OPINION 2

Memetic Mass Mailers: Time to Classify Hoaxes as Malware?

Andrew Lee
Team Anti-Virus, UK

This article is intended to provoke discussion, rather than to provide hard and fast answers; it arises after observing the statistical tracking of hoaxes (in a limited and fairly unscientific manner) over the last two years. From the trends shown by this tracking one can extrapolate that an effective hoax (which I shall define in a moment) can be as damaging as a mass-mailed fast-burning virus – and sometimes more so.

The Effective Hoax

A 'successful' or 'effective' hoax is one that works on three levels:

1. It is sufficiently attractive to draw recipients' attention to it (the subject line 'New Virus Alert' usually achieves this).
2. It spreads rapidly and widely enough, with or without modifications, to catch recipients unawares – and does so before it can be debunked.
3. It is believable enough for the recipient to deliver the payload – whether that be simply propagating the hoax further, or carrying out given instructions before spreading the message.

There are some striking similarities here with actual malware. Some of the more successful worms and viruses of recent years, such as Melissa, Loveletter, Anna (I apologise for using the populist forms of these names, but it makes for easier reading – and gives the pedants something to get their teeth into), have followed the same rules.

1. They were sufficiently attractive for people to pay attention to them: Melissa offered porn site passwords, Loveletter offered, well, love, and Anna offered pictures of a nubile sports personality. This is getting the foot in the door, and is essential for achieving a successful spread. (Let's leave the true worms out of this for a while.)
2. They spread rapidly and widely enough that many people 'contracted' them before their AV software was updated, and before alerts had been issued.
3. They were believable enough to make the recipient deliver the payload. I chose these examples specifically (rather than, for example, Klez or Badtrans.b) as they demonstrate user involvement. No software exploit was involved in these viruses – in each case, it was the recipient who delivered the payload by double-clicking on the file.

Usually, of course, a hoax requires the user to carry out its replication as well as its payload, but just as the aforementioned trio of malware delivered mass mailing as part of their payload, the successful hoax has the same result. Whether it is malware, which does the work itself, or a hoax which gets the user to do the work on its behalf is really an irrelevance, since the end result is the same.

Let's examine a couple of successful hoaxes. The technique used by each is substantially similar, with the execution being the only real difference. Rather than looking at the hoaxes from the point of view of finding out why they are hoaxes, I shall look at why they work.

Elf Bowling

First, let's look at the Elf-bowl hoax and why it was successful. (The full text of this hoax can be found at http://www.umich.edu/~vbuster/hoaxes/elfbowl.html.)

First, the hoax plays on our fears – we have all heard or read endless warnings about accepting unsolicited email attachments. Most users know they shouldn't open them, but do so anyway. In the case of Elfbowl.exe, they received it from a friend, who was sent it by a friend, who got it from who knows where, all of which adds up to a hefty uncertainty factor.

Secondly, the hoax was timely. The message appeared only a few days after the original file had been circulated, which meant that the game was still fresh in people's minds. This raised the profile of the doubt in the recipient's mind. Had the hoax message been sent a few months later, it is debatable whether anyone would have remembered the original file, and the hoax would not have had the same impact.

Finally, the message was not confirmable as a hoax for some time – no one (including the AV companies) knew for certain whether the file had been infected, or Trojanised. There was no way of knowing whether such a modified variant was out there, all that could be determined was that the *original* Elfbowl.exe was not malicious. Confusion is a wonderful vector for rumour and insinuation.

A Picnic of Teddy Bears

Now let's look at another successful and more recent hoax, the JDBGMGR.EXE hoax. (See http://www.umich.edu/~vbusters/hoaxes/jdbgmgr.html for the full details of this hoax.)

There is some discussion about whether this really is a hoax, or whether it is just well meaning misinformation – let's put that aside for one moment, and concentrate on the reasons for its success. I find it particularly surprising that this hoax was such a success, as it is almost identical to the SULFNBK.EXE hoax (with the same caveat on the use of the word hoax), which appeared almost a year earlier. So why did this one work?

