WHATEVER HAPPENED TO THE UNLIKELY LADS? A HOAXING METAMORPHOSIS

David Harley, Randy Abrams
ESET Research, 610 West Ash Street, Suite 1900, San Diego, CA 92101, USA

Email {dharley, rabrams}@eset.com

ABSTRACT

Once upon a time the most problematic chain emails were virus hoaxes, as exemplified by the Good Times hoax: however, perhaps the last really innovative malware-related hoaxes were the SULFNBK and JDBGMGR hoaxes of the early noughties. Since then, most anti-malware companies have virtually lost interest in memetic malware as its links with real, programmatic malware have declined. But does this mean the problem has gone away? Unfortunately, it hasn't. Somewhere in the no-man's land between malware and spam, the chain letter continues to create a range of problems for system administrators and IT support departments, from choked mail servers to choked support lines. However, it has also created both emotional and practical problems for the recipients as hoaxers have learned to apply increased pressure by hanging hoaxes and semi-hoaxes onto real-life tragedies and disasters such as the 2004 tsunami and missing children including Madeleine McCann.

This paper traces the changes in the Meme Machine [1] from the 1990s to 2009, from the Jeffrey Mogul metavirus [2] to the tsunami-related hoaxes that intermittently crippled public sector communication channels in the UK in the present decade, and considers some of the most recent examples, looking at underlying mechanisms as well as topical content. What has changed? What measures should we be taking to steer our users and customers away from the submerged 9/10 of this under-publicized iceberg? And if the security industry doesn't own the problem, who does?

INTRODUCTION

Was there a time when there were no Internet-borne hoaxes? Possibly: the earliest denizens of the primeval Internet were often fairly sober citizens, and certainly we aren't aware of a hoax or chain letter that predates Jeffrey Mogul's metavirus [2]. Before we review the history of hoaxes and chain mails, we should, however, start with a few definitions. Caveat: even folklorists with no particular interest in computer security use a wide variety of definitions, and security researchers with no particular interest in folklore may be quite arbitrary in their usage – for example, we frequently see the term 'hoax' applied not only to material such as chain letters, but to unequivocally fraudulent material such as phishing and 419 emails.

HOAXING TAXONOMY

'Electronic ephemera' is a term used by Martin Overton [3] to describe a wide range of transient, electronically transmitted nuisances including hoaxes, urban legends, scams, spoofs, chain mail and so on. While we find this classification useful and the label attractive, we are inclined to extend it to include spam in general. While this term covers a wide range of email abuses, it almost invariably includes an element of deception that makes it hard to separate (most) spam from scams.

Viruses Revealed [4] cited the *Webster's Dictionary* definition of a chain letter as one '... directing the recipient to send out multiple copies so that its circulation increases in a geometric progression as long as the instructions are carried out', which still works for us, though we'll use the term here largely in relation to email and other messaging media rather than traditional snail mail. More informally, any mail that asks you to forward its contents to other people without discrimination is, arguably, a chain letter, whoever or wherever it comes from, and should be regarded with scepticism.

The same work cited the *Oxford Reference Dictionary* definition [5] of 'hoax' as 'to deceive, especially by way of a joke… a humorous or mischievous deception,' but made the point that 'Other definitions incorporate the concepts of "mockery or mischief" and "deliberate trickery intended to gain an advantage… fraud, fraudulence, dupery, put-on".' These are important considerations in understanding both the mechanisms and the motivation behind hoaxes.

Phishing, 419/advance fee fraud (AFF) mails and other blatantly fraudulent material are considered here because their similarities and dissimilarities to hoaxes are informative [4], but the motivation behind hoaxes and closely related material may be significantly more complex than out-and-out criminal deception. Most significantly, the hoaxer rarely profits financially from his or her deception. We therefore prefer to avoid categorizing them as hoaxes, though some do, defensibly in terms of some dictionary definitions. Hoaxes and scams both include an element of intended deception, and may even look very similar, but the scam motivation is largely financial, whereas the hoaxer is either bolstering his own self esteem by proving how stupid others are (just like 'traditional' virus writers), purely malicious/sociopathic/mischief-inspired, or watching the fire engines go by for the sheer excitement. The psychology of the scammer relies on the depersonalization of the target/mark (scammers don't use the word 'victim' much, preferring emotionally neutral terms such as 'mark' or even the pejorative 'big fool', 'mugu' or 'mgbada' of the 419 scammers) [6].

