A first step towards automatic hoax detection

Julio César Hernández[1], Carlos Javier Hernández[2], José María Sierra[1], Arturo Ribagorda[1]

[1] Computer Security Group
Carlos III University
28911 Leganés, Madrid, Spain
{jcesar,sierra,arturo}@inf.uc3m.es

[2] Department of Computer Science
Complutense University
Madrid, Spain
chernandez@pas.ucm.es

Abstract

Recent hoaxes, specially virus-related hoaxes, have shown a previously unknown degree of danger. Although current policies against hoaxes are certainly helpful, their ability for dealing with them is very limited, especially against some of the new and more imaginative types of hoaxes outlined in this article. The expansion of the Internet, and the corresponding boost in hoax evolution, have increased the need for automatic detection tools, and everything suggest this need is going to grow in the near future. In this work, after a quick introduction to the past, present and future of hoaxes were their quick change rate and the difficulties and limits for their automatic detection are highlighted, we propose two approaches: heuristics, which should be enough for dealing with the easiest and most common ones, and traffic analysis to fight the toughest.

Keywords: hoax, chain letter, automatic detection, virus, worm, heuristics.

1. Introduction

There have always been hoaxes in the history of mankind. Their purpose has been to persuade or manipulate people and make then do or prevent pre-established actions, usually using threats, misleading them or making them believe things that weren't real. Their great influence in our history is second to none, and some of those false ideas are now part of our culture. Chain letters, that could be seen as a special case of hoaxes, are also well known for using sorts of pyramidal schemes to rip money out of the receivers, persuading them with great benefits, threatening them with destiny's will, or both.

Hoaxes are not only related to virus warnings. There are hoaxes about health, nutrition and products of any kind [8]. There are also hoaxes about enterprises, famous people, exotic countries, etc.

Now, social engineers, con artists, and rogue people of all kinds have found a powerful playground to play and experiment with hoaxes at no cost, and with optimum

0-7803-7436-3/02/$17.00 ©2002 IEEE

anonymity characteristics. The Internet is a nice place to start a false story, to experiment and try new ways of deceiving people, and follow them as they evolve from host to host, with nearly none additional effort. If the story is good enough (if it has what it takes, we will return to this later) it has a long and successful life assured.

In this article we are going to see that hoaxes, especially, but not only, false virus warnings, can be much more dangerous to an organization than what is usually believed. The present approach to solve this issue is, in many cases, based in the application of strict non-remailing policies within the organization and, although this can help, it is far from being a definitive solution. Automatic hoax detection, which is a new field with little to none previous research, can be more helpful than what we may think.

2. Why do they propagate?

Hoaxes and chain letters use the same methods of replication. They rely on some pitfall or characteristic of our design that let them use us as replication machines. Put it another way, hoaxes and chain letters are "viruses of the mind" [1], they are written in user-executable code the same way computer viruses are written in machine code or biological viruses are written in DNA. They provoke one or more actions on the infected individuals, being one of them to pass them along to new individuals.

2.1. Meme theory

Memes, first introduced in [9], are described as self-replicating patterns of information, which propagate via the human mind, interacting with it, adapting, mutating, and persisting. That is a, so to speak, "virus of the mind". Those can include ideas, thoughts, recommendations, opinions, common sentences, catching stories, etc. They can evolve trough mechanisms similar to crossover and/or mutation, interacting with other memes just in the same way sex can make our genes interact.

Hoaxes and chain letters can be seen, from this point of view, as two special cases of memes. And, as good memes with successful replication capabilities, they are here to stay. Of course we can take actions to mitigate their effect, we can even eradicate a complete family of virii (like in medicine). But we won't completely eradicate hoaxes. This pessimistic view is founded on facts learnt after years of research in medicine and computer virii, and also highlights a predictable increase in the complexity and success of hoaxes and the like, which justifies the necessity, and also the difficulties, associated with automatic hoax detection.

This relationship between memes and hoaxes also seems to imply that there could be a set of characteristics necessarily present in every successful hoax or chain letter, characteristics that interact to produce good individuals that are replicated, or bad ones that don't go much further. This assumption also means that, if this set of characteristics is nearly constant in time, successful hoaxes, chain letters and the like could be identified just by looking for those characteristics.

Although this could sometimes be the case, we believe that the identification of hoaxes and chain letters cannot be entirely relied upon an heuristic mechanism, being the human mind capable of finding ways to elude this examination. We will return to this point later, when talking about different ways to identify a hoax.

