

Malware Myths and Misinformation Part 2

David Harley 2003-05-28

Malware Myths and Misinformation, Part Two: Attachments, AV Software and Firewalls

by David Harley

last updated May 28, 2003

This article is the second of a three-part series looking at some of the myths and misconceptions that undermine anti-virus protection. In the [first part](#) of this series, we considered a class of myths and misconceptions that we summarized as the school of "I'm safe because I don't do Microsoft." In this installment, we will consider a class based on perceived immunity through mail hygiene. It is, perhaps, unfair to regard all of these as myths and misconceptions. They might, however, be regarded as problematic because they tend to lay so much stress on security that they impair an organization's ability to carry out its day-to-day business. The first one, though, is decidedly misleading.

I'm safe from viruses because I have hygienic email habits?

...I don't use Outlook/Outlook Express

Well, OK. This is still a little Microsoft-phobic, but it has some reasonably sound reasoning behind it. These utilities have exhibited an unfortunate ability to run executable code when they shouldn't. Several vulnerabilities have been reported associated with the unchecked use of embedded scripts. And yes, it's true that email viruses often look for addresses to mail themselves out to in Outlook's address books and inbox. However, they don't have to run in Outlook or OE. If you're tricked into opening an attachment, you don't have to execute it from your mail client. *Any* client that allows you to save an attachment will do, even if it won't let you execute it within the client. And the vulnerabilities referred to have been patched and otherwise addressed in subsequent versions. Indeed, it has to be said that whatever you read on mailing lists and in the computing press, Microsoft make a valiant attempt at keeping a massive code-base as secure as possible in as timely a manner as possible. At least, within their own view of security, which may not always be quite the same as yours or mine.

But doesn't avoiding Outlook stop you broadcasting viruses to your address book? Not necessarily. A number of Microsoft products make use of the Windows Address Book. There is

no magic shield that stops a virus writer parsing and plundering another email client's address book. Many viruses look for target addresses from other places on the system, such as Web files. We already know that using one of the "safer" email clients doesn't stop you executing an attached file. Would you really not care whether there was an active virus with an unknown payload lurking on your system, simply because you were sure it couldn't be broadcasting itself from your account?

...I don't open attachments

This is certainly a way of avoiding most email-borne threats. Using mail software that doesn't offer any means of automatically opening and executing attachments gives almost complete protection.

(Hey, I'm an information security professional, and therefore a professional paranoid sceptic: I'm not going to say 100%! Can you guarantee that your mailer is totally immune to buffer overflows, or doesn't have some hitherto unsuspected weakness, or that you won't be conned by a neat piece of social engineering into breaking your own rule? However, I will say 100% if you don't have access to email at all?)

Frankly, though, this isn't an option for most of us, certainly not for most of those who work directly with computers and the Internet for a living. Much (most?) electronic information is nowadays conveyed in application-specific formats not amenable to transfer as 7-bit text. If you can get away with it, good luck to you. See you in the 21st century.

...I don't open dangerous attachments

Sounds good. But how do you define dangerous? You can do what many corporate administrators do, and block/reject all the types of attachment filename extension you've ever heard of as being potentially dangerous - essentially, all the file-types that signify an executable file (or a file that can contain executable code such as macros). Or, more realistically, block all the attachments with filename extensions (like .PIF, .BAT, .LNK and so on) that are almost never legitimately and with full knowledge exchanged between computer users. However, a good number of executables are freely and legitimately exchanged. Self-extracting compressed or encrypted files are usually .EXEs, and there are sometimes legitimate reasons for exchanging screensavers within a corporate environment. (OK, very occasionally, with an extreme stretch of the imagination.)

Most systems administrators manage to persuade their management boards or user communities that the inconvenience of not using these file types is outweighed by the security gain. Sadly though, the security gain is less than desirable, given the number of strategies available for circumventing blocking techniques to pass legitimate *or* malicious executable files through (encryption, changing the filename, or compression, for instance). But what about Office documents? As we've already seen, macro viruses have not disappeared, though they don't have the same impact they had a few years ago. Yet blocking Office documents, though sometimes advocated, isn't very attractive in today's Office-dominated business environment. The business case for increasing security by blocking documents that can carry macros is outranked by the need to exchange data in feature-rich file formats. Not that you have to roll over and die in the face of the (nowadays much reduced) macro threat. Any combination of the following strategies seriously reduces the risk, and to use all of them comes close to eliminating it:

- Single or multi-layered known-virus detection, properly installed and kept up-to-date;
- Avoid unnecessary use of macros;
- Use macro-hostile file formats for data exchange (.RTF, .CSV); and,
- Configure Office installations to avoid running macros by default when documents are opened.

...I don't open attachments from people I don't know

Sadly, this particular approach has never offered much protection. It's based on the assumption that all malicious programs are directly distributed by evil virus writerz and hackerz, with cutlasses in their teeth. This misconception that has been encouraged by a number of poorly researched books and other publications, but it isn't based on real understanding of how malicious software works or spreads. How a malicious program gets "into the wild" is a fascinating and somewhat complex area. And indeed, the authors of email worms and viruses may, in fact, "seed" them by mailing them directly to individuals or (probably more effectively) mailing lists. However, once malware is out in the wild, it's more likely to be received from someone you know or have at least at some point communicated with, directly or indirectly, than from a complete stranger with malicious intentions.

...I don't read mail from people I don't know

This has some validity as a somewhat extreme security measure, in principle. Some people do

literally discard all mail from people not on their "whitelist" of people from whom they are prepared to accept mail. This has two main drawbacks. The most obvious is that they almost never receive mail from anyone who isn't on their whitelist (which in these days of escalating spam and email worms has its attractions), except by establishing convoluted mechanisms by which "legitimate" mail users can apply to be included on the whitelist. Of course, unless their filtering is exceptionally efficient, they may also find that mail with forged headers (which can include both spam and viral messages) will evade it. The second main drawback is that, as already discussed, a high proportion of infected mail is received from someone known to the recipient, so no automatic immunity is conferred. Indeed, the recipient may be more vulnerable than average because of a false sense of security.

I'm safe from viruses because I know enough about security to be sure that...

This group of misconceptions is almost harder to eradicate, because it's rooted in some awareness of reasonably sound security principles.

...I have anti-Trojan software

Trojans have tended to be a slightly overrated class of threat, historically. Their impact can be devastating, but it is generally fairly short-term, since they don't replicate. However, they are often found keeping the company of full-blown viruses and worms. Indeed, email worms that use social engineering to trick the recipient into opening them are sometimes considered, to all intents and purposes, to be Trojans. (Yes, this does mean that I've just contradicted the assertion that Trojans don't replicate. Welcome to anti-virus research.)

After all, a classically viable definition of a Trojan horse is a program that claims to do something desirable (and may even do it), but instead (or also) does something the victim did not expect and certainly would not want. (But why get into arguments about what the differences are between worms, viruses and Trojans when we could get into really interesting stuff like what the plural of virus should be?) As for the efficacy of anti-Trojan software, all that needs to be said is:

- Viruses may be considered a sort of Trojan;
- Worms may be considered a sort of Trojan;
- Worms, viruses and Trojans may hang out together sometimes; and,

- Anti-virus software often detects Trojans, though it would be a brave anti-virus vendor who would claim to detect all Trojans - or all viruses, come to that.

But anti-Trojan software generally detects Trojans rather than viruses. There is an argument for using both (and some of the other security measures we touch on here in addition), but if you insist only using one, better make it anti-virus!

...I have a personal firewall

Let's be clear: there *is* a place on the present-day desktop for the personal firewall, but there is also a tendency to overestimate the functionality and degree of protection such software offers. This is to some extent based on popular misunderstanding of what firewalls are and how they work, and we'll look a little more closely at that in the next section. To address the argument that personal firewalls confer immunity to viruses, it is probably enough to say that:

- Personal firewalls are considerably more limited in functionality than corporate firewall servers, and even those aren't particularly good at virus management (though some may work well with supplementary virus control programs).
- They are not, in general, designed to detect specific malicious programs. They are less likely to detect malware that isn't active, and once malware is on the system, its activation may not be detectable by "generic" means.
- They do a good job of blocking certain groups of activity associated with malicious software, such as the use of particular ports for malign purposes, without necessarily being aware of the exact program which is responsible for those activities. This means, effectively, that some symptoms may be suppressed, but the illness remains present, either latent or active.
- The fact that personal firewalls are not focused on specific malware may make them more vulnerable to malware aware of specific personal firewalls. It is quite commonplace nowadays for email worms to attempt to delete files and shut down processes associated with personal firewalls as well as with anti-virus software.

...I'm behind a corporate firewall

So what *is* a firewall? To understand the limitations of a "real" firewall, we have to understand not only what it does, but also a little about how it works.

Essentially, a firewall is a router. It doesn't really see network traffic as whole files, emails or

other forms of electronic broadcast, but as a long procession of packets containing the information required to forward data. The addition of firewall filtering capabilities means that certain ports, services, domains and so forth, can be blocked. These capabilities can be augmented by enhancements such as application proxy servers and plug-ins for management of viruses, spam and so on. Indeed, it's often assumed that such enhancements are routinely implemented, but this is not the case. Many firewall administrators find the cost of such measures is not only financial: the gain in security is offset by the extreme impact on processing time. Implementers of managed firewall services are often particularly reluctant to add measures that will compromise their ability to meet stringent Service Level Agreements on throughput rate. (Not all firewalls integrate easily with such tools in any case.) It is sometimes said that functionality always takes priority over security. Another way of looking at it is that of the three classical "cornerstones" of security ? integrity, confidentiality and availability ? availability is often the most urgent!

...We have an intrusion detection system

And very useful they are, too. But some security gurus who should have known better have caused some confusion. There are similarities between the signature-based IDS applications and anti-virus methodology, though the technical resemblance isn't that great. Anomaly detection systems may pick up malware-related symptoms at an early stage, and sometimes deal with certain kinds of network worm, for example, more successfully even multi-layered anti-virus scanners. But they don't do the same job. Known-virus scanners are optimised for scanning a very specific subset of malicious code in very specific contexts. IDS tends to be more heuristic in nature. They are complementary, not exclusive.

Next Time...

In the final part of this series, we'll consider a series of myths concerning the bad faith and technical incompetence of anti-virus and other security vendors, and the nobility, technical superiority and all-round invincibility of authors of malware.

David Harley lives in the UK with his partner, daughter, 3 cats and a number of guitars. He works for the UK's National Health Service, specialising in threat assessment and malware/email abuse management. He is an active member of [AVIEN](#) and several industry forums. His books include "Viruses Revealed".

Relevant Links

Malware Myths and Misinformation, Part One

David Harley, SecurityFocus

[Privacy Statement](#)

Copyright 2006, SecurityFocus