An urban legend usually has more of a narrative element than a hoax, and is not necessarily untrue, though it often is. According to the alt.folklore.urban FAQ, they 'often have a basis in fact, but it's their life after-the-fact ... that gives them particular interest' [7].

While we don't intend to wander too far down the fascinating byways of memetics on this occasion, we cannot altogether ignore the influence of the study of memes on researcher thinking on hoaxes. The meme was described by Dawkins [8] as 'a unit of cultural transmission, or a unit of imitation'. Early work in this field was also influenced by his article 'Viruses of the Mind' [9], which, although primarily anti-religious in purpose, made extensive references to computer viruses and psychological (or memetic!) mechanisms that apply just as well to the dissemination of hoaxes (including 'semi-hoaxes'): '…minds are friendly environments to parasitic, self-replicating ideas or information… [the victim] finds himself impelled by some deep, inner conviction that something is true… [victims] may feel that the less evidence there is, the more virtuous the belief…'.

A particularly pervasive meme is the joke email: spoof alerts such as the Robert Morris III spoof of the Modem virus hoax (see below) [4] fit into this category, but so do many other humorous emails, from collections of jokes around a general topic to jokes specific to the Internet and to messaging media, including ASCII art, animated .GIFs and so on. However, these do not normally contain an explicit exhortation to pass them on: they take on a life of their own according to their perceived entertainment value.

CHAIN LETTER STRUCTURE

The now-defunct hoaxbusters page at hoaxbusters.ciac.org used to define chain letters as having a tripartite structure (hook, threat, request). It's not always straightforward to separate these elements, but they do seem to be common to most chain letters [10, 11].

The hook catches the reader's interest, for instance by an appeal to greed ('Bill Gates is sharing his fortune' [12]), fear of the subversion or breakdown of technology, or sympathy (e.g. cancer or tsunami victim hoaxes and semi-hoaxes).

The threat is there to keep the chain going. Traditional chain letters threaten bad luck or worse if the ripples don't continue to spread. Virus hoaxes threaten the destruction of systems or data. The recipient will miss the opportunity to make money, or earn the gratitude and respect of others. The threat may be to others: a lost child won't be found, or people will die unnecessarily of a heart attack or terrorist action.

The request constitutes the replicative mechanism by persuading the recipient to forward it to friends and acquaintances. Chain letters are often considered to be literally viral: 'memetic viruses', or 'viruses of the mind'. Where computer viruses use infective code and biological viruses use genomic replication (biological code), chain letters rely on memetic transfer, persuading the recipient to pass the message on to others.

Many hoaxes ask you to 'help' others by disseminating 'information'. Some hoaxes ask you to generate money for yourself, for medical research, or for charity by forwarding identical messages. However, the common aim in each case is not to inform, to improve society, or even to sell a product: it is (purely or primarily) self-replicative.

We find it useful to distinguish between out-and-out hoaxes with no significant element of truth, and hoaxes that do contain some nugget of truth, but have been distorted so as to be seriously misleading. These are sometimes referred to as semi-hoaxes [12]: Overton [11] refers to 'Hybrid Virus Hoaxes… that contain some genuine information amongst the usual dire warnings.'