2.2. Current factors

Meme theory provides us with a theoretical background to analyze hoaxes, chain letters and the like. But, what characteristics do have presently successful hoaxes and chain letters? Why do they propagate so successfully? Some of the reasons (first four cited from [1]) are:

- Confidence in the sender of the mail: in our normal life we constantly have to give different levels of confidence to stories depending both on the story itself and its source. Past records from the same source affect the level of confidence we give to it. In the same way, we give confidence to a story depending on who sends it.

  Although this is pointed out in [1], they don't pay attention to an interesting effect not unique of hoaxes and chain letters: reaffirmation. Usually, hoaxes and chain letters are received more than once from different sources. Being C(S) the confidence we give to a source S, a non skeptic user can give a huge amount of confidence to a message:

  $$C(M) = \sum_{S \text{ in } Sources(M)} C(S)$$

  Although a more skeptical user can give it a more reasonable value:

  $$C(M) = MAX_{S \text{ in } Sources(M)} C(S)$$

  Usually, a user gives a level of confidence between those two values, i.e., there is a phenomenon of reaffirmation, just by receiving more than one copy of the same message from different sources.

  In this line, it is interesting to observe that receiving more than one copy *of the same* message not always contributes to increase this reaffirmation effect to the optimum. A new strategy along those lines, not previously seen in the real world, could be to make circulate more than one version of a hoax, similar but not identical, purportedly coming from different sources, thus increasing its credibility just by simulating different witnesses describing the same facts with their own words.

- Excitement: the fact of passing on the message, usually appearing it to be of such importance, gives us a sense of excitement. "The sense of power and knowledge, and the frisson of pleasure which is imparted by reading about the latest, most deadly virus, tends to encourage us to share this information more widely".

- Sense of importance or belonging to a group: sharing information with the rest of our group can make us feel more part of that group. Also, when a person is the only one to bring these 'important' notices to the attention of the group, he or she establishes as the most important provider of information, even the 'virus expert' of the group.

- Furthering our own goals: if a person has a strong commitment to a subject and has been criticized for it (for example, 'the supernatural') passing on a hoax about something related (about U.F.O's or unknown animals) can be a way to say 'See? I was right, and there is these authorized people backing me up'.

  Also, hoaxes concerning virii could be passed on by people interested in or concerned with them, as a way to call attention upon them and even to help further the cause for increased security budgets and increased personnel.

- Reinforcement of message credit: we can be a little skeptical about a message, but what if something 'proves' it? We have already seen reinforcement by having different sources for the same (or nearly the same) message. There can be other ways of reinforcement of the confidence we give to a message. For example:

  - If the hoax is about a virus (worm, etc.) described by its subject (i.e., 'Good Times' hoax), what if we later receive a mail with that subject?

  - If a hoax prompts us to search the computer for a file, registry key, listening TCP/UDP port, etc. that is supposedly present if we are already infected, and we find it (maybe just because it is a normal part of the operating system or a common application), that can give the message much more credit. SULFNBK.EXE and JDBGMGR.EXE hoaxes are two recent and well-known examples.

3. From past to future trends

Studying hoaxes and chain letters involves studying their origins and motivations. Both of those are generally uncertain, but in some cases interesting information can be deduced from the actions that the hoax asks its victims to perform (its 'payload').

Some proposed motivations are, in no particular order: just for fun, for impressing someone, for improving self-esteem or testing or showing one's capabilities, even to hurt or less the credit of a group of people or an organization. In these cases, creating a hoax and seeing how far it goes [2], especially if it gets some press coverage, gives you full credits. The higher spreading capabilities, the better.

Another motivation can be to eliminate another hoax or chain letter. In fact, some have proposed that one of the most well known virus hoaxes, the 'Good Times' virus hoax, was created to stop the propagation of a pyramidal chain letter called 'Good Times'. That still remains to be proven.

Hoaxes can also be used to attack someone's reputation or the credit of an enterprise or an entire country. A simple example of this is the 'Blue Mountain Arts Virus' hoax, which declares that all virtual cards issued by Blue Mountain Arts are infected with a virus that had penetrated its system. Organizations ranging from Palmolive to KFC have also suffered from these types of attack.

Hoaxes can also be used to promote a sort of denial of service (DoS) attack, especially by flooding web servers, mail servers, or multiple phone lines. For example, the 'Jessica Mydek' hoax asked users to forward the message and contact the American Cancer Society for further information, causing a denial of service on their servers.

