INSIGHT

KAOS on the Superhighway?

Virus Bulletin readers will have noticed the short 'Stop Press' notice regarding the KAOS4 virus which was included in last month's edition. One month on, it now appears that the spread of the virus has been checked by a prompt response from anti-virus software manufacturers and members of the *Internet* user community. However, there is no doubt that, were it not for the ineptitude of the virus writer, a great deal more damage could have occurred.

With companies climbing over each other in a scramble for increased connectivity, the incident provides an ideal opportunity to review some of the risks associated with *Internet* access.

Navigating the Internet?

One of the biggest misconceptions about the *Internet* is that it is actually run or controlled by a single body. However, given that there is a blurred definition of what the *Internet* actually is, this may require some further explanation.

Simply put, the *Internet* is a communications network. This may sound rather unimpressive, but estimates of the numbers of computers attached start at a highly conservative million, with more computers being added at a rate of hundreds or thousands a day.

The *Internet* consists of a number of sub-networks. Often these sub-networks are publicly funded, and have owners who recognise that adding connections to other networks enhances their functionality. Thus, as its name implies, the *Internet* is simply a network of networks.

One of the most visible uses of the *Internet* is for sending and receiving Email. Although only text can be transmitted via Email, it is possible to encode binary files as text, allowing executables to be transferred quickly and cheaply worldwide. This provides a way for potentially infected files to enter a system. Unfortunately, such ways are legion.

Newsgroups

In the case of the KAOS4 virus, an infected file encoded as text was posted to the *Internet* newsgroup alt.binaries.pictures.erotica. That file was downloaded by a number of users, and once on their own machines, decoded, and reconstituted into an executable file.

The *Internet* newsgroups (known as *Netnews* or *Usenet*) are, just like the *Internet*, not run by any individual body. Rather, they have evolved out of a messaging system originally designed to deal with a handful of computers linked together in a *UUCP* (*Unix to Unix Communications Protocol*) network. However, as time (and technology) marched on, this system became unacceptable, and the present system was created.

It was later decided to divide the newsgroups into sub-groups. The most common of these are:

comp	discussion of computers
news	discussion of news groups and news
sci	scientific discussion
rec	recreational discussion (e.g. pyrotechnics, chess, cycling)
talk	issue-related discussion (e.g. politics)
misc	miscellaneous topics.

This event created tension within the *Usenet* community, which in turn led to the birth of the 'alt' newsgroups (with alt standing for alternative). Even more so than the main-stream newsgroups, the alt hierarchy is completely anarchic, and contains a wide variety of topics, with groups ranging from alt.hackers to alt.swedishchef.bork.bork.bork.

Also included in the alt newsgroups is the 'erotic' picture group alt.binaries.pictures.erotica (abpe). Such newsgroups contain many megabytes of scanned GIF or JPEG files of dubious origin, as well as animation programs or picture viewers. As an interesting aside, the newsgroup abpe is responsible for a significant chunk of the network traffic which makes up *Usenet*.

Regulatory Bodies

The above discussion may make *Usenet* sound chaotic, but that would not be an unfair description. It is possible to post to *Usenet* anonymously, and (especially in the alt newsgroup hierarchy) there is no filtering or checking of the contents of messages. Thus, downloading any executable file from *Usenet* is a game of chance: although it is likely that the file is exactly what it claims to be, there is a remote possibility that it will contain a Trojan horse or a virus.

One might think that a virus author would be insane to post a new virus, as this would reveal his identity. Unfortunately, this is not the case, as *Usenet* posts can be easily faked and forged. This means that the virus author could disguise a new virus as a utility, and anonymously post the item to the newsgroup. Fortunately, this is very rare.

The user who posted the file infected with KAOS4, *Sexotica*, claims that he did not know that it was infected. This is the case for most of the viruses which have cropped up on the *Internet* so far.

As postings to *Usenet* cannot be trusted, it is worth considering other sources of information on the *Internet*. One of the most popular methods is *gopher* - this is a program which allows inexperienced users to find information or files on a particular topic by searching a simple text-based menu system. Such systems generally allow the user to hop across the globe from site to site, homing in on the area of interest.