A BRIEF HISTORY OF TIME WASTERS

The Jeffrey Mogul metavirus was clearly meant to make a serious point in a humorous way – well, it still makes us smile, if a little wryly – but it was the hoaxers who had the last laugh. In Mogul's own words, 'The beauty of this "meta-virus" is that it took me about two minutes to make it really scary and I didn't even have to write any code.' [2] Perhaps part of the significance of this proto-hoax in the context of this paper lies in a juxtaposition usually forgotten. Mogul's metavirus first appeared in Risks Digest next to a message by Martin Minow, both messages being in response to the MacMag virus that was making serious security ripples at that time (February 1988):

> 'There was a report on the computer virus scare on Sunday's (Feb 7, 88) All Things Considered (public radio news program). I took the following notes: don't expect them to be accurate.
>
> Professor Fred Cohen was interviewed. He claims that the virus will spread in 1/2 hour through a computer timesharing system and that it "is a mathematical fact" that you cannot protect against the virus if you allow sharing, transmission, and general access.'

While the Mogul metavirus set the scene for the out-and-out virus hoax of a type that appeared 'in the wild' (in a strictly non-technical sense) [13] very shortly after with the Mike Rochenle hoax [14], the doom-laden but possibly out-of-context quote from Dr Cohen – I suspect that he may have been talking about 'the virus' in a generic sense rather than the MacMag HyperCard virus – provided extra ingredients that we see now in all sorts of hoaxes, not just metaviruses. That is, an appeal to authority (Fred Cohen literally 'wrote the book' on replicative malware and anti-malware, and many of our assumptions about the field today are still ultimately derived from his work [15]) and 'mathematical fact', and the idea of the unstoppable, undetectable threat.

Of course, we don't suggest for a moment that Mogul or Minow (let alone Cohen) had the slightest intention of launching a whole class of memetic threat: only that some mischievous or malicious individuals were quick to perceive opportunities for misuse.

The (presumably pseudonymous) Mike Rochenle [4, 14] took the hoax to the next level, introducing technobabble like 'The virus distributes itself on the modem sub-carrier present in all 2400 baud and up modems. The sub-carrier is used for ROM and register debugging purposes only, and otherwise serves no other purpose. The virus sets a bit pattern in one of the internal modem registers, but it seemed to screw up the other registers on my USR.' Robert Morris III was inspired to offer another spoof [4]:

```
Warning: There's a new virus on the loose that's
worse than anything I've seen before! It gets in
through the power line, riding on the powerline 60
Hz subcarrier. It works by changing the serial port
pinouts, and by reversing the direction one's disks
spin. Over 300,000 systems have been hit by it here
in Murphy, West Dakota alone! And that's just in the
last 12 minutes.
```

However, such spoofs appeal mostly to the initiated who are capable of seeing the improbability of the 'technical' content, a fact that became manifestly obvious with the meteoric rise of the Good Times hoax [16], probably the most successful virus hoax of the 1990s, if not of all time.

```
If the program is not stopped, the computer's
processor will be placed in an nth-complexity
infinite binary loop - which can severely damage the
processor if left running that way too long.
```

It seems that hoaxers are quick to see the joke, but even quicker to see the possibilities for exploitation: aided, perhaps, by a conviction that gullibility is so much part of the human psychology, that there is no such thing as a claim so improbable that no-one will believe it.

Most of the hoaxes seen in the late 1990s were derived from the Good Times hoax. Generally they say something like

'Don't open mail with [a particular subject]'. 'LIFE IS BEAUTIFUL', 'IT TAKES GUTS TO SAY JESUS', and 'WIN A HOLIDAY' are examples of subject lines supposedly associated with 'lethal' email viruses. It is often claimed that if you read the malicious email, the virus will eat your hard drive (or at least reformat it) and send sensitive data to some remote hacker, that there is no known way of detecting it, and the message appeals to the reader to forward the mail (of course) to everyone they care about. Reinforcer text is often seen along the lines of 'It is better to receive this message multiple times than to receive the virus and open it.' [18] While such hoaxes rarely excite nowadays, they are alive and well and appear from time to time on a blog near you.

Virus hoaxes reached some sort of climax with the SULFNBK and JDBGMGR 'viruses' in the early part of the present decade.

```
The objective of this e-mail is to warn all Hotmail
users about a new virus that is spreading by MSN
Messenger. The name of this virus is jdbgmgr.exe
and it is sent automatically by the Messenger and
by the address book too. The virus is not detected
by McAfee or Norton and it stays quiet for 14 days
before damaging the system.
```

However, hoax viruses had already changed in one important respect. Almost all metaviruses have, at some point, had material introduced that is almost certainly deliberately deceptive. Many, especially the earlier ones, were pure fantasy, and are intended only to frighten you into forwarding the message. SULFNBK and JDBGMGR, however, include two realistic elements.

