Global Information Assurance Certification Paper

Recent Trends in Social Engineering and Hoaxes – Destroy Yourself

(GSEC Practical Assignment Version 1.4)

Shelley A. Waltz

Abstract

The landscape of computer and network security has changed dramatically in the last few years. Throughout the public and private business sectors, as well as in the home, awareness about computer vulnerabilities has grown enormously. As the landscape has changed, so have intruder tactics. Seeing themselves foiled by virus protection software and tighter security on computers, intruders are relying ever increasingly on an easier target and subsequent doorway to destruction - the human being.

We examine the current trends and exploits in social engineering, and how can we protect ourselves against such psychological attacks. We also examine the aggregate costs of such activity as it proliferates on the Internet.

1. Social Engineering

1.1 The Past

Social engineering has existed in the computer environment since the establishment of the Internet. In the last 10 years, the primary focus of such activity has been to gain access to confidential or valuable information unattainable by other means. Passwords, corporate account information, inside information and intelligence regarding a computer network have been primary targets. Armed with such information, a potential intruder had greater success in exploiting and compromising a computer network. Once compromised, the intruder could garner further confidential information or secrets and implement any malicious destruction desired.

The rise in awareness of computer security and vulnerabilities as well as the booming antivirus software industry has changed the playing field dramatically in the last two years. Media reports, popular culture, and personal experience have contributed to this growth in awareness and subsequent precautions and measures to ensure the security of computers and networks.

1.2 The Future

Although the type of social engineering just described still exists, an ever-increasing method of social engineering aimed at a much wider audience has recently proliferated. The nature of the attack is simple and based on time proven social engineering psychology - human fear and the need to be helpful. The focus of these newer attack strategies is to perpetrate a hoax that will cause recipients to respond in ways that self-inflict damage on their computer systems and additionally spread the hoax to new recipients. This sounds remarkably similar to how a computer worm operates. In fact, such virus hoaxes have been described as "nothing more than a manually driven email worm" (Landesman, 2002). Rather than relying on software code to do damage and spread, virus hoaxes rely on a human to do all the work.

A typical of hoax of the human worm type has typically targeted operating system files. Warnings to recipients alert them to check for the existence of particular files on their system and to immediately delete them. Recipients are also warned to alert as many others as possible by forwarding the message. This is a remarkably simple way for a perpetrator to wreak havoc - one needs only to craftily word an email and then let the recipients do the damage.

1.3 The Birth of a New Strategy

Oddly enough, subsequent to investigation, one of the initial hoaxes of this variety turned out to be a result of a mistake made by a well-meaning computer user. The investigation of the *sulfnbk.exe* virus (sulfnbk.exe virus, 2000) that surfaced in April 2001 and achieved rapid success by late May 2001 began when someone's PC became infected with the *Magistr* worm (W32/Magistr@MM, 2001). This worm spread itself through email attachments that were randomly named *exe, bat, com*, or other executable files.

The infected email messages were mailed to recipients in the compromised system's address book. Apparently one of the email messages sent out, named the attachment *sulfnbk.exe*, a file that is a real windows operating system file. The recipient detected the virus using antivirus software and searched his system for the file. Finding the file in a windows operating system directory, he tried to detect a virus in that file rather than the email attachment, and after failing, simply deleted the windows operating system file of the same name on his computer. The recipient then sent a message to all his colleagues telling them to search for the dangerous file and delete it.

The proliferation of this message caused mass hysteria as well-meaning users participated in the propagation. It was translated into many languages and took on a new life as it was rewritten and enhanced by each well-meaning recipient. Lycos listed *sulfnbk.exe* as the second most popular search phrase for the week ending 2 June 2001. The publicity and attention as well as the sheer number of recipients as a result of propagation of this hoax may have given birth to this new use of hoaxes by hackers to cause intentional damage.

2. Other Recent Social Engineering Attacks

2.1 sulfnbk.exe reborn

Early in April 2002, a nearly identical hoax to *sulfnbk.exe* started. Vmyths surmised that a "clueless well-meaning user (not a hoaxter) adapted an old *sulfnbk.exe* alert by simply changing one instruction to look for *jdbmgr.exe* (jdbgmgr.exe virus, 2002). Perhaps this was caused by confusion on the part of a well-meaning user as in the *sulfnbk.exe* hoax, but perhaps it was intentional. One can be sure that intentional hoaxes of this sort will be proliferating. Real hackers will still try the more technical and challenging ways to break into and hack computer systems, but those not so capable will take the easy route.

2.2 Instant Messaging and IRC Chat

A second social engineering attack method that began in midyear 2000 and has proliferated is the chat client exploit (CERT® Incident Note IN-2000-08, Chat Clients and

Network Security, 2000). Instant messaging (IM) and Internet Relay Chat (IRC) networks provide groups of individuals a means to exchange dialog or chat with one another as well as to swap files and pass web addresses. IM and IRC messages entice a user to download free music, antivirus software, pornography, or other software of value to the user. Once downloaded and executed, the software co-opts the system for use as an agent in a distributed-denial-of-service (DDoS) agent. Many times the messages to the chat group are engineered to stimulate fear, by warning of newly discovered viruses detected on the recipient's computer.