Another source of information is ftp sites: large software collections containing many Gigabytes of files, usually operated and maintained by universities or colleges. Unlike postings to *Usenet*, uploaded files are generally placed in a secure area, so that the system manager can check their contents and suitability before allowing other users to access them. Ftp sites can be accessed quickly and easily, and generally do not require the use of a password for access. This provides a certain level of anonymity.

"one of the first rules for avoiding virus infection via the Internet is exactly the same as for general PC use: do not use software of unknown origins"

Although ftp sites are an excellent source of information, and often represent well-maintained and catalogued software collections, the same problem of accountability still exists. The ftp site will not always have been sent the file by the author of the package (and even if the site believes that it has been, this is not always easy to prove), so it is still possible that a file could be Trojanised in some way.

Other forms of file distribution on the *Internet* are similarly unreliable. Personal Email is trivial to forge (ask any first-year computer scientist for a demonstration), and can be done automatically by several programs or *Unix* scripts.

Fighting Back

The preceding information brings little cheer to the average computer user. However, all is not doom and gloom, as many individuals and companies have begun to search for ways in which to make use of the many benefits of *Internet* access more secure.

One of the first rules for avoiding virus infection via the *Internet* is exactly the same as for general PC use: do not use software of unknown origins. In the case of the *Internet*, this will include ftp sites, and more importantly, software encoded as ASCII posted to newsgroups. Obviously such paranoia can only be taken so far. However, for a large network, it seems prudent to follow the oft-stated rule of obtaining software only from trusted sources. The ftp sites maintained by a number of anti-virus software manufacturers are obviously somewhat more reliable, and can be used (with the simple caveat that one can never be completely certain when communicating over the *Internet*).

In order to offer some sort of message authentication system, several encryption programs have been developed. The most popular, *PGP* (*Pretty Good Privacy*) uses a Public/Private key system, so that without a user's private key, it is impossible to fake messages which appear to be from him. Additionally, a message can be sent in such a way that it can only be decrypted by the recipient. Solutions to the problem of mail and file tampering by programs like *PGP* are becoming more common, as users begin to see first hand evidence of forged 'joke' postings.

Apart from encryption systems, most commercial networks connected to the *Internet* have an *Internet Firewall* set up. Although this is principally designed to deter potential hackers, the Firewall can also be configured to prevent users accessing various services and features provided by the *Internet*. The most draconian solution would be to provide access only to Email. Unfortunately even this is not completely effective: several newsgroups also exist in list form, and there are numerous ftp mail servers which can send files to users via Email.

Conclusions

From a purely virus-related point of view, the *Internet* provides nothing but trouble. However, these problems are not *Internet*-specific: they apply equally to any route by which files can enter a company.

Files which are posted on the *Internet* are not automatically downloaded by unsuspecting users: the user has to access the file, decode it, and run it, for there to be any danger to the host system. Therefore enabling Email is not a risk *per se*, as the user has to take quite deliberate action in order to spread a virus. As GUIs to the *Internet* grow in popularity, this may not always be the case - soon, files may be automatically extracted and restored to their original form.

Of all the ways in which a virus can enter a company, Email and *Internet* access probably rank as two of the lower threats. However, on a global scale it does make a very tempting target, as it allows a reasonably anonymous way to distribute virus code. Therefore, it is important that the usual precautions for dealing with programs are followed.

When made *Internet*-specific, these are:

- Do not use software of doubtful origin (e.g. executable files from public ftp archives and *Usenet* postings).
- Scan all incoming software. Note that most scanners cannot search a binary file encoded as a text file; therefore the file must be decoded first. Some *Internet Firewalls* can be configured to do this automatically.
- When transferring executable code or confidential information, always use a message authentication or encryption system.

These rules, if followed as part of a general policy, will provide an excellent preventative against viruses via Email or the *Internet*. Ignore them at your peril!