1. The files really exist, and the instructions given for removing them will work. The deceptive element lies in the presentation of a (normally) innocent file as malware.
2. There is likely to be a shard of truth behind that characterization: these hoaxes were at their peak at a time when W32/Magistr was infecting files in the system folder, including JDBGMGR [19], so that a normally innocent file *may*, in fact, be malicious.

It wasn't the first, though. For example, the Wobbler hoax is likely to have its roots in a joke program [4] at one time detected as a trojan, though that detection was later suppressed [20]. It has to be said, though, that there was a time when certain joke programs were routinely detected as trojans. The distinction between out-and-out malware and maliciously intended jokes that *don't* do any permanent damage but *are* intended to worry or upset the victim is, perhaps, pretty tenuous. False alerts such as the GHOSTS screensaver alert, based on a particular product's false positive, have had wide currency in the not-too-distant past, and scanners have not always clearly distinguished between real viruses, Trojan horses, and joke programs.

Sometimes we see alerts that are more or less accurate but so vague or outdated as to be unhelpful, or containing inaccuracies that lessen their helpfulness. Usually the impact of actual malware is dwarfed by the bandwidth occupied by panicking computer users mailing warnings to each other and to support teams. A more recent example of two and two being added together to make 666 is illustrated by the confluence of a *Symantec* unsigned patch being flagged as suspicious by *Symantec*'s own firewall, giving rise to a spate of conspiracy theories [21].

Examples of other alerts where a grain of truth has acquired a patina of mythology include the PKZ300 'Trojan Virus' and the 90# mobile phone 'scam' alert. There have indeed been trojanized versions of PKZip: however, the nuisance value of the PKZ300 alert and its variants far exceeded the very small risk posed by a trojan which hardly anyone ever saw. The 90# scam alert originated in a potential exploit which could have affected a limited range of switchboards, but was subsequently attributed, quite impossibly, with cellular networks and home phones. Local alerts are frequently based on misunderstandings and technical inexpertise, but sometimes acquire a life of their own and find their way out into the great wide world, perhaps because the original sender or an initial contact feels the need to alert people outside their immediate work environment, whether for purely altruistic reasons or for more complex reasons, such as a desire for approval.

In 1992, a confluence of mishaps led to the misidentification of a supposed new virus dubbed Alien 4 [22]. Misunderstanding of the nature of polymorphism (which at that time hardly existed in the computer virus field) led to the belief that these outbreaks represented mutations of the same 'unknown virus'. The individual who originally warned the world of this 'virus' courageously issued a second bulletin when he realized that he'd overreacted: sadly, such courage is rather rare. However, it's rarely useful to forward a virus-related alert indiscriminately, even if it's reasonably accurate. In an age of server-side polymorphism and creative social engineering, it isn't often productive to point out the existence of specific malware: you might just as well say 'keep your anti-virus software up to date', which is good advice, but doesn't bear undue repetition. (Nor is it the cure for all ills, but that would be another paper.)

CONVERGENCE

At the beginning of this century, one of the authors found himself writing 'A recent and disturbing trend is the dissemination of warnings regarding real viruses, often quite old ones such as PrettyPark. Sometimes these are more or less accurate but so vague as to be unhelpful. Sometimes the information contains inaccuracies that lessen their helpfulness. Sometimes the impact of the virus itself is dwarfed by the bandwidth occupied by panicking computer users mailing warnings to each other, creating extra work for system administrators and others who have to respond to every "Is this really true?" enquiry.' [22] However, worse was to come. It's as though dedicated hoaxers have discovered the common 419 technique of a real but irrelevant fact/site/article used for spurious validation of the big lie that is the heart of the scam.