Thus far, these motivations seem to be of little concern to the general public, unless they are directly affected by the hoax, so one could think that if the objective of the hoax has been another individual or enterprise, we would not be affected. But this is not completely true; hoaxes can have other collateral effects, even on our personnel or our systems.

For example, hoaxes can be used to lower our guard towards a certain 'virus menace'. If it is well known that the 'Good Times' virus does not exist, why don't we create a virus and call it 'GoodTimes.exe'?. Then, some people will be persuaded that this is not a virus. Any hoax warning related to a thread could be a precursor to a real attack [5]. As a matter of fact, this has already happened, for example with the AOL4FREE hoax warning (about a real and normal program that hacks some extra time on AOL for its users) that precludes an AOL4FREE trojan horse that deleted files from the hard disks of the infected systems.

Nowadays, a new type of hoax is becoming quite common. The main purpose of this new kind of chain letter is to build up a list of currently in-use, fresh, e-mail addresses, to sell it to spammers or to abuse from it immediately. This chain letters usually appear in massive e-mail services like Hotmail and, for example, warn the readers that the service is going to be discontinued to those accounts not currently used, in order to do a massive cleaning up. The mail urges the receiver to answer to a given address and also to pass it on to any friend that may have an account in the system. There seem to be many incidents of this type [2]. An interesting alternative is to circulate a mail trying to pick up signs from people supporting a particular person, cause or organization, where sometimes hundreds of persons write down their e-mail addresses, names, countries and even some professional information that makes these mails invaluable for spammers. And it shouldn't be necessary to mention how bad could be to become an objective of spammers.

This is an easy and usually successful way to obtain an up-to-date list of e-mail addresses of, and this is an important point, people that is not very skeptical. Even more, we can craft a mail to obtain addresses of people with special interests, like having stock shares of a given company, having a certain hobby, supporting a particular political cause, etc. This means we could have a group of victims we know something about, so a social engineering attack could become much more feasible, possibly affecting not only the person, but also his employer's.

No hoax is completely inoffensive, but some are especially dangerous, having very dangerous payloads like provoking the victim to manually damage one or more of the operating system's files. For example, the 'SULFNBK.EXE' virus hoax gives instructions to find that file on one's computer and delete it, as 'it contains a virus'. The same applies to the 'JDBGMGR.EXE' virus hoax and some other.

This trend could evolve towards a more dangerous version, consisting on a message that makes the reader download an anti-virus checker and/or repairer for a 'new and devastating virus' not currently reported by any anti-virus tools (Why not? Easy: many reasons are at hand: the virus itself comes from an anti-virus company, some of the anti virus tools are already infected, it uses a new stealth technology, ...). Or even one that makes the reader send a certain file (in a web form or simply by e-mail) to an automatic anti-virus service' to see if it is infected. This file can contain system passwords, for example. Those payloads are dangerous both for personal systems and for corporate ones. And they are just part of what can currently be done. Imagination is the only limit.

4. So, are they really a problem?

Hoaxes and chain letters can create a lack of resources, more precisely of space in mail servers and bandwidth on your network, not to mention the working hours lost by reading and processing (ideally discarding them, but sometimes passing them, or even phoning friends to warn about) the daily flow of them. As virus hoaxes are not detected by anti-virus software, nothing prevents them from harassing your information systems.

These are not the most significant troubles. There have been incidents in which some recipients occasionally believe a hoax to be a true virus warning and may take drastic action. Some companies panic when they receive a hoax virus warning, and quickly assume the worst - making the situation much worse by taking such drastic actions as shutting down the network or isolating it from the Internet [17]. In the same vein, end users believing a hoax can damage their workstations, by executing the hoax payload (usually, instructions to 'clean' the workstation).

Although no official research has been done in this subject, it is likely that a successful hoax with an adverse payload could cost you much more money than the average virus.

5. Identifying a hoax. Evolution

Most common hoaxes and chain letters are easy to spot at first glance. Many papers about hoaxes, especially those about false virus warnings, highlight some characteristics of a typical virus hoax.

5.1. Evolution of the 'typical characteristics'

It is worth to mention that some of those characteristics, written down some years ago, are no longer valid, showing a quite high change rate in the field. For example, these heuristic rules are no longer valid:

From [1]:

1. The message comes from an individual, maybe an executive at an enterprise, maybe just a user, but never come from the purported original source of information.
2. It asks the reader not to read an e-mail.
3. Only way not to get infected is to delete the referred e-mail.
4. Describes the virus as capable of horrendous damages to your computer (such as destroying hardware or completely erasing your HDs).

