TUTORIAL 2

Safe Hex in the 21st Century: Part 1

Martin Overton
ChekWARE, UK

Remember the Chinese curse – 'May you live in interesting times'? Well, we are living in very interesting (and busy) times – consider yourself cursed!

A Safe Hex on You

With the boundaries between data and executables becoming ever more blurred, and the Internet and email becoming an integral (and indispensable) part of everyday life, many are feeling that what was once considered safe to use is becoming increasingly fraught with unexpected dangers. Are the following fears real or rubbish?

- Emails that trigger payloads on preview or opening, people clicking on email attachments that promise love, free sex site codes, or whatever.
- The threat from a boot sector virus still haunting us almost 10 years after its creation.
- *Excel* spreadsheets fast becoming one of the main infection vectors within many companies.
- Drawing files that contain macro viruses.

It is no wonder many believe the hoax virus messages that circulate in many companies. Fact and fiction are getting mighty close! How can the users (and even the security officers) ever expect to learn about the growing number of threats in terms that they can understand?

This article aims to offer advice and suggest tools or methodologies that can be used in organisations that are battling with the scenarios outlined above.

Let's Start at the Very Beginning

Some people argue that technology is to blame, or that *Microsoft* is responsible for putting functionality before security. However, you must remember that it is ultimately (in most cases) a human being pressing the buttons, and this is the root of the problem.

I think we can all agree that *Microsoft* and other software vendors are partially responsible, but remember that we (the consumers) have helped make them what they are by our constant 'need' for improved usability and integration when it comes to technology. In effect, we have created a monster, and now we have to pay the price – bring out your Internet and computer virgins and offer them up to appease the beast!

Many people think that user education is the key to dealing with malware issues. At VB'96 in Brighton, I came to the following sad conclusion: 'You may think that trying to educate your staff about the risk of viruses is like trying to nail jelly to a wall, and about as rewarding, and in most cases you are right. Your non-IT staff will generally be either blasé, paranoid or simply ignorant about viruses. They simply see it as not being their problem.'

Last year's appearance of Melissa and last month's fiasco with 'The Love Bug' aka VBS/LoveLetter.A (and its many offspring), have forced me finally to acknowledge that anti-virus software is at least partially responsible for the 'it-can't-happen-to-me' attitude of users!

Why? Ask a user why they will read almost any email sent to them (no matter how suspect or frivolous it appears), and in many cases even blindly run attachments, with hardly a second thought. Are they really so insecure, desperate for attention, or careless? No! They think they are safe *because they run anti-virus software* – 'the panacea for all that ails!' How else can you explain why normally intelligent and otherwise savvy people risk opening the electronic version of a mail bomb?

I know some of you will disagree with my conclusion that user AV education is generally a waste of time. However, in my defence I would like to enter the following. Your PC Support and other technical staff *are* worth educating as they tend to understand the technology better and actually might be interested in what you have to offer.

Some of them may want to penetrate the mystic aura surrounding viruses and AV, and may believe you when you tell them it does not require them to chant strange incantations over the entrails of viral samples [*or frogs! Ed.*], and attend secret meetings at nodal points during the year. (Well, at least they might believe the incantations part!) If nurtured correctly this interest may actually blossom and you could end up with another valuable member of your security or anti-virus function or team. If nothing else, it might help to spread the burden and the skills.

Well, enough ranting (for now). Let us have a look at the problems and some suggestions on how they might be reduced or neutralised.

Know thine Enemy

Continuing on the education theme, obviously most of you (who are still awake) reading this are very interested in keeping up to date with new threats, viral techniques, and protection methodologies. Well, let us look at the best ways to 'know thine enemy', because if you understand your enemy, you understand what drives them and more importantly, their Achilles heel.

Most, if not all, anti-virus (and other security) companies offer 'Email Alert Lists'. These can be an excellent way to keep up to date. Try to pick a good cross-section of mailing lists, from those that post 'at the drop of a hat' to the other end of the spectrum, those (few) that post about 'in-the-wild viruses' when they are actually in the wild.