THE GREED IMPERATIVE

While we've focused so far on security-related hoaxes, there was a dramatic increase in chain letters offering free Nikes, cell phones, or even money [12] to people who forwarded the mail. A common response to such claims is 'I'm not sure I believe this, but it must be worth a shot,' and perhaps forwarding one email doesn't seem a big deal to someone who doesn't think about the consequences of amplification across thousands of recipients.

URBAN LEGENDS MEET MALWARE HOAXES

In the 90s, when many hoaxes were metaviruses, nearly all vendors addressed the issue. Now, however, there are few

(new) metaviruses, so most vendors don't bother. Consequently, while there are excellent resources such as http://www.snopes.com for establishing the accuracy of chain letters, there is little prevalence data. However, *Sophos* still maintains a top ten list [23] of the most prevalent hoaxes: on 5 June 2009, this included the following list, of which no less than five are metaviruses (numbers 4, 5, 6, 7 and 10):

1 Hotmail hoax
2 MSN is closing down
3 Bonsai kitten
4 Olympic torch
5 A virtual card for you
6 Meninas da Playboy
7 Budweiser frogs screensaver
8 Bill Gates fortune
9 Justice for Jamie
10 JDBGMGR

In fact, most of these hoaxes originate in the last decade, or have a family resemblance to older hoaxes. However, the hoaxscape is not always so predictable in the 21st century.

In the early years of the present decade, one of the authors found himself carrying much of the responsibility for malware (real and memetic) carried by messaging services for a potential user population of over a million people. At first, most of the hoax traffic seen followed the familiar hoax patterns described above, including Good Times influenced virus hoaxes, the JDBGMGR and SULFNBK semi-hoaxes, chain letters offering rewards for the forwarding of email, and alerts about various scary and mostly mythological issues that didn't have a particular focus [24]. However, increased 'always-on' connectivity in combination with some very high-profile and emotionally charged media events (the 9/11 terrorist attacks, the 2004 tsunami that followed the Sumatra-Andaman earthquake) resulted in a huge spike of disaster-related electronic ephemera, including:

- Fake alerts of new or threatened 9/11 type incidents.
- Fake tsunami alerts (some may have had a direct criminal intent, providing an opportunity to loot evacuated areas).
- Fake or wrongly attributed photographs as attachments, allegedly of a mountain-sized tsunami hitting the shore (clearly not the shore in Phuket, by the way!), or of deepwater fish allegedly discovered on the shoreline after the tsunami receded.
- Fake charitable appeals, mostly taking the form of phishing and 419s. (There were also examples of appeals that on checking appeared to be genuine, despite a close resemblance to fraudulent messages.)

THE LOST BOYS (AND GIRLS)

A particularly galling set of chain mails can be characterized as tsunami semi-hoaxes: these related to incidents where European children appeared to be orphaned by the tsunami and in at least one case, the child was (at least temporarily) unable to identify next of kin. Appeals were issued for relatives to come forward, which actually happened very quickly in all cases known to me. However, variant appeals in the form of chain letters continued to hit in waves – no pun intended – long after the children concerned had been returned to their families. Attempts were made to control their impact by standard email filtering techniques; however, these were rendered less effective when the same material reappeared with altered graphic attachments for which filenames, file hashes and so on were continually changed. The subject fields and message content also changed significantly, reducing the effectiveness of text filtering techniques. Most significantly, some of the information that was originally present, such as contact information and other contextualization such as dating that would have made it easier to determine the validity of the request, quickly started to disappear. It's hard to escape the conclusion that contextual information may have been deliberately stripped from the messages in order to prolong the life of the chain letter artificially. As with some metaviruses, a possibly useful and legitimate alert evolved into a semi-hoax with virtually no real humanitarian utility surviving in the later versions [25].

More recently, kidnap victim semi-hoaxes have taken precedence in this sector of the hoaxscape:

```
A 3-year-old girl named Reachelle Marie Smith is
missing.

IF YOUR CHILD WAS MISSING WOULDN'T YOU PRAY THAT
EVERYONE PASSED THIS EMAIL ON?!!!

PLEASE DO THE RIGHT THING AND LOOK AND FORWARD.

A 3-year-old girl named Reachelle Marie Smith is
missing.

You never know where this e-mail could end up and
I'm not going to stop passing this one around if it
means a little girl can be found!!!

Please spread this picture far and wide….You just
never know, someone you know, might know her!

PLEASE, BEFORE YOU DELETE THIS, LOOK AT THE CHILD
AND THEN LOOK AGAIN.

IF YOU CAN, PLEASE SEND THIS TO EVERYONE IN YOUR
ADDRESS BOOK. IT TAKES ONLY 10 SECONDS AND COULD
HELP LOCATE HER.

THANK YOU!
```

This version came with an attached poster containing information about the suspected kidnapping, including a photograph and description of the suspected kidnapper and his van.

As with somewhat similar chain letters from 2009 referring to the missing Madeleine McCann it's hard to escape the emotional pull of this communication. However, Reachelle has been missing since mid-May 2006 and would now be six years old. It's likely that even if she's still alive and still recognizable from the photographs, her physical dimensions have changed dramatically, while her presumed kidnapper apparently committed suicide a few days after she went missing. This incident illustrates persistent problems with information disseminated by chain letter.

- Time and mutations introduced deliberately or inadvertently as the message spreads make even valid information less and less useful.
- Emotional blackmail, the universal buffer overflow, is a powerful replicator, using the threat 'if you don't forward this, you are or will be perceived as a third-rate human being.'

Virus hoaxes resemble fake emergency calls to fire services: perhaps in motivation (we don't often get the chance to dissect a hoaxer psychologically, due to the magically

anonymizing/pseudonymizing properties of the Internet), but certainly in that resources must be expended in responding to and (in-)validating each new alert. Another powerful motivation for intentional hoaxing where there is no obvious financial profit may include ego gratification and compensation for feelings of inferiority by finding someone they can dupe, thus enhancing self-image – 'me-smart-you-dumb'. Victims may amplify the effect, not only for purely altruistic reasons, but from a desire to attract attention as an aware and responsible individual.

ANTI-HOAX MEASURES

Here are a handful of examples of hoax heuristics that have been commonly cited over the years by commentators such as Padgett Peterson, Bruce Burrell, Martin Overton and others.

- Heavy use of capitalization and exclamation marks.
- Poor spelling and grammar in an 'official' advisory.
- Message presents as a press release, but no indication of source.
- Inappropriate terminology like 'Trojan Virus'.
- No expiry date or identifiable originator.
- No contact point for reporting.
- Recipient urged to forward message indiscriminately.
- Appeal to authority (relevant or otherwise) but no supporting linking or point of contact.
- Technobabble.
- Unrealistically catastrophic consequences.

Anti-chain-letter heuristics might include some of the following; the challenge, however, would be to differentiate a hoax in an age where most businesses encourage indiscriminate top quoting:

- Key phrases
- Nested quotes
- Multiple addresses
- Heavy 'sent-to' header residue in text body

Message validation and reputation filtering as we know them in anti-spam filtering don't work very well, because hoax attacks tend to hit critical mass when they arrive from 'trusted' sources: rather like 'real' replicative malware.

Policy is frequently recommended as an anti-hoax measure, and can be effective much of the time. Sometimes, though, it can be derailed by psychological factors. Emotional and cognitive dissonance where the drive to comply with policy is overridden by emotional imperatives, and may even be used to deflect pressure back up the chain of command. Far better, but far more difficult, is to teach scepticism and a degree of resistance to social engineering.

MEMETIC VERSUS GENETIC VERSUS PROGRAMMATIC CODE

The anti-malware industry is still largely focused on code analysis, not on social engineering. We do attempt to educate, but piecemeal. (Of course, if we seriously turned our attention to hoax detection, hoaxers might also organize and raise their game, as bot herders and other cybercriminals have.) We parse email message content, but primarily we're looking for specific code-related material like domain names and passwords associated with malicious websites or archive attachments.