From [3]:

1. They don't have a date stamp, to maintain the hoax alive.
2. There's no identifiable original source.
3. It doesn't identify the affected platforms; it just says something generic like 'by e-mail'.
4. Once affected, there's no way to recover the lost information.
5. There's no governmental agency cited as the origin of the report.

Although some of the heuristics cited in those articles are still valid, such as:

- The message usually has may uppercase letters and many signs of exclamation.
- It asks the reader to forward it to as many people as she or he can.
- It tries to obtain credit citing an authorized source, like a governmental agency (CIAC, CERT, even the FCC, which does not send virus warnings).

And our favorite rule of thumb (from [5]):

- If the message seems more oriented to persuade the reader than to inform him, there's a good chance it is a hoax. Hoaxes try to push our 'emotional buttons' rather than our logic.

What we want to point out here is that the once considered typical set of characteristics of a specific type of hoax (a virus hoax) is not static, but it evolves constantly, as new hoaxes appear.

Now, not every virus hoax warns about an e-mail message containing a hoax. There are new ones that warn about a file already present on our hard disk. There can be others that can warn us about completely normal programs saying they have spyware, etc. Although uncommon at the beginning of the spread of hoaxes in the Internet, now there are hoaxes that claim to be originated by the CIAC or the CERT, and some of them include (invalid) telephone numbers to obtain more information (Why not including also valid ones? If the hoax spreads enough, it would be impossible to call those numbers, reaffirming the confidence in the message for everyone that tries to call and confirm).

5.2. Is it so difficult to spot a hoax?

We must bring into consideration two factors here: the technical knowledge of the receiver and the evolving characteristics of hoaxes.

As the access to the Internet is becoming mainstream, common and even familiar, the average technical level of the people connected decreases, even thought new generation's user's expertise is greater, as they begin to know computers earlier (but that doesn't mean their technical level is superior). At the same time, the amount of knowledge that a virus expert needs to learn to keep up-to-date is growing everyday. Hoaxes evolve as well: for example, some easy-to-spot false claims of older hoaxes are no longer present in new ones. At the same time, the greater level of interoperability of software components and some newly discovered software hacks make possible what was once considered impossible. For example, it was once assumed that no virus (or worm) could spread by only reading a mail (as the 'Good Times hoax' claimed, that was one of the main arguments of the people who first discovered the hoax). But that is now possible, as some buffer overflows have been discovered in the way some popular e-mail clients (like Microsoft Outlook) work with dates, and in the way some embedded HTML parsers (like Internet Explorer) render HTML pages. As some e-mail messages can be in HTML, and when we want to read them some clients (like Outlook) opens them right away without any warning, some viruses like the Kak worm and BubbleBoy (see [10], [11], [12], [13]) and others alike ([14]) have successfully spread just by reading them or, what is worse, just by seeing them in the preview panel (open by default in Outlook).

So, although it is still easy to spot some hoaxes, more elaborated ones can be very difficult to discover, even to a technician or an expert. If the warning message is good enough, our only trusted source of information should be the recognized sources (CIAC, CERT, etc.). But, what if the message doesn't appear there? Or even worse, what if someone finds a meme capable of gaining more trust from the reader that those authoritative sources? In general, without an authoritative source, hoaxes can be very difficult to spot even to a trained technician.

As one can easily imagine, the reasons fore-mentioned make us expect that a solution based on heuristics would be capable of dealing only with the least elaborated hoaxes. If we want to raise its usefulness, we are going to reach a degree of false positives (for example by classifying a legitimate mail as a hoax and thus avoiding it to pass the enterprise mail server) that can be as bad as the original problem hoaxes pose.

6. Present solutions

Currently available solutions base themselves in two pillars: authoritative information and behavioral policy of the employees (relating to e-mail, Usenet and any other way of direct communication over the Internet).

Nowadays one common way of dealing with hoaxes, chain letters and the like consists in:

- Designate one person (or workgroup) as the one in charge of dealing with all e-mail warnings. They should use methods such as PGP signature verification for validating the information received from and present in the referred sources, and even personal communication with the sources to check the information.

  They should be the only authoritative source of information in the organization, and all the true and verified alerts should come from them.

- Then, the organization urges every employee not to pass on warnings to other employees, but to this person or group, thus imposing a policy on the use of the e-mail and other available means of communication such as Usenet.

- While imposing this policy, it's important not to concentrate on a determinate type of hoax (like virus warnings) but to be as broad as possible to make people react the same way to new types of hoaxes and chain letters.

Those solutions have some important drawbacks:

- They don't pay attention to personal systems: these policies and authoritative sources are well suited to work properly in a hierarchical organization. But they don't work in a distributed or non-hierarchical environment. For example, they won't work fine in a magazine with many free-lance writers that occasionally connect to its network. They won't work either for the person that uses his personal computer at home. When that person goes to his worksite he can carry infected software or infected ideas from home.

- They impose a struggle for confidence: nowadays, hoaxes and chain letters only have to fight with the (frequently low) skepticism of the reader. Setting up those policies will make them fight also versus the confidence of the reader in the people that his organization has designated to manage those messages, and also in the confidence he has in his organization. If the message is capable of reaching a high degree of confidence in the reader, it still can win the battle.

- They won't be of use when a new type of meme particularly capable of dealing with that particular security policy would arrive. Of course, anyone can argue that such an argument is very broad one and difficult to prove. We don't think so.

  For example, imagine a hoax about some spy software used by enterprises, and that gives people the opportunity to get rid of it. Imagine a hoax more or less like:

> WARNING - YOUR ENTERPRISE COULD BE SPYING YOU
>
> Software that lets big bosses watch what you're doing has been recently discovered by well-known antiviral researcher and rights fighter Nikolai Kavspersky. This software is designed to spread through an organization network using virus and worm techniques like n-tier replication and mail infection, so you can have it running even without knowing it.
>
> The software lets your boss see what you are doing, the web pages you are visiting, the mails you receive or send, and any program you use in your computer. It is well known that some employees have been already fired after being spied with this tool, although the fact this tool was used to collect information, and its name, was not released at the trial.
>
> How can you know if you have it?. You just have to search for MYDOCS.DLL (a nickname, probably after My Documents) in the Windows\system folder. If you have this file, you are infected! Watch out!
>
> You CANNOT delete it, as your boss will know immediately. Best practice is replacing it by a variant of MYDOCS.DLL created by the people at Kavspersky Tech. Labs. This variant lets you choose which program you want your boss to see or not. By default, it lets your boss see any MS Office program, but not Internet Explorer or any e-mail programs, so you would appear as a very working fellow.
>
> You can download the crafted copy of MYDOCS.DLL at http://.... or searching for it in http://...
>
> Be warned: some people using this spy software will try to prevent this advice to reach you or even say it is a hoax. You should know whom to believe.

When having to choose among themselves or the organization, many people would choose themselves. So people who believe this message or any variant of it, won't send it to the person or group in charge of alerts, as they are part of 'the organization'.

This is, then, an example of a meme that can pass on even with the e-mail policy of your organization. We believe there will appear other types of memes, much more wise, complex and elaborate, capable of such, it's just a matter of time and evolution.

7. Proposed solutions

Although trying to prevent hoaxes with automatic tools may seen to some as trying to kill flies with air-force jets, we believe this is the best solution considering all the former limitations of the current approaches to hoaxes.

7.1. Signature and heuristics analysis in anti-virus software

We believe that there is no reason for not expanding the anti-virus software capabilities to include hoaxes and chain letter signatures, and also to include some heuristics capable of dealing with the easiest hoaxes around.
In future works we will focus on these heuristics, although some ideas have already been presented in this article.

7.2. Traffic analysis

To deal with the toughest ones we think that a different approach is necessary, as heuristics (very possibly the better ones will be designed by people clever enough to avoid heuristics) and even message signatures (remember they are unknown, so signatures are not available yet) won't be enough. Here, we propose a new method based on traffic analysis to study the propagation of incoming mails.

Hoaxes and chain letters have a peculiar way of spreading, totally characteristic. It's a different way than those followed by e-mail viruses (worms) and the like. The main difference being hoaxes are forwarded by a human mechanism, which establishes a filter on who to forward it to. Worms, in the opposite, forward themselves using pre-established mechanisms: to all the addresses available, to all the address book, to a random subset of the addresses available or to a random subset of the address book, to the 20 first addresses in the address book, etc. Hoaxes, on the other way, are generally forwarded to people, which have a special relationship with the forwarder (same workgroup, classmates, friends, etc...), but, for example, not usually to bosses. Another difference between the two is that the spreading path of hoaxes is usually repeated or at least very similar for different hoaxes.

How can we differentiate both of them? We can learn the difference. The procedure should imply spreading some inoffensive hoaxes in the organization and learning its spreading paths. Then we should assign to every electronic address that has received a hoax its 'forwarding set' (Frwd(address)), the sets of addresses to which it forwards the hoax. Also, we can automatically calculate a sort of mean and variance for this set, by computing it when faced with different kinds of hoaxes and chain letters. We should compute this set for every electronic address, so if there are addresses not affected by the initial spreading, they should be automatically sent the hoax to figure out the forwarding set. Obviously, as the overall set of electronic addresses changes from time to time, this test should be run more than once.

The technical difficulties of running such a test are out of the scope of this article, but we can point out some of the difficulties and how to deal with them:

- After spreading a hoax, if we have not data to figure out Frwd(X), then we should send a -different- hoax to X, as the rumor of the initial hoax could have been propagated to X by other means.
- Another possibility is to send a hoax H to all the e-mail accounts of the company and filter out their forwarding messages so they are not really sent outwards. Thus, we can calculate Frwd(X) for every electronic address X in the company.
- Also, we can study how reaffirmation affects each individual X by sending crafted copies of the hoax H from their colleagues (for example, from their most frequently used e-mail addresses) until they fire H again.

It is important to mention that following the spread of the hoax as it is sent and read by the people of the company, although has some serious privacy related implications, is extremely easy to perform technically. A good way to do it is to use the above-mentioned technique of executing code by reading a mail, and/or including one micro image embedded in html code that opens a connection to a web server, connection that can be easily logged.

In any case, the hoax alert should be raised when there's one message that spreads in a significantly similar way to the path previously learned. This 'significance' degree must be calculated by hand, but a degree as low as 0,5 (over 1) should be enough in most cases. Also, when calculating this degree, one should take into account old and deleted e-mail accounts and new ones (of which we don't know yet their 'forwarding set', but it can be learned on the fly).

8. Conclusions

We believe hoaxes and chain letters are here to stay, and that they pose a real threat, especially virus hoaxes. We think their hit level is going to increase in the near future, and that their payloads would become much more dangerous than those found on present hoaxes.

Issuing a central communications and viral policy is a good start, but it is not enough for a comprehensive level of protection. We also believe that automatic detection is the way to go: anti-virus software should take into account at least virus hoaxes (if not all kinds of hoaxes), as a normal e-mail enabled anti-virus server is the best place to analyze incoming traffic. Both signatures and some sort of heuristics should be employed.

At a higher level, controlling all the SMTP servers of an organization using traffic analyzers with new technology, specifically suited for hoaxes and chain letters, after studying their propagation paths through your organization, should be enough for guarding it from the more sophisticated ones.

References

1. Hoaxes and Hypes. Sarach Gordon, Richard Ford and Joe Wells. http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html.
2. Information about hoaxes - Hoaxbusters. http://hoaxbusters.ciac.org/HBHoaxInfo.html.
3. Dealing with Internet Hoaxes/Alerts. David Harley. http://www.sherpasoft.org.uk/anti-virus/hoaxes.txt
4. Urban Legends and Folklore. http://urbanlegends.about.com/library/howto/hthoax.htm?once=true&
5. Internet Hoaxes: Is there Danger?. Jeff Langdon. http://rr.sans.org/malicious/hoaxes.php. 2001.
6. Virus hoaxes: are they just a nuisance?. Darren Grocott. http://rr.sans.org/malicious/hoaxes2.php. 2001.

7. Internet hoaxes: the truth is out there. Jeff Henning. http://rr.sans.org/securitybasics/hoaxes.php. 2000.

8. Centers for Disease Control and Prevention: Health Related Hoaxes and Rumors page. http://www.cdc.gov/hoax_rumors.htm.

9. The Selfish Gene. Richard Dawkins. Oxford University Press. 1976.

10. Bubbleboy virus description at F-Secure. http://www.europe.f-secure.com/v-descs/bubb-boy.shtml

11. Kak and Irok worms press note at F-Secure. http://www.europe.f-secure.com/news/2000/20000330.shtml

12. Kak (KakWorm) virus (worm) description at F-Secure. http://www.europe.f-secure.com/v-descs/kak.shtml

13. KakWorm worm description at TrendMicro. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=JS_KAKWORM.C&VSect=T

14. BigPig virus description at TrendMicro. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=VBS_BIGPIG.A&VSect=T

15. Microsoft Outlook GMT buffer overrun exploit explained at McAfee. http://vil.mcafee.com/dispVirus.asp?virus_k=98744

16. Don't fall for a virus hoax. Sophos Virus Center, 1999. http://www.sophos.com/virusinfo/articles/hoaxes.html