As with the virus-warning hoax, this attack relies on a human being to make the decision to download the trojaned software and then to run the downloaded executable software. Reports to CERT/CC as of March 2002, indicate that tens of thousands of systems had been compromised in this manner.

3. Why It Works

3.1 The Ingredients

Why does this mechanism or vector for infecting computers work? Why are humans so easily duped? The psychology involved in producing the correct stimulus to produce the desired response, or the crafting of a working computer hoax is founded in the time proven craft of scammers practiced for centuries. Some of the ingredients of a well-crafted scam or hoax are the following.

- The information in the hoax is real sounding enough to guarantee a high degree of faith.
- The person who sent the hoax is trusted; the message is from a known source.

Technical sounding language is the cornerstone of virus hoaxes. Non-technical persons can easily fall victim to such techno-speak. Paired with the message coming from someone one knows, claiming his or her system has been compromised, such a warning can push a person to panic and act before getting any verification or substantiation as to its validity.

3.2 Victim profiles

Those most susceptible to such attacks are individuals who are not particularly computer literate. Most victims when passing the information on to colleagues and friends act out of a sense of moral duty and a desire to be helpful. Some persons also get a thrill from passing on scandalous or hot news to friends and colleagues – it gives them a sense of power and importance. Additionally, many persons lack a sense of skepticism about information obtained or read on the Internet (Rothke, Ben, 2000). Perpetrators of hoaxes rely on these characteristics and behavior and specifically target these emotions and failings with their craft.

3.3 False Authority Syndrome

But it is not the naive and gullible well-meaning computer user alone who falls prey to such social engineering attacks, it is also those suffering from what has been classified as "False Authority Syndrome" (Computer Viruses and "False Authority Syndrome", 2000). There are many people who speak with authority about computer viruses who have little knowledge and no genuine experience. Such persons feel competent or qualified to discuss such issues because of their job title, expertise in a computer related field, or simply because they use a computer. Persons with inflated credibility can have an extremely damaging effect when their signatures accompany the hoax.

3.4 Loss of Trust

There are other mitigating psychological factors that influence the success of these social engineering attacks. In the recent past, antivirus software has failed to detect newly discovered viruses. As a result, these viruses propagated rapidly, infecting and damaging many systems in a short time. The lack of or lag in detection ultimately caused many users to lose faith in virus detection software. Consequently fearful users are susceptible and vulnerable to hoaxes and warnings about newly discovered viruses from non-authoritative sources. Computer users will fall victim to trusting their eyeballs to detect viruses rather than trusting their antivirus software.

4. The Cost

Hoax virus alerts can have more impact than real viruses and can constitute a huge denial-of-service attack. In addition to consuming the time of help desk staff and system administrators as they try to respond to panicking users, network bandwidth is consumed and mailboxes are loaded with the propagating spam that constitutes the hoax. Additionally, when users self-inflict damage to their own systems by deleting essential operating system files, the cost of repair in system administrators' time and resources skyrockets.

If we access the risk and cost of handling a single hoax were it received by every user on the Internet (Information About Hoaxes, 2002), the amount multiplies significantly. Were everyone on the Internet to receive one hoax message and spend one minute reading and discarding it, the cost would be (assuming a person's time is worth $50/hr. and there are 50 million persons using the Internet), $41.7 million. This does not take into account the cost of the repairing damaged systems of those who acted upon the hoax virus, nor the congestion and loss of productive bandwidth attributed to sending all these messages. The chaos produced by the sending of such messages, the activity on the Internet to verify the hoax, and the loss of productivity all constitute a denial-of-service attack (Harley, David, 1998).

A virus hoax has the ability to multiply rapidly as each person forwards the message on to everyone in his or her address book. If each person sent the message on to 10 other people, by the 6^{th} generation, one million email messages will have been generated. Clearly such hoaxes can be very damaging and enormously costly to an organization and the entire computer user community.

The Internet is the perfect medium for the propagation of hoaxes. The effectiveness of delivering and propagating a hoax or human driven worm on the Internet is what makes it so dangerous. To compound the effects of hoax mail, it has been reported that email spammers and bulk mailers harvest email addresses from such forwarded hoax message headers.

5. How to Recognize a Hoax or Social Engineering Attack

Most hoax messages have three recognizable parts (Information About Hoaxes, 2002):

- A hook - to catch your interest and get you to read the message.
- A warning - about imminent danger if you do not react and respond.
- A request - to warn everyone you know about the danger.

The hook is designed to get one's attention by using words such as "Warning", "Danger", or "Virus Alert". These will get one's attention so one will respond by reading on to the threat. The use of capital letters and exclamations is characteristic and conveys a sense of urgency. The threat is loaded with technical sounding language in order to convince one it is real. Once again, the use of capitals and exclamations heighten the sense of urgency in order to incite panic and rapid response. The request is designed to make one pass the hoax on to others with whom one has email contact. One is made to feel morally obligated to do so and guilty if one fails.