Could we usefully match tokens found in well-known hoaxes? Content filtering on textual content has been used, but there are issues with newer transport media such as *PowerPoint* slides and PDFs.

Text is often fairly standard, but it's hard to apply 'exact' or 'near-exact' ID techniques with anything like the same accuracy that we can with binaries. Many hoaxes are even more stereotyped than traditional 419s and first-generation phishes in construction and language, so it's possible that Bayesian and Markov models (exploiting the probability that certain tokens will follow other tokens) could be used as bases for hoax filtering, as suggested by Overton [28].

However, motivation (malice/benevolence) is not generally programmatically determinable, as we've long known with reference to real trojan malware. Why would you forward a known hoax benevolently? Well, you might want to flag a hoax to your user population, certainly. Of course, there are several preferable solutions: primarily, refer to a web page rather than forward with an explanatory note. After all, if email was really suited to alert transmission, the hoax problem would never have been a major problem. Whether the problems with email lie in the medium itself or with human frailty is another question.

Nonetheless, successful automated detection of even some hoaxes and semi-hoaxes, while useful in its own right, would also fit nicely into a more proactive approach to scanning that took into account user behaviour as well as programmatic behaviour. That, however, is a topic that will be explored elsewhere [29].

EVERY PICTURE TELLS A STORY

Graphics, often PPTs and PDFs, are a common hoax medium (and malware carrier/facilitator). Graphics, it seems, are seen as somehow more trustable (not trustworthy!). The presence of an appropriate photograph has long been used by the occasional 419-er as circumstantial 'proof' (the camera never lies, apparently!). Graphics can also be used to obfuscate and/or conceal filterable text (we like to think of this as memetic steganography) from automated detection, a technique used from time to time to conceal stock fraud and other spam. Cute photos have greetings card appeal, even when they centre on grim message topics like a baby with a life-threatening disease. They 'personalize' a message, even when they're totally unrelated to the topic.

Identification of a graphic, slide deck or PDF attachment by hash is perfectly feasible in principle, of course: however, past experience suggests that determined hoaxers may introduce changes into the mix comparatively quickly and frequently, though it's unlikely that such responses would ever approach the efficiency of server-side polymorphism.

NON-AUTOMATED RESPONSE

Unfortunately, many of the heuristics previously described are far easier to implement in wetware (people) than software (never underestimate the power of education, properly resourced and applied [30]). The same applies to many of the following countermeasures.

Informational websites using an encyclopaedia-like database, for instance http://www.snopes.com, provide a useful manual corrective to common hoaxes, though creative hoaxers have actually managed to use snopes.com in particular to provide 'corroboration' of an unrelated hoax. Checking a suspected hoax can also be a challenge in terms of finding appropriate search terms.

Recursive remediation is a means of dealing with a received hoax by sending a response back down the list of recipient addresses, naming and shaming senders by implication. However, experience indicates that as more people learned about the hoax problem, sending a response all the way down the chain generated mail storms of debate and irritation at receiving the same counter-hoax messages time and time again. One variation that has been somewhat useful is to offer a 'verification service' down the chain (which can, of course, be expanded by publication through more conventional channels). This also has the advantage of acting as a honeypot for new hoaxes and variants [12].

CONCLUSION

Let us share with you an idea that came out of the semi-hoax deluge of 2004–2005, though it remains for the present a gleam in the originator's eye. A technique that might also help would be a site offering a service based on a repository of 'valid' chain letters with enough information on the facts behind the chain letter to counter the time-expiration problem. To be successful, such a site would not only allow but actively encourage prospective hoax victims to assess the validity of a chain letter. It would, however, also 'legitimize' chain letters that met so far undefined criteria for accuracy, which would be anathema to the 'Old Guard' of the Internet: consider, for instance, the following section from RFC1855 [31]:

- Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your local system administrator if your ever receive one.

It could, however, allow a degree of voluntary (self) regulation both at global and local level that is almost completely absent from chain letter dissemination at present. For example, it might be a requirement that legitimate chain letters carry standard subject lines and possibly other header fields, topic date-stamping, use a semi-standard format, and so on: they would also refer primarily to the repository website rather than to information carried within the message. While it's safe to assume that dedicated hoaxers would seek (and find) ways to subvert these approaches on occasion, we also believe that such an approach, in combination with appropriate policies and guidelines within organizations, could be combined with standard mail-filtering tools to make a significant impact on an ongoing problem.

REFERENCES

[1] Blackmore, S. The Meme Machine. Oxford University Press, 1999.

[2] Mogul, J. Virus paranoia: Re: RISKS 6.22/"Macintosh Virus Hits CompuServe" http://catless.ncl.ac.uk/Risks/6.23.html#subj3, 1988.

[3] Overton, M. Hoaxes and other electronic ephemera. Proceedings of the 11th Virus Bulletin International Conference, 2001.

[4] Harley, D.; Slade, R.; Gattiker, U. Viruses Revealed, Osborne, 2001. http://momusings.com/papers/.

[5] Oxford Reference Dictionary. Oxford University Press, 1986.

[6] Overton, M. Out of Africa. Virus Bulletin, May 2003.

[7] The alt.folklore.urban FAQ. http://tafkac.org/faq2k/.

[8] Dawkins, R. The Selfish Gene. Oxford University Press, 1976.

[9] Dawkins, R. Viruses of the Mind. http://cscs.umich.edu/~crshalizi/Dawkins/viruses-of-the-mind.html.

[10] Harley, D. AVIEN Malware Defense Guide for the Enterprise. Syngress, 2007.

[11] Overton, M. http://cluestick.info/hoax/Definitions.htm.

[12] Harley, D. Bill Gates shares his fortune – not. http://www.eset.com/threat-center/blog/?p=543, 2009.

[13] WildList International Organization. http://www.wildlist.org/faq.htm.

[14] Slade, R. Hoax Viruses and Virus Alerts. Handbook of Information Security Vol. 3. (Ed. Bidgoli). Wiley, 2006.

[15] Cohen, F. A Short Course on Computer Viruses, Wiley, 1994.

[16] Jones, L. Good Times Virus Hoax FAQ, 1995. http://www.cityscope.net/hoax1.html.

[17] Hoax Slayer. Postcard Image Virus Hoax. http://www.hoax-slayer.com/postcard-virus-hoax.shtml.

[18] Harley, D. Hoax: 'Life is beautiful'. 2008. http://www.eset.com/threat-center/blog/?p=169.

[19] Overton, M. Mind Wars: Attack of the Memes. Presented at Open University conference 'Combating Vandalism in Cyberspace', 2004.

[20] http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=10170.

[21] Harley, D. PSST! It's PFTS! http://www.eset.com/threat-center/blog/?p=695.

[22] Harley, D.; Gattiker, U. Man, Myth, Memetics and Malware – Why Aren't We Winning? EICAR Conference Proceedings, 2002.

[23] http://www.sophos.com/security/hoaxes/recent/.

[24] Barber, M. Urban Legends. Summersdale, 2007.

[25] Harley, D. Viruses of the Mind Re-Visited (Return of the Memetic Virus), or How the NHS was Swamped by the Tsunami. Presentation for UK CERTs, 2005.

[26] Harley, D. When is a hoax not a hoax? 2009 http://www.eset.com/threat-center/blog/?p=717.

[27] Kabay, M. Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy. EICAR Conference Proceedings, 1998.

[28] Overton, M. Canning more than SPAM with Bayesian filtering. Proceedings of the 14th Virus Bulletin International Conference, 2004.

[29] Debrosse, J.; Harley, D. Malice through the looking glass: behaviour analysis for the next decade. Proceedings of the 19th Virus Bulletin International Conference, 2009.

[30] Abrams, R.; Harley, D. People Patching: is User Education of any Use at all? AVAR Conference Proceedings, 2008.

[31] Hambridge, S. RFC1855 – Netiquette Guidelines. 1995. http://www.faqs.org/rfcs/rfc1855.html.