TUTORIAL

Safe Hex in the 21st Century: Part 2

Martin Overton
ChekWARE, UK

How do you get a 100% secure and virus-free system and keep it that way? Unplug the computer, take it outside, place it on the ground and drive over it a number of times with a large steamroller. Once its nice and flat, liberally splash with petrol and flambé for a number of hours. Once extinguished, place the contents into a safe deposit box. *Voilà*, a secure and virus-free system that will stay that way. In other words, there is no such thing as a fully secure system that is usable (in the normal sense) that cannot be infected/affected by malware. Got it? Good! Please pass the message on.

If we don't break out of the 'virus-scanner-is-king' mind set that many have fallen into then we will be doomed to keep repeating the same mistakes forever. Virus scanners have their place *but* (and it's a big one) virus scanners are no longer enough. We (the consumers) have taken the evolutionary short-cut to virus protection when what we really should have done was take the longer, twisting path towards proper security and system integrity which would have minimised many of the current threats.

There follow some suggestions for dealing with the current malware problems:

- Do not open attachments coming from unknown sources. Delete them.
- Before opening a file apparently coming from someone you know, if possible ask the sender if they actually meant to send it. If not, delete it and tell the sender that they may have a virus. If yes, scan it before opening it.
- Disable script (and HTML) support for mail and news.
- Disable Java and JavaScript in your browser and enable them only when required.
- Uninstall the *Windows Scripting Host* (*WSH*) if you don't need it.
- Set the boot sequence to C, A in the BIOS.
- Change *Explorer* to show all file extensions.
- Make backups of your data regularly.
- Encourage the use of safe file formats for data exchange (such as PDF).
- Encourage the use of URLs in emails rather than attachments.
- Set up a good solid 'Acceptable Use Policy' for email and Web use, and get your staff to sign it.
- Teach 'Safe Hex' to your support and other technical staff. For the non-technical staff, make sure that any policies are written in a suitable style so that there is no room for misinterpretation.

Should companies re-evaluate how email attachments are dealt with and what types are acceptable and safe? Yes! To paraphrase that great philosopher Forrest Gump, 'Email is like a box of chocolates, you never know what you're gonna get.' If you and your users have not already developed a healthily paranoid attitude (assume that all attachments/emails are suspect and may contain a virus), then you/they will continue to be victims. What can you do to minimise these risks?

To Scan or Not to Scan?

Scanning may no longer be enough, but it *is* still needed so let's look at the best way of using this tool.

I am somewhat uneasy about using ISP scanning within a corporate scenario for the following reasons:

1. Privacy – if they are scanning your email they may also be reading it, especially if it is flagged as suspicious.
2. Encryption – this will walk right through ISP scanning (unscanned).
3. Liability – if the ISP informs a sender and the intended recipient that he has sent a virus, could this cause loss of confidence? What if it is a false positive or worse a false negative and the recipient gets infected, who's to blame, where's the legal recourse?
4. Over-reliance – I can hear board managers all over the world stating that they no longer need to protect their workstations, file/print servers or scan email ever again as their ISP will do it for them and think of all the money they'll save for their company.

Gateway (SMTP) scanning is a definite must as it can make the biggest impact on virus penetration within your company. There are a few caveats. It is best to use a different virus-scanning vendor from the one you use at the desktop or file/print servers. Encrypt/decrypt at the gateway so that viruses cannot sneak through, or block/quarantine all encrypted email, password-protected ZIPs (and other compression formats).

Lotus Notes or *Exchange* scanning is another very important scanning point as these servers can act as 'viral foxholes' allowing malware a safe haven from where they can strike out again. Once more, I would strongly suggest using a different scanning engine from those on the desktop and file/print servers. You may even want to use a different scanning engine from the one on your SMTP email gateway. In security, diversity of products/technologies is in itself a protection mechanism and should be encouraged at every (practical) opportunity.

Content scanning (and lexical analysis) is fast becoming an extremely powerful function for limiting and immediately blocking new threats, be they infected attachments, documents, embedded scripts, as well as pornography and other unacceptable content. Why? Simply because you decide what is acceptable and allowed and are always in control. If you want to you can block all scripting languages' executable attachments, *Microsoft Office* files, etc.

VBA and Macros

VBA is the successor to the separate (but similar) *Office* product-specific Macro languages. Is *Office* now a mini-operating system itself, or is it just that *Office's* tentacles infiltrate the underlying 'real' OS? I don't know and I really don't care, except where this impinges on my (and others) security and productivity. Let's call it a mini-operating system and look at the problems this brings.

Macros are the biggest threat to most companies, as documents (and other *Office* files) are passed around with wild abandon. This is compounded by the number of people using *Word* as their default email editor. What can you do to minimise this threat?

Stop using DOCs. Use pure Rich Text Format for your Word documents. Some macro viruses intercept File SaveAs RTF and save a file with a .RTF extension which actually contains a DOC format file! So it needs to be true Rich Text Format. Also RTF files can contain OLE components that in themselves could be a threat. Use Adobe Acrobat (PDF format) as this is currently not known to be capable of carrying a virus. Tell people that you would rather they sent you CSV files than XLS. Finally, use the in-built protection in *Word*, *Excel* and other *Office* products.

I predicted (at VB'99) that *Visio* would soon be targeted by virus writers as it uses VBA, so it was no great surprise when it came to pass just weeks before *Microsoft* took ownership of the company. What can you do? Add *Visio* files to the list of formats that you might consider filtering at the SMTP gateway and ensure that your virus scanners can detect viruses in *Visio* files.

Getting Your Backup

Regular backups of data on your system are still very important. You can replace program files easily enough from master disks, but corporate data is worth a lot more to your company and is hard to replace if damaged or destroyed. In many firms data is the very lifeblood of the company. So, don't bleed to death, back up that data before it's damaged or destroyed by a virus or other malware.

Make a WSH

A new class of virus now uses what is effectively Visual Basic Scripting language. This scripting language can be used to perform any task and use any application it can access. This has already been used by a number of new VBS/*WSH*-based script viruses/worms/Trojans.

Allowing this support to be turned off (as required) can effectively render this new threat dead in the water. The latest virus to take advantage of *Windows Scripting Host* was the recent and infamous ILOVEYOU virus aka VBS/LoveLetter.A aka LoveBug. It is highly advisable to turn off *Windows Scripting Host* if you do not need it. At the very least block all scripting languages coming in to your company in email.

How do you tell if you have got *WSH* installed? The simplest way is to search the hard disk for WSCRIPT.EXE. If it exists (usually in the *Windows* SYSTEM or SYSTEM32 directories) then it almost certainly is installed.

Windows Scripting Host is installed by default in *Windows 98*, *NT 2000* and on any version of *Windows 95* and *NT* when *Internet Explorer 5.x* is installed. Be aware though that it can also be installed as a separate entity on systems that do not have *IE 5.x* (such as *Windows 95* or *NT 4*). While I'm covering scripting, I would strongly suggest that if you are using *Outlook* or *Outlook Express* you ensure that your standard build has HTML format for email and news disabled, as this in itself will help to slow down (or stop) some malware that uses embedded scripts.

Trust me, I'm … Signed

This is a technology that has been touted as the solution to many of the recent problems with malware. This has its place as part of a multi-layered approach to malware protection, but it is not a total solution as it is fatally flawed in one respect, you have to trust the signer absolutely! Does the following sound familiar? Software vendors assure you that their code/control/application is safe until a bug is exploited by a piece of malware and you have to download the patch. This is what happened with the Kak worm. The counsel for the prosecution rests its case.

Recipe for Success

Use scanners wisely and update them regularly. Deploy a diversity of products at different points. Encourage the use of safe alternatives. Instil a healthy paranoia into your staff and back it up with solid policies. Train your technical and support staff. If you do not use scripting languages in your company, disable them before someone disables/damages your systems. Set up an AV section on your Intranet and point your staff to that. Monitor vendor and security sites/mailing lists and ensure you patch your systems and applications when new vulnerabilities are found. Change the boot sequence on your systems, and finally, make regular backups of at least your data. Safe computing!