First, there is a heightened awareness of malware in the media at the moment. Nimda, CodeRed, SirCam, Badtrans.b and Klez have each had many media column inches devoted to their 'Internet-destroying' properties. This heightened awareness is usually fairly undirected – in other words, there is a lot of fear, uncertainty and doubt, and no greater level of knowledge. Arguably, this leaves the less clued user open to exploitation by new hoaxes that play on these shifting fears.

Secondly, the message is cleverly worded. Well, I mean 'clever' in that it exploits natural human naïveté. Many people still believe things that are written down – newspapers being a classic example – and apply little actual thought beyond the face value of information. So, when something reads, 'This is not a hoax, I found it on my machine', combined with 'I think I may have sent you a virus', it creates a powerful rationale which the reader accepts unswervingly.

Finally, this hoax will almost always work. The fact that the file named by the hoax exists on 99 per cent of normal *Windows* installations will almost certainly fool some people. Add to that the file's unusual icon (a teddy bear of all things), and you have the makings of a great hoax.

Destructive Payloads

The aim of much malware is to deliver a payload (of course, many viruses simply replicate and have no payload). Payloads range from nuisance value, such as intermittent beeping or displaying a graphic, through mass-mailing, right up to destroying data on the infected machine.

The traditional payload of hoaxes is time wasting and increasing user anxiety about the virus threat. Replication is achieved by suckering the punter into sending it on – effectively, a simple user-assisted replication.

Hoaxes such as SULFNBK.EXE and JDBGMGR.EXE add a level of destructiveness to the payload. In these cases it is the deletion of a single system file, and the files in question are fairly irrelevant – at worst their deletion causes an inconvenience – but it would be naïve to assume that this will always be the case. What if the recipient were instructed to delete a folder, or a more important file or set of files? The possibilities are endless, and because there is little technological detection available for such hoaxes (though some products do claim to detect them), the chances are high that such hoaxes will replicate successfully and deliver their payload.

It has been argued (convincingly) that the SULFNBK.EXE and JDBGMGR.EXE hoaxes are both instances of 'well meaning misinformation'. This may be the case – certainly SULFNBK.EXE was a very commonly mailed file when W32/Magistr.a was at its peak, and there is some justification for believing that someone put together the instructions for its removal in good faith. However, this seems less likely with the JDBGMGR.EXE hoax – mainly because it appeared almost exactly one year after its earlier variant when W32/Magistr.a has long been known about. Perhaps we shall never know, but it may be wise to consider this a glimpse of a possible future trend.

The fact is that there will always be malicious (or just silly) pranksters who take great delight in knowing that their creations have caused widespread damage and/or panic. In fact, I would go so far as to say that, as more virus writers are dragged through the courts, hoaxing may become a safer way of spreading an idea.

Recently, some AV vendors have begun to provide up-to-the minute hoax metrics and alerts, in much the same way as they have traditionally done for viruses. This in itself is a double-edged sword. There has always been a certain 'respect' to be gained amongst writers for getting a creation onto the WildList or a vendor site, and this may be the same for hoaxters. But, of course, such sites and lists are also valuable (and eventually essential) tools for overworked system administrators.

Whatever the state of play at the moment, there is no doubt that the potential for damage becomes greater with each new hoax. When I first connected to the Internet (or at least its rudimentary beginnings) I could count on one hand the number of friends who had email addresses. Now it seems that everyone and their dog has (sometimes several) email addresses. This has proved rich pickings for the fast-burners like Melissa, Loveletter and Anna, but without doubt the hoaxters have had their fun too. Hoaxes account for close to 95 per cent of the 'alerts' that I see every week, and I know I am not alone.

There is a huge cost loss associated with hoaxes, and it is way beyond that which most viruses cause. There are psychological costs too. The worry caused by deletion of files that should not have been deleted. The humiliation of realising that one has been duped. The fear, uncertainty and doubt that is caused by thinking that there is an 'Undetectable Virus' on one's computer – and anyone who underestimates the power of that fear has never worked on an AV support desk.

I predict (or at least have a fairly large prescient twitch) that hoaxes will evolve in complexity over the next few years, until they are, effectively, indistinguishable from malware. Techniques for detecting hoaxes have always been based on pattern matching and intuition – the basic model for heuristic scanners. This has become increasingly difficult, and our 'scanning engine' (the brain) has had to be fed all sorts of new information to keep up. Goodbye Good Times.