Global Information Assurance Certification Paper

Charles Coffman
SANS Security Essentials
GSEC Practical Assignment
Version 1.4b, Option 1
January 3rd, 2003

Gotcha! : Virus and E-mail Hoaxes

Introduction

Virus and E-mail hoaxes are a real issue in today's electronic culture. They can be classified as a form of social engineering. "In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures."[1] The existence of virus and e-mail hoaxes uses resources, costs money, and picks and pulls at the already frayed nerves of the often overworked, understaffed information technology corps. Hoaxes are nothing new. They are created by people to trick people. They come in a myriad of formats, claiming all sorts of "good." The only good news about them is that virus and e-mail hoaxes can be detected, contained, and virtually eliminated.

The great Greek orator Demosthenes said, "A man is his own easiest dupe, for what he wishes to be true he generally believes to be true."[2] Did you ever think that they would really give you 5 bucks for every person to whom you forwarded that e-mail? Did you really believe that restaurants were offering genetically mutated meals in place of their normal fare? You may have actually worried about the gang initiations that take advantage of women drivers traveling alone. Your heartstrings were probably tugged by the plea for help from the parents of unfortunate children. Whatever the case, we have all been affected by the never-ending barrage of virus and e-mail hoaxes. It has been said that a sucker is born every minute. Are you one of those suckers? If not, you probably know one. "Does it really matter?" you ask. Well, let us find out.

What are they?

The Merriam-Webster dictionary defines the word hoax as follows: "To trick into believing or accepting as genuine, something false and often preposterous."[3] Hoaxes have been around since the beginning of history. People have been duping and being duped since the serpent tricked Eve in the Garden of Eden. Pop recording artists have tricked us into believing that they were actually singing on their albums and on stage. More recently, we learned that the timeless "Bigfoot" legend, supported by supposed actual photographs, was nothing more than the efforts of one individual attempting to take advantage of the gullibility of the entire society.

Conventional mail hoaxes have taken the form of chain letters, threat letters, and as of late, the famed anthrax scares. The birth of electronic mail only served to confirm that there is nothing new under the sun. Anything you can do through conventional, or snail mail, can be done better, bigger, and faster through e-mail. The virus hoax is a bit more specialized in design. I will discuss virus hoaxes in more detail. Keep in mind though that the primary vehicle for the virus hoax is e-mail. It is a combination threat, a one-two punch, so to speak.

E-mail hoaxes generally target the emotions of unsuspecting users. These types of hoaxes often include a message referring to e-mail tracking software that pays a person for every "hop" a message takes that was forwarded by that person. There is no such software on the market. There are many "free stuff" hoaxes floating around on the Internet. There has never been a confirmed case of anyone receiving anything because of these hoaxes. Another hoax claims that either "something bad" will happen or that "something good" will not happen unless a person forwards a particular message "x" number of times. This is a case of the famous omniscient e-mail message. Believe it or not, e-mail messages are not aware of you or themselves. Many times, an e-mail hoax creator's intent is to prey on the lack of knowledge of e-mail/internet users. Common e-mail (non-virus) hoaxes include but are not limited to the following:

Give-Away Hoaxes
Sympathy Hoaxes
Threat Hoaxes
Scam Hoaxes

A more extensive listing of e-mail hoaxes can be found at http://hoaxbusters.ciac.org/HBHoaxCategories.html

Virus hoaxes are created to look like helpful information. If a person heeds the "alert," they will be helping everyone in their organization. They will be helping to save money. They will be helping to prevent the spread of a malicious virus across the network that could cripple their company (more about that in a bit.) They will be helping the already overworked IT professionals with their daily network monitoring responsibilities. People just want to help. This is what virus hoax creators are counting on. Common virus hoaxes include but are not limited to the following:

WTC Survivor
Jdbmgr.exe virus
A Card for you virus
Bud Frogs virus

A more extensive listing of virus hoaxes can be found at http://www.symantec.com/avcenter/hoax.html. From this point on, virus and e-

mail hoaxes will be referred to together as “hoaxes” unless one or the other is specified.

Where do they come from?

Even though hoaxes cause trouble, not all hoaxes are created out of malicious intent. That is, not all of the hoax creators are intending to cause any type of harm and sometimes they don’t even know that they have created a hoax. There are several different types of hoax creators. Some hoaxes are products of creative writers. They are just stories intended as entertaining reading. Achieving hoax status only requires that one person take the story seriously. Other hoaxes are urban legends that have been circulating for a very long time and eventually ended up in an e-mail message. Many hoaxes actually include some degree of legitimacy. That is why they make the rounds as they do. Meaning, some hoaxes are circulated over the years, and each time, the false information is embellished to one degree or another. Hoax creators also include pranksters, disgruntled employees and customers, and hackers.

The prankster is just that, a person that pulls pranks. They think that it’s amusing to cause confusion and distress among their fellow human beings. An example of this follows. A caller rings your phone and asks, “Is your refrigerator running?” You answer, “Why, yes. It is.” The caller responds, “Well then, you had better go and catch it.” “What’s the big deal,” you ask? Look at the clock. It’s three in the morning. Amazingly, many people think that this is funny… until it happens to them. Electronic pranks, on the other hand, can cause the loss of much more than a little sleep and they are not nearly as funny.

The disgruntled employee is a person that spreads a slanderous rumor in the form of a malicious message in an attempt to defame their employer because of some conflict that has caused them to become uncomfortable to the point of retribution. Many people consider themselves disgruntled, but lack the motivation and/or resources to complete the job.

The unhappy customer was not always that way. They bought and used a particular product. The product didn’t perform as advertised and they didn’t get the expected response and/or service from the product provider. That’s all it takes. The customer is now unhappy and launches their own personal war against the product provider with hopes of convincing millions of other actual or potential customers to boycott the offending provider.

Then there is the hacker. A hacker is defined as, “a person who illegally gains access to and sometimes tampers with information in a computer system.”[4] The hacker’s main purpose is to attack, compromise, and/or disable network resources. Hackers may be classified in a number of ways. They may be and probably are one of the aforementioned hoax creators. The argument can also

be made that all of the previously define perpetrators are themselves hackers. Either way, their products and services are damaging.

How do they get here?

The term ultracrepidarian is used to define a person who gives opinions beyond his or her scope of knowledge. When a person or an organization makes a claim, question their authority. Do they have the necessary experience in the field that they are commenting on to be considered an expert in that field? What are their credentials? Who can vouch for them? Find out! Some experts describe False Authority Syndrome as a condition in which a person claims to be an authority on a subject when in reality that person has little or no experience in the field. Their self-assumed authority stems from the fact that they are considered an expert in a related field. Just because a person can use a computer, does not make that person an expert on all computer related subjects. For more on False Authority Syndrome, check out the article at http://vmyths.com/fas/fas1.cfm.

The news media is a major vehicle for the transmission of hoaxes. The power of mainstream media must not be taken for granted. Unfortunately, many in charge of security act on information that they received from a major news network in the morning while they were having their coffee. "Empirical Research Systems (a computer industry polling firm) conducted a survey in 1991 of corporate employees tasked in some way with computer security. 43% of respondents -- almost half -- formed their opinions about viruses just by reading newspapers!"[5] Often, when a potential problem is discovered, the news media will spread rumors of the problem without actually verifying the credibility of such claims. There have been cases where a problem did exist but its severity was falsely escalated by the opinions of unknowing media outlets. One such case can be reviewed at http://vmyths.com/hoax.cfm?id=249&page=3&cat=Media%20flops,%20media%20fiascos.

Contact lists are a very popular mechanism for spreading electronic chaos. Some viruses depend on e-mail lists, or address books, to propagate their messages of confusion. All it takes is just one electronically connected person to start a chain of lies. That one person receives or creates false information. They assess the credibility of the information. They tell two friends. They tell two friends… and so on, until everyone knows.

