Macs and Macros - the State of the Macintosh Nation

David Harley

Imperial Cancer Research Fund, PO Box 123, Lincoln's Inn Fields,
London WC2A 3PX, UK.
Tel +44 171 269 3114 * Fax +44 171 269 3124 * Email D.Harley@icrf.icnet.uk

ABSTRACT

The Apple Macintosh has received little recent attention from virus writers or, indeed, anti-virus researchers. Though the number of native Mac viruses has stayed virtually static for several years, the recent upsurge of macro viruses has not left the Macintosh community unscathed. Many viruses which infect Microsoft Office applications will do so as happily on a Macintosh as on a PC. Even Mac users who don't use vulnerable applications or application versions may, without appropriate anti-virus software, unknowingly pass on infected files. Many Mac sites, however, are only just waking up to these facts, belatedly and expensively. This paper briefly reviews the shared history of viruses and the Mac, summarizes the current situation and considers future possibilities and strategies.

1 INTRODUCTION

The Macintosh platform doesn't seem to interest virus-writers or anti-virus vendors much. While the number of PC viruses continues to rise dramatically, the number of Macintosh-specific viruses has been stalled (for years, literally) at around 35, some only a significant threat on older systems running versions of Mac OS earlier than System 7.

On the anti-virus side, several companies have abandoned the Mac and only one major player has actually launched a known-virus scanner for the Mac in the last two years. Traditionally, most Mac users have been content to rely on the freeware package Disinfectant, and/or the postcardware package Gatekeeper.

Apart from system viruses and a few non-replicating Trojan Horses (which, almost by definition, usually have a fairly short shelf-life), the nearest thing to a growth industry in the land of Mac viruses was a slow trickle of Hypercard infectors - arguably the first wave of in-the-wild macro viruses, but specific to a niche product which has had more impact as a catalyst in hypermedia and multimedia than as a killer application in its own right.

Summer 1995, though, shook things up somewhat with the first in-the-wild Word macro virus. From the start, there was a certain fascination with the fact that Concept and its younger siblings had the potential for infecting across hardware platforms. Unfortunately, the existence of this potential bypassed the Mac community altogether, for a while, and even now there is an assumption prevalent among Mac advocates that non-users of Word 6 need not concern themselves with what is seen as a PC problem.

It would be surprising today to see a new PC known-virus scanner which didn't address the macro virus problem, and a range of solutions have appeared which primarily or exclusively target macro viruses and Trojan horses (nearly all of them PC-specific). On the Macintosh platform, too, all the 'big four' commercial anti-virus products for the Mac now include macro virus definitions in their updates. There are, after all, many more macro viruses and variants, intended viruses, virus generators and Trojan horses reported in the wild now than the combined total of all Macintosh-specific malware.

Nonetheless, postings still turn up in Mac-related newsgroups asking if anyone has heard of something called Concept, or advising that there is no need to spend money on Mac anti-virus software since Disinfectant and Gatekeeper are (more or less) free. In 1997, research-oriented hospitals and other academic sites in the United Kingdom have been subject to severe panic attacks: these sites, which tend to be more Mac-friendly than most commercial sites, have been particularly prone to this fallacy. However, as more people have replaced legacy 68K Macs with the higher-specification PowerMacs realistically required to run Word 6.x in real time, they've come to notice that they can only save documents as templates, or have been brusquely informed by their PC-using peers that they're distributing infected documents.

2 CLASSIC MACINTOSH MALWARE

Viral and other malicious software which exclusively targets the Macintosh is, in general, well-documented elsewhere, and does not currently constitute a major threat to Macintosh users. Malware in this category is not discussed at length here with the exception of HyperCard viruses, which are discussed comparatively rarely elsewhere.

2.1 System and File Infectors

Native Macintosh viruses (apart from HyperCard viruses, which are essentially macro viruses) are sometimes classified as either system or file viruses: in fact, system viruses are generally a special case of file virus, since they normally infect the System file, system extensions, or the Desktop file. File viruses normally infect applications, but may infect control panels, system extensions, and even data files*.

System & application infectors comprise the most numerous class of native Macintosh viruses, but no new examples have, to my knowledge, been reported since 1995. Most of the known variants and synonyms are listed in Appendix A.

*Of course, macro viruses may also be considered a special case of file virus. An appealing suggestion [Lesch] is to draw a distinction between 'document viruses'—HyperCard infectors and other macro viruses—and other file viruses, including application infectors and system file infectors.

2.2 HyperCard Infectors

HyperCard is a tool for building applications. While it's sometimes been described as a solution without a problem, many people have found it useful as a prototyping tool, or as an easy-to-use database system with graphical capabilities, for example.

HyperCard was distributed as system software prior to the release of System 7: subsequent releases have included HyperCard player software, but excluded development facilities. The ‘official’ scripting language for System 7 and later (including Rhapsody) is AppleScript [InfoWorld]. Nevertheless, there is a previously announced plan to make Hypercard integral to the QuickTime Media Layer [MacWeek].

HyperCard stacks (hypermedia documents) contain links between on-screen buttons and pieces of information (graphics, text, sound) and can be created without direct programming. Nonetheless, stacks are based on the HyperTalk programming language, a high-level macro scripting language incorporating a set of sophisticated graphical objects and an object-orientated, event-driven view of the world. The principal competitor to HyperCard in this market is SuperCard, which is based on SuperTalk, a superset of the original HyperTalk.

Though not numerous, HyperCard viruses have been the nearest thing to a growth area in native Macintosh viruses, in recent years. HyperTalk authoring (scripting), like macro-programming in WordBasic or Visual Basic for Applications, is pretty high-level:

powerful operations can be implemented with a few simple statements. Knowledge of processor architecture, detailed understanding of other hardware, the Macintosh Programmers’ Workshop, or “Inside Macintosh” is not required.

While high-level languages are often despised by hard-core virus programmers, they are a gift to the “wannabe” virus writer without assembler or even C or Pascal skills. (The mention of Pascal, often thought of only in terms of teaching programming, is not as odd as it might appear: the Macintosh operating system was originally coded in Pascal.) HyperCard viruses also resemble macro viruses in that their dissemination is aided by the characteristic presence of data and executable code in the same file.

All the major commercial anti-virus packages scan for HyperCard viruses. A number of HyperCard-specific solutions have been offered. Vaccine, by Bill Swagerty, is a well-known solution available as a HyperCard stack - it deals with MerryXmas and variants, HC 9507, and Antibody, but not Dukakis or 3 Tunes.

It has been reported [Gay] that it is possible for a general virus scanner to generate a false positive report after a stack has been disinfected, where an identifiable snippet of viral code remains in ‘free space’ within a disinfected stack. In fact, this might be be better described as a ‘ghost positive’, by analogy with misreporting of viruses on PC disks where virus traces have been left in ‘slack space’. [Virus-L] Vaccine is not susceptible to this sort of misidentification: since it is a HyperCard stack, it “sees” only functional code, whereas commercial anti-virus software scans the entire data fork.

Infection mechanisms and some HyperTalk protection mechanisms which are sometimes put forward are discussed briefly in Appendix B, which also contains a list of known HyperCard infectors.

There are no viruses currently associated with AppleScript. It is probably possible to write at least a Trojan horse, dropper, or simple overwriting virus in virtually any language (how successfully such a virus will replicate is a different issue). However, AppleScript in its own right has a fairly limited set of high-level “terms” which limit its potential as a stand-alone systems language, and is probably not very

attractive to virus writers, in general. It should be noted, though, that it is capable of serious macro-processing when used with a "scriptable" (AppleScript-aware) application, through the "Do Script" event. One such scriptable application is, a little discomfitingly, Word 6.x. [Microsoft1]

2.3 Trojan Horses

In principle, it's simpler to write a basic Trojan horse than to write a virus, since it avoids the complications of replicative code. A simple-minded Trojan may, for all of its inelegance, be devastating in its impact, but they're usually easily traced to their point of entry, since in general they lack the means of covert dissemination by self-replication (unless you accept the argument that a virus is a special case of a Trojan, which is rather beyond the scope of this paper).

It's not quite as easy in MacLand to create a Trojan as it is in PC-Dystopia, where a simple batchfile making a surreptitious call to DELTREE could be very destructive, but it doesn't require great programming skill (and a Macintosh-specific Trojan is trivial to write and conceal - see section 3.6). Comparatively few Mac-specific Trojans are actually known, let alone still seen. The documented examples of Macintosh Trojans are listed in Appendix C, and are usually detected by commercial anti-virus software.

3 CROSS-PLATFORM ISSUES

The most obvious issue here is the macro malware problem. In fact, there is a surprisingly wide range of other issues, though.

3.1 Hoaxes

Hoax virus alerts are rarely aimed specifically at Macintosh users: in fact, hoaxes which include circumstantial quasi-technical detail tend to use PC-centric jargon. Most, however, are actually intentionally vague as to mechanisms and targeted platforms, and a technically-disadvantaged Mac user is as likely as an equivalent PC user to fall for common hoaxes.

Most organisations lack the resources to teach the average user all the practical computing skills needed to evaluate hoaxes accurately enough to realise that (for example) JPEG files are
not a likely virus transmission vector. It's far more practical (1) to encourage a technically-minded IT person to keep track of current hoaxes, chain letters, and related issues and (2) incorporate a statement into E-mail policies, Acceptable Usage Policies etc. to the effect that users should -not- pass on -any-chain letters or launch into panic measures without checking with a suitably qualified and authorized person. [Harley1]

3.2 Apple File Exchange

One of the strengths of the Macintosh has always been interconnectivity and interoperability. Apple themselves have long dabbled in such goodies as Apple IIe cards (for compatibility with the old Apple II systems), DOS-compatible 5.25" external drives, PC Compatibility Cards etc., and many (often cheaper!) third-party utilities have appeared to address compatibility issues. However, this very connectivity can be a cause for concern.

The earliest known instances of in-the-wild viruses [Slade] probably originated on Apple II systems in 1981/1982. “Apple II computer diskettes of that time, when formatted in the normal way, always contained the disk operating system. The programmer attempted to find the minimum change that would make a version of DOS that was viral and then tried to find an “optimal” viral DOS.” I was reminded of this by a posting to Virus-L in which the writer mentioned using a PC Transporter Card to transform his cuddly IIgs into a PC-XT clone for use in virus testing: an interesting pre-figuring of the DOS emulation issue which will be addressed later in this paper. Most contemporary Mac users are unlikely ever to meet with an AppleDOS/ProDOS disk at all, let alone an infected one. It is quite possible to read a ProDOS disk with Apple File Exchange (AFE), a utility supplied with some versions of Mac OS, but not for the infection mechanism to work across such disparate operating systems.

Most users are more concerned with compatibility with the PC than with the Apple II, and that is what Apple File Exchange is/was generally used for. AFE is not memory-resident: it is run for as long as it is needed to mount an ‘alien’ disk and copy files to or from it, then terminated: otherwise, programs running concurrently are liable to get confused. It includes limited file translation capabilities, but third parties such as DataViz made available extra AFE translators. AFE is hardly transparent, but generally works quite well.

There were a few somewhat similar DOS packages such as MacSee and Mac-ette: these were even clunkier and could not read Mac double-density disks (this is a limitation of the hardware which also applies to later and more sophisticated utilities).

The viral implications of this class of software are addressed below, since they are not significantly different in principle to the implications of memory-resident disk-mounting utilities.

3.3 Memory-Resident PC-Disk Mounters

Apple File Exchange was supplied with Macintoshes up to System 7.5. From 7.5 onwards, the PC Exchange control panel was included with the system software. PC Exchange and similar products such as DOS Mounter require the use of the DOS-compatible high-density 3.5” SuperDrive supplied with nearly all Mac models from 1989. There are somewhat similar utilities for DOS and Windows which are less commonly used. Again, PC-hosted utilities of this sort can’t read double-density diskettes.

Macintosh utilities in this class generally work by counterfeiting a Mac Desktop and Resource Fork on the target diskette to allow the diskette to be mounted in the same way as a Mac diskette, though more recent versions are able to work with write-protected diskettes. The Macintosh ‘footprint’ on a modified floppy disk is normally seen by MS-DOS as hidden files and directories, though older PC operating system versions sometimes get confused and see the disk as corrupted or containing bad sectors. (Some memory-resident Macintosh anti-virus utilities also leave a hidden footprint on DOS diskettes.) They usually allow the formatting of diskettes in MS-DOS (or ProDOS) format (in fact, Apple File Exchange does this, too, rather less transparently).

DOS disks infected with PC boot-sector infectors can usually be read by such utilities, but boot sector viruses are not a direct threat to Macintosh disks, since there is no way

for the bootstrap code to be executed except under PC emulation - see 3.5. The same applies to conventional PC-specific file infectors. Macro viruses affecting applications common to both platforms are a significant danger. And, of course, infected files and disks can be passed on via a system which is -not-vulnerable to a system which -is-. [Harley2] Obviously, infected files can be transferred or copied in either direction. It's perfectly possible for a Mac-specific virus to be transmitted via PCs, even though PC operating systems don't directly support the dual-fork file format characteristic of MacOS (see Appendix I).

I have received reports of Mac diskettes being read on a BSI-infected PC using an appropriate utility, whereupon the diskettes became unreadable on a Macintosh. It's also important to realise that while some PCs can read/write cross-formatted PC disks (high-density diskettes formatted to 720k or double-density disks formatted to 1.44Mb), Macintosh utilities are not so tolerant. Cross-formatting is, in any case, -never- a good idea. [Harley3]

3.4 Shared media

Some media, such as Zip disks, Syquest cartridges and Compact Disks, can (with appropriate software and hardware) be read and/or written to on PCs -and- Macintoshes. PC boot-sector and partition-sector infection is rarely an issue. However, the same issues apply to these as to diskettes, as regards native and cross-platform file and macro viruses. In fact, reports of Macintosh CDs containing macro-virus-infected documents are circulating as I write (June 1997).

3.5 PC Emulation

The situation is quite different where a Macintosh runs actual PC emulation. In this case, Mac-specific viruses are not usually the problem, though PC emulators usually support direct transfer of files between the emulated PC and the Macintosh desktop, in which case the issue of heterogeneous virus transmission may arise. The most common scenario is infection of the emulated PC by an infected disk or file from a 'real' PC, though it's perfectly possible for an infected emulator to transfer infection to a real PC.

I am aware of three major current options for full emulation of the IBM-compatible PC on Macintoshes, though Lismore Software Systems are due to release a similar (but less ambitious) product in summer 1997. (http://www.lismoresoft.com/)

Insignia Solutions have offered DOS emulation on the Macintosh and some Unix platforms for many years. They currently offer SoftWindows 3.0 (which, confusing, actually incorporates Windows 3.1 rather than 3.0), and SoftWindows 95. They also have a product called NTRIGUE, a Windows NT application server which supports Macintosh clients, among others. SoftWindows is, in principle, vulnerable to most of the virus risks associated with 'the real thing', though the precise effects of a specific virus may be unpredictable. The virus-related risks associated with NTRIGUE are not documented, and not considered further here. (http://www.insignia.com/)

Connectix Corporation are, at time of writing, due to release Virtual PC, another software emulation solution which is claimed to be capable of running just about any Intel-hosted operating system, including PC-compatible versions of Unix. (http://www.connectix.com/)

Both these products claim extensive emulation of PC hardware capabilities and connectivity using the native peripherals. However, both require serious Mac hardware and copious memory to function acceptably.

PCI-based Power Macs can also make use of Apple's own PC Compatibility Cards, essentially a Pentium on a card. These can be fast and effective, but don't integrate so easily into the Mac desktop. The Orange Micro DOS Compatibility Card is said to be more compatible, and also to support a wider range of PC operating systems.

Informal testing with a selection of common PC viruses, SoftWindows PC emulation software, and standard PC anti-virus software, indicates that the emulation is usually robust enough to accommodate both infection and disinfection, though it would surprise me if -all- viruses and -all- anti-virus software behaved identically on -any- emulated PC under -all- conditions. Certainly there are may be problems with Windows VxD anti-virus software, for instance, though this tends to be true of 'real' Windows PCs, too.

3.6 Macro Malware

Many Macintosh users don't use Word 6 (previous versions of Word for the Mac don't support WordBasic) or a vulnerable version of Excel. Most macro viruses (if they have a warhead at all) and Trojans target Intel platforms and assume PC FAT-based directory structures and a logical drive C, rather than the Macintosh Hierarchical File System (HFS), so they usually have no discernible effect if and when they trigger on the Macintosh. There have been attempts to write Mac-specific or multiplatform viruses, though, and viruses that manipulate text within a document may work just as well on a Macintosh as on a PC. Specific damage to files and file systems on the Macintosh is easily implemented (see below).

Irrespective of hardware, Mac users with Word 6 or versions of Excel supporting Visual Basic for Applications are vulnerable to infection by macro viruses which are specific to these applications. Indeed, these viruses may infect other files on any hardware platform supporting these versions of these applications.

Word for the Macintosh (version 5.1 or below) does not support WordBasic, and is not, therefore, vulnerable to direct infection. Not only do versions of Word for Macintosh prior to 6.0 not understand embedded macros, but they can't read the Word 6 file format unaided. There is, however, at least one freeware utility which allows Word 5.x users to read Word 6 files. This doesn't support execution of Word 6 (or WinWord 1 or 2) macros in Word 5.x, so infective or damaging (or even innocent) macros can't work and are not retained. To be strictly accurate, the filter opens a Word 5.x formatted copy of the original file. The formatting of the original file is preserved as far as forward compatibility allows, but macros are discarded.

However, Word 5.x users may contribute indirectly to the spread of infected files across platforms and systems. It is perfectly possible for a user whose own system is uninfectable (and who doesn't have macro-aware anti-virus software installed) to act as a conduit for the transmission of infected documents, whether or not s/he reads it personally, since the original file is not modified when it is read by the Word 5.x filter.

A similar scenario occurs where a user uses word-processing software from a different vendor. If File | Save As or an equivalent command is used instead of Save (provided the document is not Saved in the beforehand), the file may be saved as a

new file in the format native to the current word-processor, while the original file is remains unmodified. Given the problems that can arise when translating one file format to another, especially in the case of a complex document (one containing graphics or other embedded objects, for example), it actually makes sense in principle to keep the original file unmodified. In this case, however, the only guaranteed way to avoid passing on an infected file without using a known-virus scanner is to avoid passing on the original file. This strategy seems to me to be unreliable, in that it may demand 100% comprehension and co-operation from a range of users.

Suggestions sometimes made include using a safe common format such as Rich Text Format (RTF) or generating a -new- document in the -original- format—usually Word—from the Saved As copy. It's unlikely, though, that this would result in a Word file identical to the original in all respects (quite apart from the absence of macros). The File | Save As operation can also be spoofed by a virus to report untruthfully that the file has been saved to a safe format.

It's therefore usually necessary to protect systems that aren't themselves directly vulnerable, firstly with a view to protection in the future from infected files acquired now, if the user should change to Word/Office in the future, but mostly to guard against the inadvertant spreading of infected files by Mac users sharing files via floppy disks, file servers, electronic mail, etc. (a phenomenon sometimes referred to as heterogeneous virus transmission). [Radatti]

Allow me to refer you to Harley's 1st Law of Virus Management:

> Just because a virus doesn't infect or trigger on -your-system, that doesn't mean you can never be held responsible for spreading it.....

Let us consider an instance where Word 5.x user A passes on an infected file to WinWord user B, and either that file or secondarily-infected files are passed on through users C, D, E and F before the infection is noticed by G, who is running an up-to-date commercial scanner on his system. For many macro viruses, the infective mechanism works irrespective of the hardware or operating system used by the intermediate users, as long as they're running a vulnerable application, usually Word 6 or later. However, this scenario does not depend entirely on the infective macro: passing on the original file will do just as well.

Inadvertant transmission across platforms can have a number of unpleasant consequences.

3.6.1 Direct damage to vulnerable systems which aren't themselves protected.

Some macro viruses have a payload such as deleting all files matching a given path/filename template. This is particularly easy to do on a PC, where it's a reasonably safe bet that there's a C:\DOS, C:\WINDOWS etc. on a Windows 3.x machine, but it's entirely feasible to write Mac-specific code along the lines of the following snippets of pseudocode:

- If (This_is_a_Mac) THEN (delete_all_files_in_current_folder)
- If (This_is_a Mac) THEN (delete_all_files_in(StartupDiskName:system))

In this instance, all users from A to F risk direct damage *if* they use a vulnerable application or application version. (Of course, G is not invulnerable, but in this

scenario his/her likeliest risk is from a virus or Trojan not yet known to his scanning software.)

3.6.2 Loss of reputation

A to G are all at some risk, even if G detected the virus with an on-access scanner at the point of entry. One of the reasons useful virus damage statistics are practically non-existent is the corporate fear that -any- association with the 'v' word will lead to loss of reputation. Such is the mystique of virus, that this fear is not without justification. As a trivial example, "I hear G. discovered a virus" translates rather easily to "Apparently G. had a virus", transforming G from an informed user taking due precautions and reacting appropriately, to a victim who may have been responsible for his or her plight, due to carelessness or worse.

3.6.3 Loss of goodwill

A to G are at risk.

Viruses promptly detected at point of entry rarely excite much excitement and antipathy as far as the detecting organization or individual is concerned, though a prudent organization will have policies regarding the notification of such incidents to the immediate source of the infected file, and monitoring further transactions with that source. However, the 'guilty party' F may be less than grateful to G, and even less to E.

Where the virus has the chance to propagate and/or trigger on G's system(s) before detection, cordiality is likely to degrade accordingly.....

3.6.4 Loss of trust - Scapegoating and witch-hunting

A to G are all at risk.

If G's discovery of the virus is not immediate (detected, for instance, by a scheduled scan or scan at boot-up after infection, the source of the infection may not be clear. G may even be accused of 'spreading' the virus. Harley's Second Law of Virus Management:

> The degree of corporate panic, expressed as scapegoating, is inversely proportional to the effectiveness of an organisation's anti-virus measures.

3.6.5 Indirect damage through user/management panic

A to G are at risk.

It's not unusual for panicking users and organizations to cause damage through inappropriate action such as unnecessary reformatting, reinstallation, destruction of floppy disks etc., totally disproportionate to the destructive potential of the virus. Such a reaction may also be the result of a degree of over-engineering in security policies: for instance, the default recommended response to the discovery of a virus on National Health Service systems in the United Kingdom is:

- memory and disks should be wiped clean

- safe master copies of software should be reloaded
- data should be reloaded from the most recent backup

(Disinfection with a commercial utility is a permitted alternative under fairly strict conditions) [IM&T]

G's understanding of the situation may not match the ability of G's scanner in terms of virus detection, or the scanner may detect but not clean the virus. In this case, G's grasp of virus issues may be critical.

Harley's Third Law of Virus Management:

> The degree of corporate panic, expressed as over-reaction and inappropriately severe recovery measures, is inversely proportional to the general level of corporate understanding of virus and anti-virus technology and management issues.
>
> (It could well be argued that the 2nd Law is a special case of the 3rd, of course.)

3.6.6 False Positives

A to G are at risk from the possibility of inappropriate action as a result of G's scanner false alarming. A to F are also at risk from false positives from other sources. G is less so, but remains at risk, depending on how effective his/her scanner is, or is perceived as being. If a scanner known to be prone to be false alarms detects a virus, where a scanner known to be more accurate doesn't detect it, a knowledgeable person is likely to incline towards the second scanner where both are sufficiently up-to-date, but will probably check independently with a third scanner. A less knowledgeable person is likely to assume that the first scanner is correct and that the second is less 'capable'.

3.6.7 Legal Action

A to F are principally at risk.

This normally takes the form of civil action, though it's by no means inconceivable, given the low general level of understanding of virus transmission issues, that an individual or organization inadvertantly transmitting a virus might find themselves accused of the deliberate, malicious transmission of a virus.

Civil action may result from perceived breach of trust, breach of contract, or negligence.

It's possible that lack of due diligence resulting in a breach of data protection legislation might lead to criminal -or- civil action, depending on context.

Virus writers are rarely identified, so not often arrested or sued. However, I expect to see more instances of firms and individuals who unwittingly pass on infections facing litigation. Apart from an upsurge of interest in these issues by those wonderful people who brought you ambulance-chasing, managers and accountants often seem more concerned with establishing responsibility than constructive repair.

Is it reasonable, though, that users of vulnerable applications (let alone non-users!) should be held responsible for secondary infections transmitted through their systems?

After all, it is often argued that Word's extreme vulnerability derives from a number of design decisions which are, from a security point of view, seriously flawed.

- Macro code can exist and execute transparently when embedded in what to the user looks like a data file. Compare the tiny numbers of successful macro viruses parasitising other applications which preserve a distinction between data files and macro files. Viruses generally rely upon the invisibility of infective code, of course, but this transparency adds an extra layer of invisibility both to viruses and to Trojans, since even users who are aware of the risks of running unchecked executable code may be unaware that they are doing so when they open a document.
- The WordBasic macro language is so wedded to the command structure of the application that it simply isn't feasible to simply "switch off" the macro feature.
- A further layer of invisibility is added by the fact that macro code can be 'execute-only': that is, encrypted so that it can't be modified or read, even if its existence is known. While the encryption is trivial, and utilities now exist which will perform the decryption, the use of such utilities is by no means common. The concept of execute-only macros is consistent with Microsoft's implementation of GW-BASIC, where a program file could be SAVE-d in an encoded format so that it could not be LISTed or edited. This has obvious advantages for programmers in either language wishing to protect their code, for legitimate -or- malicious reasons. The maliciously-minded have chosen to make more use of this facility in WordBasic than in GW-BASIC, however, and we are all obliged to live with the consequences of the need for an additional layer of protection.

WordBasic and Visual Basic for Applications (VBA) combine a comparatively simple syntax which presents few problems to users familiar with other dialects of BASIC, with a rich, powerful command-set. It's not surprising that malware using these programming platforms are proliferating at a rate which renders the traditional 1-to-3 month definitions update increasingly ineffective. Unfortunately, the irresistible and rapid rise of the macro virus has significantly raised the amount of commitment to financial and administrative investment needed to ensure effective protection. Sadly, the average user, only just beginning to comprehend this fact, is probably much more at risk than Microsoft's design teams. Microsoft shows no sign of admitting to ownership of this problem, emphasising instead the steps it is necessary for users to take to protect themselves. [Microsoft2]

Microsoft does not show signs of commitment to a ground-up rebuild of Word and WordBasic: rather, its strategy seems to centre on making proprietary information available to the National Computer Security Association (NCSA) and to the "anti-virus community". Since most vendors focus primarily on known-virus scanning (though heuristic analysis is now starting to be seen applied in anti-macro technology), this seems to leave the anti-virus community with most of the responsibility for keeping abreast or ahead of macro-malware technology, while Microsoft shelters behind its Non-Disclosure Agreements and the presumed absolute expertise and authority of the NCSA.

3.7 Other Emulation Issues

PC emulation on the Macintosh is not, of course, the only cross-platform virus issue. Macintosh emulators exist for Amiga and Atari models with a Macintosh-compatible Motorola CPU, and viruses specific to the Aladin emulator are known to exist (see

Appendix A). It's also known that Macintosh viruses may damage files on Sun systems running MAE (Macintosh Application Environment) or AUFS [Spafford]. These issues are not further discussed here.

4 SOLUTIONS

4.1 Software Solutions

The range of available freeware, shareware and commercial anti-virus packages has contracted dramatically over recent years. The likes of Virus Rx, CE Software's Vaccine CDEV, Ferret, KillScores, 1st Aid, Interferon, AntiToxin, VirusBlockade, VirusDetective, and Mac-Tools Anti-Virus are rarely seen now, and are not discussed further here.

4.1.1 Gatekeeper

Gatekeeper was (and is) not a scanner, but a generic tool, essentially a behaviour blocker. Primarily, it is a system extension which monitors classes of operation which might flag virus infection. Programs which can legitimately perform such operations can be granted file privileges, to reduce the incidence of false negatives: a list of such programs is distributed with the program, and programs not included can be added with the "Gatekeeper Controls" control panel. Later versions of Gatekeeper also include Gatekeeper Aid, a system extension which scans for and removes known viruses and close variants, with the intention of combining the advantages of both behaviour blocking and known-virus scanning.

It is no longer supported, maintained or developed by its author, apparently because of the maintenance workload, but is still available on some sites, including the University of Texas. The author passed on some third-party reports of some problems with System 7 Pro, but further research and development with later versions of Mac OS or models of PowerMac has not been reported.

It appears that a number of Mac users are still using Gatekeeper [some in tandem with Disinfectant]. Current users are likely to find that the utility puts up an alert message on launch indicating that the program is out-of-date. This message can be (and is) frequently ignored (in fact, it can be disabled with ResEdit), since it is, in general, the whole intention of generic solutions to bypass the need for updating. Unfortunately, since development ceased before the onset of the macro virus plague, the known-virus scanner doesn't address the macro virus problem, and informal testing indicates that the operations associated with macros (viral or otherwise) are not flagged by the behaviour blocking component.

4.1.2 Disinfectant

At the time of the last upgrade of Disinfectant (version 3.6 in April1995), there were no known macro viruses in the wild, HyperCard infectors apart. Disinfectant deserves its reputation as an excellent anti-virus package with exemplary on-disk documentation, and no price tag. Indeed, the comparative rarity of native Macintosh viruses is probably largely due to the large number of Disinfectant users, past and present. However, it was never a complete solution, since it doesn't detect all the forms of malware that a commercial package usually does. In fact, Disinfectant was always intended to deal with conventional viruses, not trojans, jokes or macro/script

viruses, and its author has been at pains to point this out in his documentation, on Usenet and elsewhere. Unfortunately, many users are nonetheless unaware of the distinctions between these classes of malware.

Neither Disinfectant, Gatekeeper, nor the combination of both, can now be regarded as sufficient protection for systems on which applications vulnerable to macro viruses are installed. Nor are they adequate for systems which are not directly vulnerable but which may be a channel for the inadvertant dissemination of macro viruses.

There are two freeware macro packages which address the macro virus problem. Both are predominantly generic, though Microsoft's ScanProt protection tool can often detect and remove WM.Concept.

4.1.3 Microsoft's Protection Tool (ScanProt/MVTool)

Microsoft's Macro Virus Protection Tool detects (some strains of) Concept (Nuclear and DMV are also mentioned in the documentation, but it's clear that they are mentioned only as examples of how ScanProt deals with possibly malicious macros generically: there is no indication that it actually recognises them), but its principal purpose is merely to warn users that the document they are about to open contains macros and offer the choice of opening the file without macros, opening it with macros, or cancelling the File Open.

There are a number of ways of opening a document with the Microsoft macros operational which bypass them, e.g. dragging a document onto the Word icon, opening a mail attachment, or by using the Recent Documents list.

The Protection Tool can be used to scan and clean Concept infections, but there are a number of possible problems with it.

- Earlier versions could only handle a limited size of directory tree, and ran very slowly if a large number of files required scanning. Speed is certainly still a problem: I haven't tested the overflow problem so far, on Mac or PC.
- Files created in Word for Windows won't be scanned until they've been opened from within Word 6 for Mac (this is a system issue, not a bug in the code). However, Microsoft suggest opening the file in Word for the Macintosh and saving it before scanning. This will indeed result in the document being stamped with the correct file signature, but also risks execution of the infection mechanism if the file is, in fact, infected.
- Infected files embedded in OLE2 files or e-mail files will not be detected.
- The protection tool is not consistently able to disinfect templates.

Microsoft themselves formerly pointed out the limitations of MVTOOL on their webpage and now recommend the use of an NCSA-certified anti-virus utility [Microsoft3]. Macintosh users should, however, be aware that:

(i) NCSA certification is a comparatively slow process. Given the current rate of growth of the macro virus threat, there may be a significant discrepancy between the test set in use when certification was awarded, and the set of viruses currently in-the-wild when a customer actually receives the product.

(ii) Macintosh-specific viruses are not included in the WildList: NCSA certification is simply not very Macintosh-oriented. Macintosh-hosted known-virus scanners do not normally share 100% identical virus definitions with their PC-hosted siblings.

The Microsoft tools should only be considered as better than nothing at all as long as users are aware of their limitations and weaknesses: they can detect and clean only (some strains of) Concept; they can't distinguish between malicious and legitimate macros; and they can be bypassed, deliberately or otherwise. Scanning tool functionality is built into some versions of Word, Excel and Powerpoint, but should not be relied upon exclusively. As with Microsoft's dabbling in anti-virus software with Microsoft Anti-Virus, a false sense of security may be more dangerous than being unprotected but aware of the risks.

4.1.4 MacroList

Padgett Peterson's MacroList macro detection tool is also a generic tool, not a scanner. It checks for the presence of macros, disables (optionally) automacros, includes a CLOSE DOC button for a safe exit from a possibly infected document, flags key reassignment and enables examination of macros.

4.1.5 Roll-Your-Own Solutions

Suggestions are frequently made on Usenet, mailing lists etc. for protective measures which can be made within Word. These may be effective in some instances, but none of them are a universal solution.

- Disabling automacros (AutoOpen, AutoClose, AutoNew, AutoExit)

This can be done with a simple snippet of code calling DisableAutoMacros. It can't be used to disable AutoExec, and doesn't have any effect on the sizeable body of macro viruses which don't infect by using automacros. Alas, it's not possible to disable macros altogether. Even if you could, they're such an integral part of the way that Word works, that the application would become more or less unusable. Until Microsoft decide to rewrite Word from the ground up using a safe quasi-java sandbox security model, I don't see much likelihood of this changing. Disassociating data files from macro files would be a good start, though: the idea of having macros and data in the same document has not turned out well.

- Disabling the autoexec macro by holding down the shift key at startup or using the /m Startup switch.

Unfortunately, this is not reliable on Macintoshes -or- PCs. The mechanism by which Startup switches are activated on Macintoshes is startlingly ineffective in all respects.

- Write-protecting the Normal template

Not insurmountable. "Anything which can be done in software can be undone in software." [Virus-L]

In any case, Normal/NORMAL.DOT isn't necessarily the global template, and write-protecting it can cause a nuisance when it needs to be modified legitimately.

Replacing with a clean copy every time Word is launched is sometimes suggested, but relying on it exclusively is not recommended, since it doesn't stop infection of other files and their subsequent dissemination, or temporary reinfection of the global template.

* Using a safe common format such as RTF

Using Save As doesn't guarantee that the file -has- been saved in the intended format. It's only possible to be sure if it's possible to examine the file outside the Microsoft Office environment (with teachtext or a viewer utility, for example). Not all viruses are as considerate as Concept about flagging the fact that they're Saving As templates (though it's possible to see whether a file is a template if "By Icon" is selected in the Finder's View menu option). Suggestions which involve using Word commands can not be guaranteed 100% safe, since there is usually a corresponding WordBasic statement such as FileSaveAs or FileConfirmConversion, with the consequent risk of subversion by a malicious macro with the same name. Vesselin Bontchev lists 122 system macros from Word 6 and Word 97 which might be intercepted by malicious macros [Bontchev].

- Using a filter or another word-processing program to strip the macros from a possibly-infected document.

The filter usually used to enable Word 5.x to read Word 6 documents doesn't actually modify the original document, it opens a new one which contains the same content, but not the macros. Consequently, using Word 5 as a filter doesn't, by itself, save the user from the risk of having infected files still on their system and, worse, passing them on to other vulnerable users. The same may not be true of other file conversion/transfer programs such as those marketed by DataViz (http://www.dataviz.com/), but it's likely that many users would take a copy of the original before working on one or the other copy in a 'safe' application, so the risk would still exist of an infected file being passed on.

4.1.6 Commercial packages

There are four main commercial anti-virus packages for the Macintosh, currently: Virex, SAM (Symantec AntiVirus for Macintosh), McAfee ViruScan, and Dr. Solomon's Antivirus Toolkit for Macintosh. All four detect Trojans, HyperCard infectors, and other macro viruses. Dr. Solomon's also detects boot sector viruses on DOS diskettes, though it can't clean them.

- Scheduling

All four packages offer some sort of scheduling, i.e. scans launched automatically at pre-determined times or intervals.

- Real-time (on-access) scanning

All four packages include a system extension or control panel which ensures that files are scanned when accessed, as well as offering scanning 'on-demand', i.e. when the

user chooses to scan. Low-end Macs, especially 68K models, may have problems running these.

- Behaviour monitoring

Optionally, the SAM Intercept puts up an alert box if it detects ‘suspicious activity’.

- Checksumming

Offered by SAM and Virex. Possible virus infections are flagged by detecting changes to the application.

- On-demand scanning

The classic defence against known viruses, offered by all four packages. Regular updates are available.

Sophos don’t have a stand-alone Macintosh scanner. There is a Macintosh version of their Intercheck client software, however. This runs as a system extension on the client Macintosh, which calls a server copy of their Sweep scanner. Since there isn’t a version of Sweep for Mac Os, this isn’t a realistic solution for ‘pure’ Apple networks. Most server-hosted scanners now detect macro viruses, but not usually Mac-specific viruses. Notable exceptions are VFind (Unix) and Norton AntiVirus for NetWare.

4.2 Administrative Solutions

Contrary to the impression given by vendor advertising and some widely publicized surveys, the main costs of virus control are rarely those entailed by recovery from damaging virus payloads, but the costs of establishing detection and protection in the hope of not incurring greater costs as a result of direct or indirect damage such as those types considered in section 3.6.

Nevertheless, the costs of not establishing these measures can be considerable, especially in corporate environments. Macintosh sites are now learning that the myth of Macintosh immunity to mainstream virus problems has no basis in reality.

Regrettably, few sites can now allow themselves the luxury of relying on freeware solutions which were never intended or claimed to defend against the full range of current threats. Most are now obliged to consider expensive commercial solutions. These are largely focused on known-virus scanning, though I believe that generic solutions can be helpful as a supplementary defence, if implemented properly (not only at the software engineering level, but in terms of how the software is administered within an organization).

I believe strategy and implementation to be a major and largely unconsidered cost centre, even in the PC world, where virus-related threats are more familiar and (a little) better understood. It is, however, a necessary cost: simply buying software is, in itself, no protection whatsoever.

There are no one-fits-all administrative solutions, and any anti-virus vendor or security consultant who brushes aside these issues should be kept firmly in their place. If there were such solutions, this paper would not, in any case, be the place to discuss them at length. However, the issues raised below are as relevant to Macintosh virus-management as to other platforms, and deserve careful consideration.

4.2.1 User Education

This is sometimes offered as a panacea. In reality, it is always under-resourced. At best, it is expensive and difficult to administer and maintain, and never to be relied upon. It's probably best to teach as many people as possible a bare minimum about general principles, make software administration as transparent as possible, and make sure that there is a core of IT expertise available (and that users and helpdesk personnel know that it's there). Better to teach them to ring the appropriate number than to expect them to learn about polymorphism. If it's practical to block some entry points with supplementary software such as access control software, viruswalls, or virus-scanning on servers, such measures should be considered, but not taken to be a substitute for protecting the desktop.

4.2.2 IT Staff Training

No organization of any size can afford to be without at least one appropriately qualified and designated person who understands or is prepared to learn about security and virus-management (two issues which are far too often treated as being totally discrete). Inevitably, time spent on these matters entails opportunity costs. More time dealing with and forestalling virus threats means less spent on other tasks, just as money spent on insurance or business continuity measures means less to spend on more glamourous projects. That isn't to say that every organization needs a full-time virus expert, but virus-management isn't something which should be done during coffee breaks.

It isn't always a good idea to farm it out to busy system administrators, firewall administrators etc., at least without ensuring that they have the necessary breadth of knowledge or committing them to specialist training.

It isn't practical to train up every IT person as a virus expert. They should be taught enough to stop them turning a problem into a crisis, and when to refer a problem to someone with more appropriate expertise. The most difficult task is often to stop them assuming they are experts (a problem not confined to computer virology, by the way).

4.2.3 Policies

Unimplemented policies are worthless. However, a good policy can be the backbone of good practice.

Anti-virus policies should be considered carefully. All too often, such policies, including the model policies available from some major security sources, focus on small risks such as pirated software and bulletin boards and ignore large risks such as exchange of infectable documents, or passing on infected media to third parties. Nor should they be considered as completely isolated from other an overall security policy, system security policies, and policies dealing with specific issues such as acceptable use of the Internet (possibly including use of E-mail and newsgroups), or the procurement, use and disposal of disks, diskettes and other media.

6 CONCLUSION

Summer 1995 changed a great deal in anti-virus circles, and the ripples continue to spread. Apple have also gone through many changes, and the future consequences have yet to be seen. One thing is clear, though: as far as virus management is concerned, the Macintosh is back in the mainstream.

ACKNOWLEDGEMENTS

This paper is long enough already. Nonetheless, I owe a debt of thanks to:

- Past and present employers Ron Caterall and John Wise for their encouragement.
- All those (too many to list here) who contributed material, ideas, proofing, and general encouragement to the alt.comp.virus FAQ and the "Viruses and the Macintosh" FAQ.
- Jacqueline Landman Gay for her considerable help on HyperCard and HyperCard viruses.
- Susan Lesch for her encouragement, proofreading, and suggestions for improvements to this paper and everything else of any substance that I've written in the last two years.
- Katy Andrews for proofreading and many years of friendship.
- My daughter Katherine, for reminding me that there's more to life than virology.

REFERENCES

[Lesch] Susan Lesch: personal communication

[InfoWorld] http://www.infoworld.com/cgi-bin/displayArchives.pl?97066.eapplescript.htm

[MacWeek] http://www.macweek.com/mw_1045/ga_qtml_anal.html

[Gay] Jacqueline Landman Gay, Hyperactive Software: http://www.hyperactivesw.com/

[Virus-L] Nick FitzGerald et al.: "Frequently Asked Questions on Virus-L/comp.virus" Version 2.0 (comp.virus).

[Microsoft1] Microsoft Word Developer's Kit: Microsoft Press.

[Harley1] David Harley: "Dealing with Internet Hoaxes/Alerts" (EICAR News Volume 3 No. 2).

[Slade] Robert Slade: "Guide to Computer Viruses - 2nd Edition" (Springer)

[Harley2] Harley, David: "Viruses and the Macintosh FAQ"
http://webworlds.co.uk/dharley/
http://www.totalweb.co.uk/dharley/

[Harley3] David Harley et al.: alt.comp.virus FAQ
http://webworlds.co.uk/dharley/
http://www.totalweb.co.uk/dharley/

[Radatti] Radatti, Peter: NCSA Conference 1992, as quoted in "The NCSA Guide to Enterprise Security" by Michel E. Kabay (McGraw-Hill).

[IM&T] The NHS IM&T (Information Management and Technology) Security Manual, V1.0, February 1996 (NHS Executive Information Management Group).

[Microsoft2] http://www.microsoft.com/

[Microsoft3] http://www.microsoft.com/msword/freestuff/mvtool/virusinfo.htm

[Norstad] John Norstad: "1997 Apple Worldwide Developers Conference (WWDC) - NUMUG Trip Report - a Rhapsodic Adventure" (Northwestern University, 1997).

[Spafford] Professor Eugene Spafford: personal communication.

[Gay2] Jacqueline Landman Gay: personal communication.

[Swagerty] Bill Swagerty: Vaccine Documentation.

[Bontchev] Vesselin Bontchev: "Possible Macrovirus Attacks and how to Prevent Them" (Proceedings of the Sixth International Virus Bulletin Conference).

APPENDIX A: Macintosh File & System Viruses

<Condensed from "Viruses and the Macintosh" [Harley2]>

- AIDS - infects application and system files. No intentional damage. (nVIR B strain)
- Aladin - see Frankie
- Anti (Anti-A/Anti-Ange, Anti-B, Anti Variant) - can't spread under system 7.x, or System 6 under MultiFinder. Can damage applications.
- CDEF - infects desktop files. No intentional damage, and doesn't spread under system 7.x.
- CLAP: nVIR variant that spoofs Disinfectant to avoid detection.
- Code 1 - file infector. Renames the hard drive to "Trent Saburo". Accidental system crashes possible.
- Code 252 - infects application and system files. Triggers when run between June 6th and December 31st. Runs a gotcha message ("You have a virus. Ha Ha Ha Ha Ha Ha Ha Now erasing all disks... [etc.]"), then self-deletes. No intentional damage. Can crash System 7 or damage files, but doesn't spread beyond the System file. Doesn't spread under System 6 with MultiFinder beyond System and MultiFinder.

- Frankie - only affects the Aladdin emulator on the Atari or Amiga. Infects application files and the Finder. Draws a bomb icon and displays 'Frankie says: No more piracy!"
- Init 17: infects System file and applications. Displays message "From the depths of Cyberspace" the first time it triggers. Accidental damage, especially on 68K machines.
- Init 29 (Init 29 A, B): Spreads rapidly. Infects system files, applications, and document files (document files can't infect other files, though). May display a message if a locked floppy is accessed on an infected system 'The disk "xxxxx" needs minor repairs. Do you want to repair it?'. No intentional damage, but can cause several problems.
- Init 1984: Infects system extensions (INITs). Works under Systems 6 and 7. triggers on Friday 13th. Damages files by renaming them, changing file signature and time stamps, deletion.
- Init-9403 (SysX): Infects applications and Finder under systems 6 and 7. Attempts severe intentional damage. Only found on Macs running the Italian version of Mac OS.
- Init-M: Replicates under System 7 only. Infects INITs and application files. Occasionally deletes files.
- MacMag (Aldus, Brandow, Drew, Peace) - first distributed as a HyperCard stack Trojan, but only infected System files. Rarely found, since trigger date was in 1988.
- MBDF (A,B): originated from the Tetracycle, Tetricycle or "tetris-rotating" Trojan. The A strain was also distributed in Obnoxious Tetris and Ten Tile Puzzle. Infects applications and system files including System and Finder. Accidental damage.
- MDEF (MDEF A/Garfield, MDEF B/Top Cat, C, D): infect System file and application files (D doesn't infect System). Some unintentional damage.
- nVIR (nCAM, nVIR A, B, C - AIDS, Fuck, Hpat, Jude, MEV#, nFlu, nVIR-f, prod, zero): infect System and any opened applications. Extant versions don't cause intentional damage. Plays tricks with sound.
- Scores (Eric, Vult, NASA, San Jose Flu): aimed to attack two applications that were never generally released. Unintentional damage.
- T4 (A, B, C): infects applications, Finder, and tries to modify System so that startup code is altered. Under System 6 and 7.0, INITs and system extensions don't load. Under 7.0.1, the Mac may be unbootable.
- WDEF (A,B): infects desktop file only. Doesn't spread under System 7. Various unintentional damage.
- Zuc (A, B, C): infects applications. Plays tricks with mouse cursor.

APPENDIX B: Hypercard Infectors

(i) Infection and Protection

Generally, HyperCard viruses append replicative code to the scripts of stacks they infect. HC 9507 also copies resources. [Swagerty]

The Home stack is normally the first stack that HyperCard accesses when it is launched, and is essentially an index

resource, rather like a World Wide Web home page with numerous hot links. By default, the first card in the Home stack (the Home card) is the first card displayed when the application is launched, and usually contains a number of hyperlinks. The Home stack may also contain cards which contain pointers to pathnames (path variables).

All the Home stack's resources can be accessed throughout a session, and its stack script open and active in the message hierarchy, so that all system messages must pass through it. [Gay]. This makes it a prime target for infection. It is possible to take some generic precautions against infection, the most obvious of which is to lock the Home stack under Finder (select the file, press Command-I or select the Get Info option in the File menu, and check the 'Locked' box).

It's also possible to lock a stack with 'set cantModify to True' (HyperCard version 1.2 and higher), and to password the cantModify property. However, it's trivial to unset cantModify from a script (and doesn't require a password).

A further possibility is to "Set lockMessages to true" when messages are not required: this not only offers some measure of defence against infection by not passing messages such as OpenCard, but also speeds up handler execution. However, even if it were practical to cross-script so as to lock messages every time a stack is opened, blocking openCard, openStack and openBackground messages throughout a session would probably seriously degrade performance and functionality. Nor would this be an effective defence against viruses which also trigger on idle. (HyperCard sends a stream of Idle messages to the current card when no handler is being executed and no response is pending to an Answer or Ask command.)

A 'set' handler can be implemented to intercept modifications to the stack script - one such handler is included on the "Hypercard Virus Compendium" web page. [Gay2] Note that this handler will not intercept HC9507 infection, which is not message-based, and that not all stack modifications are a sign of virus activity.

An openStack handler could be used to monitor covert attempts to infect a stack. It's perfectly possible to implement simple integrity-checking in HyperCard by checksumming scripts and checking them against a stored hash code, but it's impractical [Gay] to do this except by implementing it in each stack to be protected.

Inoculation by appending known search strings to the Home stack is sometimes suggested. This is not a generic defence: it can only be implemented for known viruses. It may, of course, trigger false positives if used in combination with known-virus scanners.

(ii) Known HyperCard Infectors

<Condensed from "Viruses and the Macintosh" [Harley2]>

- Dukakis - infects the Home stack, then other stacks used subsequently. Displays the message "Dukakis for President", then self-destructs.
- HC 9507 (Pickle) - infects the Home stack, then other running stacks and randomly chosen stacks on the startup disk. On triggering, may hang the system. Home stack, then other running stacks. No intended effects, but may damage the Home stack.

- HC virus/Hypercard/Two Tunes/Three Tunes - infects stack scripts. Visual/Audio effects.
- MerryXmas - appends to stack script. On execution, attempts to infect the Home stack, which then infects other stacks on access. There are several strains, most of which cause system crashes and other anomalies. At least one strain replaces the Home stack script and deletes stacks run subsequently. Variants include Merry2Xmas, Lopez, and Crudshot.
- Antibody - propagates between stacks checking for and removing the MerryXmas virus, and installs an innoculation script.

APPENDIX C: Trojan Horses

<Condensed from "Viruses and the Macintosh" FAQ [Harley2]>

- ChinaTalk - system extension - supposed to be sound driver, but actually deletes folders.
- CPro - supposed to be an update to Compact Pro, but attempts to format currently mounted disks.
- FontFinder - supposed to lists fonts used in a document, but actually deletes folders.
- MacMag - HyperCard stack (New Apple Products) that was the origin of the MacMag virus.
- Mosaic - supposed to display graphics, but actually mangles directory structures.
- NVP - modifies the System file so that no vowels can be typed. Originally found masquerading as ‘New Look’, which redesigns the display.
- Steroid - Control Panel - claims to improve QuickDraw speed, but actually mangles the directory structure.
- Tetracycle - implicated in the original spread of MBDF
- Virus Info - purported to contain virus information but actually trashed disks. Not to be confused with Virus Reference.
- Postscript hack which disabled some printers by changing the printer password at random (some printers had a firmware counter which only allowed the password to be changed a fixed number of times) so that it was necessary to replace a chip on the printer logic board. [Spafford]
- Welcome Datacomp - the text string ‘Welcome Datacomp’ appears in documents without having been typed. This is the result of using a Trojanised 3rd-party Macintosh-compatible keyboard with this ‘joke’ hard-coded into the keyboard ROM. It’s not a virus - it can’t replicate - and the cure is a new keyboard.

APPENDIX D: Hoaxes, Jokes, Erroneous Alerts - further information

ftp://usit.net/pub/lesjones/good-times-virus-hoax-faq.txt
ftp://members.aol.com/macfaq/good-times-virus-hoax-faq.txt
ftp://usit.net/pub/lesjones/Good-Times-Virus-Hoax-Mini-FAQ.txt
http://webworlds.co.uk/dharley/hoaxes.txt
http://ciac.llnl.gov/ciac/
(Includes pages on hoaxes and chain letters. The virus database includes Mac jokes and false alerts)
http://www.soci.niu.edu/~crypt/
(Crypt newsletter - worth reading for its general anti-hype content)

http://www.csmil.umich.edu/~chymes/newusers/Think.html
http://www.av.ibm.com/current/FrontPage/
"Anti-Virus Online": includes hype alerts and a good article by Joe Wells, plus Jimmy Kuo's "That's Not a Virus!" paper on virus-related false alarms.
http://www.urbanlegends.com/
http://www.kumite.com/myths/
http://www.drsolomon.com/
Includes an excellent article on hoaxes by Graham Cluley.
http://www.salig.demon.co.uk/hoaxFAQ.htm
Martin Overton's Hoax FAQ

Most of the other useful vendor sites now include hoax information, including:

http://www.datafellows.com/
http://www.symantec.com/
http://www.mcafee.com/

APPENDIX E: WordBasic and the Mac [Microsoft]

(1) WinWord-Specific Statements & Functions

A number of WordBasic statements and functions are specific to Word running under Windows. Most of them relate to controlling application windows.

AppMaximize; AppMaximize()	AppSize
AppMinimize; AppMinimize()	AppWindowHeight; AppWindowHeight()
AppMove	AppWindowPosLeft; AppWindowPosLeft()
AppRestore; AppRestore()	AppWindowPosTop; AppWindowPosTop()
AppSendMessage	AppWindowWidth; AppWindowWidth()
AppShow	

Connect - connects with network drive (on Mac use MountVolume).	HelpWordPerfectHelpOptions
ControlRun - runs Clipboard or Control Panel.	MicrosoftAccess
Environ$() - returns a string associated with a DOS environment variable.	MicrosoftPublisher
ExitWindows	MicrosoftSchedule
FilePrintSetup - changes printer or printer setup	RunPrintManager
HelpWordPerfectHelp	ToggleScribbleMode - Toggle hand annotation mode (Windows for Pen Computing only).

(2) Macintosh-Specific Statements and Functions

There are also a number of statements and functions valid only on the Macintosh. Those prefixed with AOCE or FileAOCE are valid only if PowerTalk is installed. (PowerTalk is a network mail system utility supplied with System 7.5 and later.)

DlgStoreValues - save custom dialog box settings.	FileDocumentLayout - Page formatting controls.
DlgLoadValues; DlgLoadValues() - retrieve custom dialog box settings.	FileMacCustomPageSetupGX
EditCopyAsPicture - copy to Clipboard as graphic.	
EditCreatePublisher - relate to Publish & Subscribe.	FileMacPageSetup
EditPublishOptions	FileMacPageSetupGX
EditSubscribeOptions	FilePrintOneCopy
EditSubscribeTo	FileQuit - exit Word.
EditFindBorder - specify formats in Find/Replace.	ListCommands - list built-in commands with key & menu assignments.
EditFindFrame	MacID$() - converts application signature or file type to a value equivalent to the application filename. Can be used with Files$(), FileOpen and Kill to use file types to identify groups of files, since the Mac doesn't support "*" and "?" as wildcard characters.
EditFindTabs	MacScript, MacScript$() - run an AppleScript

	script resource. Note that WordBasic on the Macintosh offers substantial AppleScript support independently of MacScript and MacScript$() through the "Do Script" AppleScript term.
EditReplaceBorder	MountVolume - mount a network disk or folder.
Edit EditReplaceTabs ReplaceFrame	Outline, Outline(), Shadow, Shadow()- relate to Outline or Shadow formatting.
FileCreator$(), FileType$(), SetFileCreatorAndType - Get/set Macintosh file signatures/filetypes.	ShowClipboard

(3) Platform-Specific Arguments

A number of statements corresponding to dialog boxes have arguments which aren't supported on all platforms.

ConvertObject - .IconFilename and .DisplayIcon are ignored on the Macintosh.	FormatBordersAndShading - .FineShading is ignored in Windows.
DlgVisible - LastIdentifier is valid only on the Mac and on Windows NT.	InsertObject - .IconFilename and DisplayIcon ignored on Macintosh.
EditFindFont, EditReplaceFont - .Outline and .Shadow valid only on Macintosh.	ToolsOptionsCompatibility - some arguments valid only for Mac and NT.
FileFind - .ShowFolders valid only on Macintosh.	ToolsOptionsPrint - .Draft and .Background arguments ignored on Macintosh.
FilePrint - .OutputPrinter valid only on Macintosh.	

(4) Cross-Platform Differences in Effect

Some statements and functions behave differently according to platform.

Beep	InsertSound
DDEExecute	Kill
DigSetPicture	MailMerge* - ODBC not supported on the Mac.
FileFind [.ShowFolders]	MsgBox, MsgBox()
FileNameInfo$()	Name
FileOpen	Picture
Files$()	ScreenUpdating
GetAttr(), SetAttr	ShadingPattern,ShadingPattern()
GetSystemInfo, GetSystemInfo$()	Shell
InputBox$()	ToolsCustomizeKeyboard

APPENDIX F: Vendor information

Datawatch Corporation (for Virex)

234 Ballardvale Street
Wilmington MA 01887
+1 508 988 9700
fax: +1 508 988 0105
http://www.datawatch.com/
ftp://gateway.datawatch.com/pub/

McAfee (for VirusScan).

McAfee Associates
2710 Walsh Ave
Santa Clara, CA 95051
95054-3107 USA
Voice (408) 988-3832
FAX (408) 970-9727
BBS (408) 988-4004
CompuServe ID: 76702,1714 or GO MCAFEE
mcafee@netcom.com
ftp://ftp.mcafee.com/pub/antivirus/
http://www.mcafee.com/

Dr. Solomon's Software Ltd. (for Dr. Solomon's AntiVirus ToolKit)

Alton House
Gatehouse Way
Aylesbury
Buckinghamshire HP19 3XU
United Kingdom
UK Support: support@uk.drsolomon.com
US Support: support@us.drsolomon.com
UK Tel: +44 (0)1296 318700
USA Tel: +1 617-273-7400
CompuServe: GO DRSOLOMON
Web: http://www.drsolomon.com
FTP: ftp://ftp.drsolomon.com

Symantec Corporation (for SAM)

10201 Torre Avenue
Cupertino CA 95014
+1 408 725 2762
Fax: +1 408 253 4992
US Support: 541-465-8420
AOL: SYMANTEC
European Support: 31-71-353-111
Australian Support: 61-2-879-6577
http://www.symantec.com/
ftp://ftp.symantec.com

Symantec also market the Norton Utilities for Macintosh: a useful diagnostic/repair resource, if carefully handled.

Sophos plc (for Intercheck)

The Pentagon
Abingdon
Oxon
England OX14 3YP
http://www.sophos.com/

Microsoft (for the SCANPROT protection tool)

http://www.microsoft.com/msoffice/
(look for mvtool1222.hqx)
MSN: GO MACROVIRUSTOOL
AOL: the Word forum
CompuServe: the Word forum
Microsoft Product Support Services
206-462-9673 (WinWord)
206-635-7200 (Word Mac)
email: wordinfo@microsoft.com

Padgett Peterson's MacroList can be downloaded at:

http://www.freivald.org/~padgett/index.html (under Anti-Virus Hobby)

MacroList is freeware, but the author requests that individuals intending to download it read the TRIALS link.

Disinfectant is available from:

ftp://ftp.acns.nwu.edu/pub/disinfectant
CompuServe
GEnie
America Online
Calvacom
Delphi
BIX
sumex-aim.stanford.edu
rascal.ics.utexas.edu
comp.binaries.mac

Since Gatekeeper is no longer supported, I can't guarantee that documented sources for the latest (last) version will still apply when you read this. However, you may still find it at (among other sites):

ftp://microlib.cc.utexas.edu/microlib/mac/virus/
ftp://ftp.utexas.edu/pub/mac/virus/gatekeeper-13.hqx

Chris Johnson, its author, has a page on Gatekeeper at:

http://gargravarr.cc.utexas.edu/gatekeeper/gatekeeper.html

Vaccine is available from:

ftp://ftp.visi.com/users/hyperact/Vaccine3.2.hqx
http://www.hyperactivesw.com/

HyperActive Software offer a virus detection service for previously unknown HyperCard infectors.

http://www.hyperactivesw.com/

CyberSoft market a number of Unix security tools. VFind is a Unix-hosted scanner which detects PC, Macintosh, and Amiga malware on server.

CyberSoft, Inc.
1508 Butler Pike
Conshohoken, Pennsylvania 19428-1322 USA
Voice: +1 (610) 825-4748
Fax +1 (610) 825-6785
Info@cyber.com
http://www.cyber.com

A number of other vendors have Unix scanners, but to the best of my knowledge, these detect only PC viruses and the very few known Unix viruses. However, a Unix scanner which detects macro viruses as well as PC-specific viruses is still a potentially useful resource in a predominantly Macintosh environment: even more so if there are Macintoshes running PC emulation.

Vendors with Unix-hosted scanners include McAfee and Dr. Solomon's (contact details as above).

APPENDIX G: Macintosh Troubleshooting

<Adapted from the “Viruses and the Macintosh” FAQ [Harley2]>
Native Mac viruses are actually rather rarely found in the wild. Previously unknown Mac viruses are even rarer, so if a competent known-virus scanner detects no viruses on a problematical system, it’s worth trying some of the techniques and sources listed below rather than assuming an unknown Macintosh-specific virus. [Harley2]
However, Word files which appear on the desktop as a template icon rather than a document icon are very likely to indicate a macro virus problem.

- Visual phenomena such as unusual animated cursors, audio effects and text messages are unlikely to be virus-related unless they correspond specifically to known virus symptoms. It’s always worth checking extensions and control panels for a pointer to such problems. Screensavers seem to be a particular source of confusion, but there are many other possibilities such as joke programs and system bugs like the “Bluets and granola Bars” message in System 7.6.

- Rebuilding the desktop is by no means a cure-all, but rarely does any harm. It may be worth disabling extensions when you do this, especially if the operation doesn't seem to be completed successfully.
- To disable extensions, restart the machine with the shift key held down until you see an Extensions Off message. If you're rebuilding the desktop, release the shift key and hold down Command (the key with the Apple outline icon) & Options (alt) until requested to confirm that you want to rebuild.
- Disabling extensions is also a good starting point for tracking down an extensions conflict. If booting without extensions appears to bypass the problem, try removing extensions with Extensions Manager (System 7.5) - remove one at a time, and replace it before removing the next one and booting with that one removed. Remember that if removing one stops the problem, it's still worth putting it back and trying all the others to see if you can find one it's conflicting with. Extensions Manager also lets you disable control panels. If you don't have Extensions Manager, try Now Utilities or Conflict Catcher.
- Parameter RAM (PRAM) contains system information, notably the settings for a number of system control panels. 'Zapping' PRAM returns possibly corrupt PRAM data to default values. A likely symptom of corrupted PRAM is a problem with date and time (but could be a symptom of a corrupted system file). With system 7, hold down Command-Option-P-R at bootup until the Mac beeps and restarts. You may have restore changes to some control panels before your system works properly. If the reset values aren't retained, the battery may need replacing.

APPENDIX H: Further information

Most of the resources quoted here are on-line. While pointers given below are as accurate (E&OE) as possible, permanence is not the way of computer networks and internetworks. Much of the material below is reproduced from the "Viruses and the Macintosh FAQ" (URL below), and pointers therein will be kept as up-to-date as possible for the foreseeable future.

Macintosh Viruses

http://www.symantec.com/
http://www.datawatch.com/
http://www.mcafee.com/

McAfee Mac Virus Encyclopaedia (includes macro viruses)
ftp://ftp.mcafee.com/pub/antivirus/mac/vencyc.hqx

http://ciac.llnl.gov/ciac/CIACVirusDatabase.html
ftp://ftp.ucs.ubc.ca/pub/mac/info-mac/vir
http://hyperarchive.lcs.mit.edu/HyperArchive/Abstracts/vir/HyperArchive.html
http://wwwhost.ots.utexas.edu/mac/pub-mac-virus.html
http://lipsmac.acs.unt.edu/Virus/macvirinf.html

Kevin Harris's Virus Reference (HyperCard stack):
http://www.sperspect.com/sperspect/
ftp://ftp.el-grove.k12.il.us/pub/sperspect/
eWorld: shortcut "Perspective"
AOL: HyperCard, Operating Systems, and User Group Connection areas.

"Viruses and the Macintosh" FAQ
http://webworlds.co.uk/dharley/
http://www.totalweb.co.uk/dharley/

http://www.macvirus.com/ (Opens officially Summer 1997.)

HyperCard issues

"HyperProgramming - Building Interactive Programs with HyperCard": George Coulouris & Harold Thimbleby (Addison-Wesley).

"The Complete HyperCard Handbook": Danny Goodman (Bantam).

"HyperCard Virus Compendium": http://www.hyperactivesw.com/

"Hypertalk" (Programmer's Quick Reference Series): Lon Poole (Microsoft Press).

Vaccine: ftp://ftp.visi.com/users/hyperact/Vaccine3.2hqx
(includes some information on HyperCard viruses)

Macros/Macro-viruses

Word for Macintosh FAQ:
ftp://mirrors.aol.com/pub/info-mac/info/sft/word-mac-faq-04.hqx

Richard Martin's macro-virus FAQ [not updated recently]:
ftp.gate.net/pub/users/ris1/word.faq
http://learn.senecac.on.ca/~jeashe/hsdemonz.htm
mailto://Bd326@TorFree.Net Subject: PLEASE SEND FAQ

Macro Virus List from Virus Test Center, Hamburg:
ftp://ftp.informatik.uni-hamburg.de/pub/virus/macro/macrolst.*

Just about all on-line virus information databases include information on macro viruses. Some worth trying include:

http://www.vdsarg.com/
http://www.drsolomon.com/
http://www.datafellows.com/
http://www.commandcom.com/
http://www.avp.ch/avpve/
http://www.sophos.com/

Microsoft Word Developer's Kit (Microsoft Press)

Vesselin Bontchev: "Possible Macrovirus Attacks and how to Prevent Them" (Proceedings of the Sixth International Virus Bulletin Conference).

General Virus Information

http://www.symantec.com/
http://www.mcafee.com/
http://www.drsolomon.com/
http://www.sevenlocks.com

Virus Newsgroups:
comp.virus/virus-l
alt.comp.virus

VIRUS-L FAQ:
ftp://cert.org/pub/virus-l/FAQ.virus-l
ftp://ftp.datafellows.com/pub/misc/anti-vir/vlfaq200.zip
ftp://cs.ucr.edu/pub/virus-l/
ftp://ftp.cs.ucr.edu/pub/virus-l)
Regularly auto-posted to comp.virus.

alt.comp.virus FAQ
http://webworlds.co.uk/dharley/
http://www.totalweb.co.uk/dharley/
Regularly auto-posted to alt.comp.virus and comp.virus.

AntiVirus Catalog/CARObase: information on Macintosh file/system viruses (among others)
ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/catalog/
ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/carobase/
ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/viruses/
ftp://ftp.uu.net/pub/security/virus/
ftp://sunsite.unc.edu/pub/docs/security/hamburg-mirror/virus/

The specialist magazine “Virus Bulletin” has not dealt specifically with Macintosh virus issues for a while, but deals frequently with macro viruses, hoaxes and other issues which are not necessarily PC-specific. (http://www.virusbtn.com/) The same applies to other security publications such as “Secure Computing” and “Computers & Security”. N.B. while articles in “Computers & Security” are generally sound and carefully refereed, the abstracts of recent articles, while no doubt accurate as regards the original content, are not necessarily pointers to quality information.

There are a number of papers by Peter Radatti at http://www.cyber.com/ relating to indirect virus transmission. These generally consider the problem in Unix-centric terms, but the principles are often applicable to other server and client platforms.

General Macintosh Information

Sensei Consulting Macintosh WAIS Archives:
http://wais.sensei.com.au/searchform.html
"Inside the Apple Macintosh" - Peter Norton & Jim Heid (Brady)
"Inside Macintosh" (Addison Wesley).
Essential reading for Mac programmers. Downloadable in Acrobat format from <http://devworld.apple.com/>
MacFixIt "Troubleshooting for the Macintosh"
http://www.macfixit.com
MacInTouch home page (info and services)
http://www.macintouch.com
"Sad Macs, Bombs and other Disasters" (3rd Edition).
Ted Landau (Addison Wesley)
MacWEEK magazine
http://www.macweek.com/
Macworld magazine
http://www.macworld.com/
MacUser magazine
http://www.macuser.com/
TidBITS
http://www.tidbits.com/

ftp://sumex-aim.stanford.edu/info-mac/
ftp://ftp.ucs.ubc.ca/pub/mac/info-mac/
ftp://wuarchive.wustl.edu/mirrors/info-mac/
ftp://ftp.apple.com/

List of anonymous ftp sites with Macintosh files:
ftp://sumex-aim.stanford.edu/info-mac/info/mac-ftp-list*.txt

comp.sys.mac.apps
comp.sys.mac.comm
comp.sys.mac.misc
comp.sys.mac.system

FAQs for comp.sys.mac.misc, comp.sys.mac.system
http://www.macfaq.com/miscfaq.html
http://www.macfaq.com/systemfaq.html

FAQ for comp.sys.mac.comm
http://www.cs.ruu.nl/wais/html/na-bng/comp.sys.mac.comm.html

Appendix I: Glossary

- 68k: commonly-used abbreviation used with reference to Motorola's 680x0 series CPU, used on all Apple Macintoshes prior to the introduction of the PowerPC RISC chip used in PowerMacs.

- Change Detectors/Checksummers/Integrity Checkers - programs that keep a database of the characteristics of all executable files on an individual system and check for changes which might signify an attack by an unknown virus.
- Data fork/resource fork: Macintosh files may (but don't necessarily) consist of two physical components, a data fork and a resource fork. The data fork generally contains data, strangely enough. The resource fork of an application file contains resources such as icons, program code, menus etc.
- Dropper: a program that installs a virus or Trojan, often covertly.
- E&OE: Errors and Omissions Excepted.
- File signature: file identification data which affects how the Macintosh operating system deals with the file. A four-letter creator code identifies the application which created or 'owns' the file: a Word document, for instance, has the creator code MSWD. A four-letter type code identifies the file type. A system extension, for example, has the type code INIT.
- Freeware: software for which no charge is made, though it may or may not be in the Public Domain. Some freeware authors retain copyright without making any charge.
- Generic - catch-all name for antivirus software that doesn't know about individual viruses, but attempts to detect viruses by detecting virus-like code, behaviour, or changes in files containing executable code.
- Heuristic scanners - scanners that inspect executable files for code using operations that might denote an unknown virus.
- Malware: malicious software including viruses and Trojans.
- Monitor/Behaviour Blocker - a memory-resident program that monitors programs while they are running for behaviour which might denote a virus.
- On-access scanner: whereas an on-demand scanner runs only when required and scans all disks and files specified, an on-access scanner runs in the background all the time and scans files as they are accessed.
- On-demand scanner) - a program that looks for known viruses (or unknown viruses, using heuristic algorithms ("educated guesses").
- Postcardware: Gatekeeper is a famous example of a program for which no charge is made, but if the user finds it useful, s/he is expected to send the author a postcard of their hometown.
- Shareware: software which is made freely available, but not actually free. If the user finds it useful, s/he is expected to pay for registration.
- System extensions & control panels: system extensions add functionality to the basic system. Control panels are for adjusting system settings. Both can load software into memory at startup, and may comprise the memory-resident scanning component of anti-virus software.
- Trojan (Trojan Horse) - a program intended to perform some covert and usually malicious act that the victim did not expect or want. It's usual to distinguish between Trojans and viruses according to whether the program can self-replicate.
- VBA: Visual Basic for Applications. A dialect of BASIC which is intended to become the common macro language for Microsoft Office applications.
- Virus - a program (a block of executable code) that attaches itself to, overwrites or otherwise replaces another program in order to reproduce itself, usually without the know ledge of the computer user.
- VxD scanner: a Windows driver which executes on-access scanning.