What a Load of Bulletins

Another useful tool for the security managers and their staff are the numerous security bulletins, including the rather busy 'Microsoft Security Bulletin' pages on their Web site. These can warn of new security loopholes and if they are acted on can help to thwart new malware attacks that use the published exploits. A good example is the extremely widespread Kak worm and the earlier BubbleBoy virus, which uses the 'eyedog' exploit. *Microsoft* (for all its failings) posted a fix for this on 31 August 1999, yet today the Kak worm is still the most frequent virus I see trapped by many email scanners. Why?

Do very few IT or security staff monitor this useful site and the many others which feature known exploits for products used in numerous companies, or is it just a case of 'it-can't-happen-here' syndrome? I know some of you monitor these sites and some of you act on the information that you find. What are the rest of you doing – fighting and cleaning up the malware that uses these exploits?

Did you Myth Me?

How can virus hoaxes, other hoaxes, myths, chain letters, etc be defused successfully? This is a difficult, but not insurmountable problem. I do not know about you but I used to spend more time debunking and dealing with hoaxes than dealing with real viruses. Please note the past tense, as this is not the case now. How this state of affairs was turned around is revealed below.

Here are some guidelines as well as some useful links. As mentioned before, information and a good security policy can go a long way to managing this problem. However, information and a few savvy members of staff are probably the most important factors in the never-ending battle against the hoax email. The problem has got somewhat worse over the last eighteen months or so, as we have started to see malware that does what we always told our users could not be done.

Simply reading an email is no longer perfectly safe. HTML mail, along with Visual Basic Scripting (also known as *Windows Scripting Host*), JavaScript, and *LotusScript*, and possibly others, have shown that we must be careful. What we say is safe today may well be dangerous tomorrow. So, now let us get on to some possible useful methodologies for you to consider.

Set up a good hoax policy and get it endorsed by your board. Once approved, send it to all your staff, either electronically or as an addendum to their terms and conditions of employment. (You might want to check out the legal implications of this!) An example might look like this: *'If information about a new virus threat is received this must be passed to Security [or a named contact] for verification. They will then decide if a general alert should be posted, which will include a confirmation or denial of the reported threat and any further steps that are required. Only Security [or named contact] is authorised to distribute virus alerts. Failure to follow this policy may result in disciplinary action.'*

If you run an Intranet, put a link from your home page to a good virus hoax site, e.g. http://www.kumite.com/myths, or to just about any AV company on the Web. Or, I give you my permission to re-post the hoax and myths information pages from the *ChekWARE* site on your own Intranet. You can find this at http://arachnophiliac.com/hoax/.

The above simple recommendations have cut the re-posting of hoaxes by around 80% in one company. It has also significantly reduced the number of calls that the company's help desk receives about hoaxes and other related electronic ephemera.

Still Putting the Boot In

Why is the Form virus still a problem in many companies and how can the threat from it finally be eradicated? This venerable boot sector virus is still a regular in the *Virus Bulletin* Prevalence Table and has hardly been out of it since Form was released. Why are we *still* seeing infections from this non-Internet, non-File, sneaker-net-dependent virus? A simple and cost-free change on any PC built in the last five or six (or maybe more) years can render Form incapable of infecting.

To take the sting out of Form and other boot (DOS Boot Record) and partition (Master Boot Record) sector-infecting viruses, simply change your CMOS boot-up sequence from the usual default of A: drive then C: drive to C: drive then A: drive. This means that if you accidentally have a floppy infected with a DBR virus like Form or an MBR virus like Parity_Boot, you could boot by default from drive C instead, thus robbing the boot sector virus of its ability to infect another system. If you do occasionally need to boot from a floppy disk, then the CMOS can be quickly switched back to the default A: drive then C: drive (but do not forget to switch it back again). This simple trick will defeat all pure boot and partition-infecting viruses, but not multi-partite samples in their boot sector-infecting state.

In Summary

Hopefully this has given you something to think about. I welcome feedback and comments, both via *Virus Bulletin* or private email (martin@arachnophiliac.com). The next part of this article will deal with what can be done to minimise or neutralise the risks from the greatest threats to many companies – emails, attachments and the scourge of Macros, VBA, *WSH*, etc.