Websites can be used not only to advertise false information, but also to serve as a repository for corrupt software. Patches, updates, fixes, and add-ons can be modified to carry a malicious payload that, when launched, may or may not produce the expected results, but will definitely produce unexpected results. All software should be obtained from trusted, verifiable sources. Manufacturer

websites are usually the best bet but even the big boys have been known to release questionable fixes.

Some messages advertising a fix are actually viruses in disguise. People are shammed into thinking that they are fixing or preventing issues when, in reality, they are just launching and many times propagating more problems for themselves, their organization, and possibly even the global networked community. A fix for a reported issue is mailed with an attachment. The user is instructed to run the attachment in order to fix the problem. The user follows the instructions and infects himself or herself with a self-propagating worm that queries their address book and sends itself to all of the user's contacts. This could be disastrous depending on the size of even one user's contact list. Another mechanism that hoaxes employ is to convince the user to find and delete files from their computer that are supposedly infectious files. Users will delete these files without any clue that they have just deleted critical system files. The result is often a denial of service that renders the computer useless.

What do they do?

Mass coincidental electronic communications can bring a network to its knees. Hoaxes are usually designed to make users want to let everyone know what is going on. Whether the users' intentions are to do good deeds and warn everyone or to display their technical ability, the result is the same. When all users in an organization or networked community start sending everyone in their contact list messages about anything, real problems will occur. Computer messaging and network systems are designed to handle a predetermined volume of traffic. When this predetermined threshold is exceeded, network activity can slow or even cease.

Once an organization has been foisted by a hoax, the users that it affects must find out what is going on. As with every other unknown in their daily battle with their computers, they are going to call the helpdesk. Many helpdesks do not have the resources to respond to legitimate troubles, much less fake ones. In today's IT world of doing more with less, helpdesks are undermanned. There is absolutely no provision for any out-of-the-ordinary troubles. Besides being swamped with reports of virus infections, helpdesk personnel do not have time to find out the truth. Their strategy in dealing with the threat is purely reactionary and eventually very costly.

The users spend time thinking about the supposed issues. They spend time spreading the messages. They consume their time and the helpdesk's time calling in bogus trouble tickets. All of this time that they are committing to investigating false claims could be spent thinking about things that matter. They could actually be working.

System unavailability, human and physical resource overload, and loss of productivity all affect one thing. The common denominator is cost. What is it that really concerns upper management in an organization? It's cost. What keeps them up at night? That's right… cost. No successful business is built for fun. Making money is at the heart of entrepreneurship. If there is a way to make money by providing a service, it'll be done. Cost is the driving factor in many business settings. Sure, an organization may have been birthed under the realization that customers want excellent products and second-to-none service. Venture capitalists can even make that a reality. That is not to say that the original foundation on which the business was formed cannot continue to exist but, eventually, the cost must be managed and a happy medium must be achieved. Businesses can ill afford to just deal with their electronic infrastructure being unavailable for any length of time. Although the tolerance for a broken network varies from company to company based on their wired, or on-line dependencies, the fact is that time is money. Increased down time translates to increased cost.

How do we spot them?

What is truth? What is fiction? In most instances, a hoax can be easily detected. There are signs that accompany the transmission of a hoax. The question is whether the signs will be recognized and interpreted correctly. Knowledge and understanding are the main weapons that we have at our disposal in the war against the confusion that hoaxes introduce in to our society. Knowledge is the key to understanding but knowledge must be sought. Some signs include promises of money, inside information, guilt trips, details that just do not make sense, the lack of first-hand information, and appeals to our fears and senses.

The first concept that a person should grasp concerning hoax recognition is identified by two words – Be suspicious. Suspicions spawn questions and questions spawn answers. Asking questions is critical to the process of gaining knowledge. However, be careful about from where the answers that you seek come. As mentioned earlier, many sources are just itching to spew answers with no regard as to the accuracy of their conclusions. There are however, trustworthy sources available to which an individual may inquire about the legitimacy of almost any claim. I will discuss this further in the next main section.