Warnings that have been forwarded many times and do not contain the original signature or a person's name or contact information are indications that the information has questionable validity. Remember also that a successful hoax has technical sounding language and credibility by association with a credible organization or person. One should be alerted by messages asking one to "Send this to everyone you know", or stating, "This is not a hoax". No credible source of virus information would make such statements.

6. How to defend against Social Engineering Attacks

Clearly, questioning the credentials of the authority sending the virus warning is paramount. Users of computer networks need to be educated about whom to trust as an authoritative source of information on such warnings. They also need to know how to trust the authority.

Authoritative sources of information to the users of a network need to be able to identify themselves without compromise to the users they serve. Information from antivirus software companies as well as from network administrators needs to be digitally signed and verifiable. Computer security response teams (CIAC, CERT, ASSIST, NASIRC) all digitally sign their web site warnings and email warnings using PGP. Users must be educated to trust only verifiable sources and to discard information from non-authoritative sources. Upon receiving a warning, users should verify the information with an authoritative source and be instructed to not forward the message.

7. Conclusion

7.1 Awareness and Education

It is essential for users to understand the implications of propagating unsubstantiated warnings and hoaxes. Awareness programs which offer security information and foster security acceptance among individuals in an organization can help prevent many of the existing and future exploits. An internal web site or email listserver can be used to keep users aware of security issues and current social engineering exploits. Stressing to users that they respond only to authoritative information is a necessity and such educational resources can help immensely in accomplishing this goal. Adding language to one's Computer Use Policy to address acceptable behavior in such situations can also help elevate awareness and increase the caution taken by users in their responses.

7.2 Trust and Currency

To reduce the probability of panic and chaos ensuing following the release of virus hoaxes, system administrators, antivirus software vendors, and trusted security information sites need to be on top of things and get information to users before an incident snowballs. Signed email and trusted web sites can do much to allay the fears produced by socially engineered virus hoaxes and provide the user community with a readily available legitimate source for verification. Having a reliable source with very current information is essential in curbing such attacks.

References

Griffith, Eric. "How to Spot a Virus Hoax, Identifying Real Virus Hoax Warnings.", 2002.
URL: http://www.cliffsnotes.com/internet/virus.html

"jdbgmgr.exe virus", 6 July 2002.
URL: http://www.vmyths.com/hoax.cfm?id=275&page=3

Lemos, Robert. "Virus hoax pulls in victims.", 16 May 2002.
URL: http://zdnet.com.com/2100-1105-916204.html

Landesman, Mary. "The Hoax That Cried Virus - Gullible users turn hoaxes into manually driven worms.", 2002.
URL:
http://antivirus.about.com/library/weekly/aa102300a.htm

Landesman, Mary. "Sulfnbk.exe, When Hoaxes Harm.", 2002.
URL:
http://antivirus.about.com/library/weekly/aa051601a.htm

"CERT® Incident Note IN-2002-03, Social Engineering Attacks via IRC and Instant Messaging.", 19 March 2002.
URL: http://www.cert.org/incident_notes/IN-2002-03.html

"Information About Hoaxes.", 2002.
URL: http://hoaxbusters.ciac.org/HBHoaxInfo.html

"sulfnbk.exe virus", 7 June 2001.
URL: http://vmyths.com/hoax.cfm?id=257&page=3

Holland, C.C. "Never be suckered again! How to spot (and sink) an e-hoax.", 8 June 2001.
URL:
http://www.zdnet.com/anchordesk/stories/story/0,10738,2770611,00.html

Coursey, David. "Well-intentioned but stupid: Are you the Net's weakest link?", 1 June 2001.
URL:
http://www.zdnet.com/anchordesk/stories/story/0,10738,2767075,00.html

"W32/Magistr@MM is a combination of a files infector virus and e-mail worm.", 13 March 2001.
URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99040&

Stevens, George. "Enhancing Defenses Against Social Engineering.", 26 March 2001.
URL: http://rr.sans.org/social/defense_social.php

"CERT® Incident Note IN-2000-08, Chat Clients and Network Security.", 21 June 2000.
URL: http://www.cert.org/incident_notes/IN-2000-08.html

"Computer Viruses and "False Authority Syndrome".", 2000.
URL: http://www.vmyths.com/fas/fas1.cfm

Rothke, Ben., "The Growing Problem of Virus Hoaxes.", Information Systems Security, Sep/Oct2000, (Vol. 9, Issue 4): p51-55

Bissett A. and Shipton G., "Some human dimensions of virus creation and infection.", International Journal of Human-Computer Studies, May 2000 (Vol. 52, No. 5): p899-913.

Harley, David. "Re-floating the Titanic: Dealing with Social Engineering Attacks.", 1998.
URL: http://www.sherpasoft.org.uk/papers/eicar98.html

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS