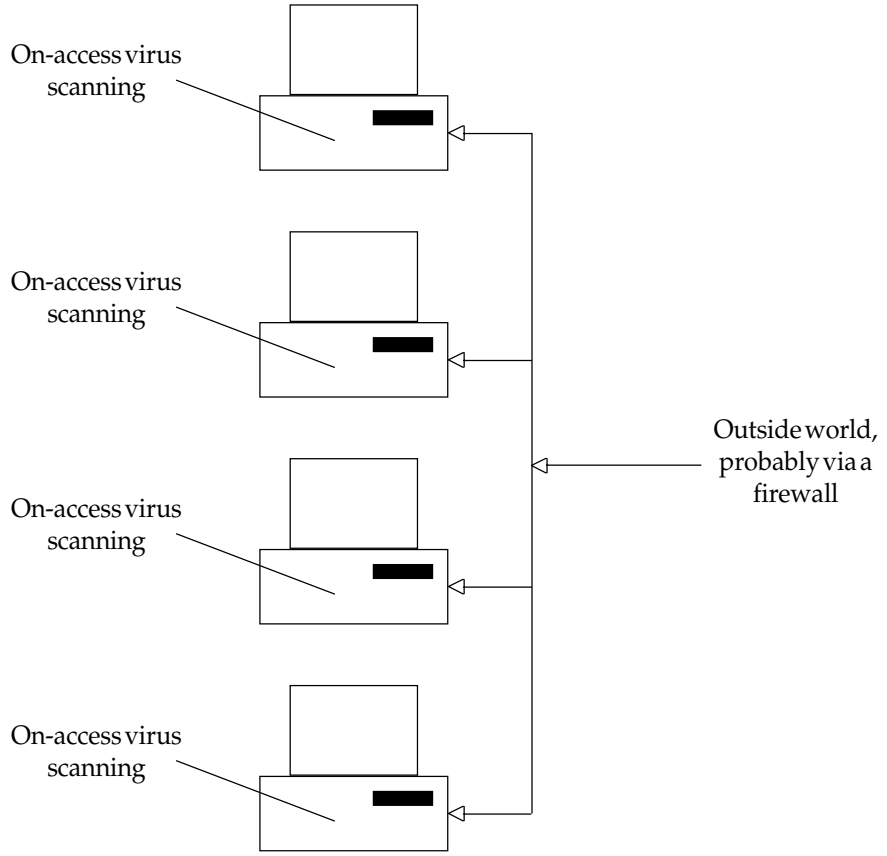
Virus checking gateway

This seemingly attractive technique is based on intercepting mail coming into the organisation, detaching the attachments, unpacking any encoded parts, sending them to the virus detector and either discarding them or passing them through to the recipient. Unfortunately, there are several problems with this approach.



Virus-checking gateway

© 1997 Sophos Plc, The Pentagon, Abingdon, OX14 3YP, England. Tel (+44) 1235 559933, Fax (+44) 1235 559935, Email technical@sophos.com, http://www.sophos.com/. 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.



On-access virus-scanning

There are numerous 'standards' for Internet mail attachments which convert binary information into 7-bit ASCII text in order to ensure their unaltered passage across the network via SMTP. This typically makes files bigger, so they are often compressed before conversion using numerous available compression methods. The gateway can only verify attachments that are compressed and encoded using the algorithms it knows about. Furthermore, binary files can be manually encoded into printable text (eg. UUENCODE) or encrypted (eg. PGP) and included into the message. The gateway needs to recognise these parts, decode or decrypt them and check them. The problem is simply too complex (or practically impossible for encrypted files) and no available gateway can (or claims to) solve it completely. Although there is no such thing as 100% security, the use of a technique which may be able to check only a small proportion of objects is difficult to justify.

The use of a gateway must be supplemented by other anti-virus techniques since, even apart from the above limitations, it cannot detect viruses in potential carriers such as floppy disks, CDs etc which are widely used. After all, it was a CD which spawned the Winword/Concept distribution.

On-access virus scanning

On-access scanning provides virus detection at the workstation. Although it may seem wrong to let a potentially infected object come so close to the end-recipient, this technique is much safer than any alternative. On-access scanning involves intercepting *file open* and *file close* operations*, virus checking the file and allowing the file access or execution to proceed only if no viruses are found. The questions of how a file is packed, whether it is compressed, encrypted or where it comes from, become irrelevant: the virus will be caught on unpacking, decompression or decryption. If the file is, for example, compressed with ZIP, unZIPping it will cause every executable item to be checked as it is created and, if a virus is found, the on-access scanner will prevent access to the offending item.

Since Windows 3.X, Windows 95 and Windows NT are not hampered by the DOS's 640K memory limit, on-access virus scanning has become a feasible and practically usable option. The scanner is a VxD (Virtual Device Driver for Windows 3.X and Windows 95) or an FSD (File System Driver for Windows NT).

* In practice, a few more things are checked.

© 1997 Sophos Plc, The Pentagon, Abingdon, OX14 3YP, England. Tel (+44) 1235 559933, Fax (+44) 1235 559935, Email technical@sophos.com, http://www.sophos.com/. 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.

On-access virus scanning is a powerful technique which still depends on scanning to detect viruses. Scanners have to be updated as new viruses appear and no on-access virus scanner will catch a virus that it does not recognise as such. The burden of scanner updating is still present and unlikely to disappear in the future, although good anti-virus software usually provides an automated way of distributing the updates in networked environments.

Conclusions

Boot sector viruses currently cause the highest percentage of infections, but they are easily preventable. Easy connectivity and wide use of networks facilitates the spread of parasitic, multipartite and macro viruses, however macro viruses are likely to become the major virus problem of the future. The best solution to the virus problem today is a regularly updated on-access virus scanner.

Reference

1. Steve White et al, The Changing Ecology of Computer Viruses, *Proceedings of the Virus Bulletin Conference*, Brighton, England, September 1996

© 1997 Sophos Plc, The Pentagon, Abingdon, OX14 3YP, England. Tel (+44) 1235 559933, Fax (+44) 1235 559935, Email technical@sophos.com, http://www.sophos.com/. 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.