Often times, the format in which the hoax is presented is the first indicator that something is awry. What is the message suggesting the user do next? Authentic alerts and/or requests do not urge the recipient to forward the message to as many people as they can. Authentic messages use verifiable propagation methods such as trusted websites, mailing lists, and media sources. Can the source of the message be verified? A trusted source can be identified by longevity in the industry and past proof of trustworthiness. That leads us to another sign.

Where did the message come from? Is the message originator an expert on the subject? Does the person have the authority to offer the deal? Again, can the source be verified, or is the whole thing based on hearsay? The originator may be just another victim of False Authority Syndrome. Computer users must learn whom they can trust.

What do we do about them?

The spectrum is broad when deciding what an organization might do about a hoax. The options range from the unwittingly passive strategy of ignoring everything until it has an effect to the passionately aggressive strategy of unplugging the network to ensure that nothing can get through. Obviously, these are the extremes. The optimal solution lies somewhere in between them and is a combination theories and actions depending on the individual environment. There is no magic bullet when it comes to dealing with hoaxes. No single device can eliminate the threat. As with all issues relating to information security, the solution is a package deal. The problem will not go away by itself. The solution is not accidental and can't be realized or achieved by wishing or hoping. Hoaxes must be dealt with directly and intentionally. They must be addressed internally as well as externally where the organization, their employees, and their customers are concerned.

Education and training is central to combating hoaxes. Education is the primary and sometimes only tool that an organization can use to thwart the propagation of hoaxes through their infrastructure as their business relates directly to their customers. Users must be empowered to check things out for themselves. The following is a short list of trusted internet sources that regularly post updated information about hoaxes:

http://www.trendmicro.com/vinfo/hoaxes/hoax.asp
http://vil.mcafee.com/hoax.asp
http://www.vmyths.com
http://www.sophos.com/virusinfo/hoaxes/
http://www.truthorfiction.com

As you can see, there are more than enough trusted repositories of hoax information. Users that can find out the truth for themselves, can stop the spread of hoaxes at the point of entry. Educated users are less likely to be the catalyst for the impending chain reaction. Businesses have many more options when it comes to controlling hoax infiltration internally and relative to their own employees. Not only can they make the rules, they can also enforce them.

Organizations must include provision for hoaxes in their information security policies. Security policies should be the foundation of any IT organization. No other measures of defense will be effective unless there is a

supported and enforceable policy in place. By supported and enforceable, I mean that executive management must accept and approve every aspect and detail of a security policy from the general instructions all the way to the consequences incurred by not following the policy. This approval must be obtained in writing. Do not assume that it is o.k. just because someone said so. Encourage the executive staff to own the policy. A sample security policy pertaining to hoaxes follows.

Do not forward any virus warnings to anyone other than <*insert name of security representative* > at <*insert e-mail address of security representative*>. It is the responsibility of a designated security representative to verify and distribute all virus warnings. Any virus warning which comes from any other source are to be ignored.

A suggested policy for personal use is described below. Erase every mail with an attachment that comes from an unknown person. Establish a free e-mail account on an Internet-based server for all jokes and the like. Never try an attachment your home computer unless you are protected by a firewall. Many of those little programs do not like being contained and will not run behind the firewall. Do not forward mail to others, especially at the e-mail originator's request. It is acceptable to forward good thoughts or jokes if they come as plain text. Plain text does not execute anything on the computer. Erase the message headers that show the paper trail as a courtesy to the reader. Do not forward any virus warnings. Tell your friends to upgrade their virus definitions. If you must forward good jokes that have the form of a virus warning or a chain letter, mark them as such before sending them.

Anti-virus strategies not only address explicit virus threats, but they can also detect hidden threats such as the fix that is really a virus. Anti-virus programs scan the innards of an e-mail message increasing the possibility that a hidden virus is detected even when it is not obviously present. Important aspects of an anti-virus strategy that must be remembered are:

1. Virus scanner coverage – Is every susceptible machine in the organization covered?
2. Virus scanner engine version – Does every at risk operating system run the most current version of the scanner engine?
3. Virus definition file version – Are you scanning your machines with the latest known virus signatures?

New viruses are discovered everyday. The Ten Immutable Laws of Security are generally accepted as an encompassing description of the issues that information security professionals face. Law number eight of the "Ten Immutable Laws of Security" states, "An out of date virus scanner is only marginally better than no virus scanner at all."[6] There are anti-virus management tools on the

market, such as McAfee's ePolicy Orchestrator, which will facilitate an organizational virus protection policy.

Organizations should use every technology at their disposal to keep themselves from being deceived. Firewalls, e-mail hubs, and intrusion detection software and hardware can be configured to block, dump, or track nearly any combination of attachment, text, and/or hoax signature. Alerts can be set to notify IT staff immediately on detection of any anomaly related to hoax transmission. In addition to internal detection measures, there are many internet resources that an IT security staff can use to stay up-to-date on the latest hoax information. The earlier an issue is detected; the sooner measures can be taken to eliminate the threat.

Conclusion

Do not wait until it happens to you before you take the issue of virus and e-mail hoaxes seriously. Too often, in the cat and mouse world of information technology security, the knee-jerk principle is in effect. Information technology organizations wait until they have been compromised before they address the problem. The old saying that an ounce of prevention is worth a pound of cure is true. Get out there and do the research. Stay informed. Educate the users. Deploy and configure the tools. If it does happen to you, don't panic. Virus and e-mail hoaxes are a real problem, but there is a real solution. The cost associated with implementing a strategy that will help detect and prevent the danger of hoaxes will not even come close to the cost associated with the damage that can be done by a successful widespread infestation of one virus or e-mail hoax. The state of human nature requires that people stay on their guard.

Visual Developer editor Jeff Duntemann sums it up best: "If people exercised greater discretion in who and how and to what degree they place their trust, we would know more as a community -- and we would know it better. There would be fewer paths for bad or phony knowledge."[7]

References

[1] "Social Engineering." searchSecurity.com Definitions. 5 Apr 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html (10 Jan 2003)

[2] Demosthenes. "The Third Olynthiac Oration, 349 B.C." The Columbia World of Quotations. New York: Columbia University Press, 1996. www.bartleby.com/66/89/16089.html (5 Jan 2003)

[3] Merriam-Webster Online. 2003. URL: http://www.m-w.com/home.htm + enter "hoax" to get this reference. (6 Jan 2003)

[4] Merriam-Webster Online. 2003. URL: http://www.m-w.com/home.htm + enter "hacker" to get this reference. (6 Jan 2003)

[5] "Magazines, Newspapers, TV." Computer Viruses and "False Authority Syndrome." 2000. URL: http://vmyths.com/fas/fas5.cfm (3 Jan. 2003)
[6] Culp, Scott. "The Ten Immutable Laws of Security Administration." Nov 2000. URL: http://www.microsoft.com/technet/columns/security/essays/10salaws.asp (12 Jan 2003)
[7] "Conclusion." Computer Viruses and "False Authority Syndrome." 2000. URL: http://vmyths.com/fas/fas8.cfm (3 Jan 2003)
[8] Buhler, Rich. "Anatomy of a Rumor." 2002. URL: http://www.truthorfiction.com/anatomy.htm (11 Jan 2003)
[9] "Don't fall for a virus hoax." 23 Nov 1999. URL: http://www.sophos.com/virusinfo/articles/hoaxes.html#prevent (11 Jan 2003)
[10] "Virus Hoaxes." 2003. URL: http://vil.mcafee.com/hoax.asp (3 Jan 2003)
[11] "Hoaxes." Security Response. 2003. URL: http://www.symantec.com/avcenter/hoax.html (4 Jan 2003)
[12] "Hoax Categories." CIAC Hoax Categories. 26 Feb 2001. URL: http://hoaxbusters.ciac.org/HBHoaxCategories.html