Internet Hoaxes: Is there Danger?
By Jeff Langdon
12 June, 2001

Introduction

Recently, some e-mail users received warnings from friends, instructing them to search their systems for a file that, if found, was a virus. Unfortunately, this file was not a virus but a normal Windows 98 system file.

The Danger

It is my intent to demonstrate that Virus and other Internet hoaxes are more than just a minor nuisance that can basically be ignored. Hoaxes can cause damage in several ways. When users acting with good intention needlessly forward hoax messages, the result could be clogged e-mail systems and wasted bandwidth. Another concern is that users could be lulled into thinking that an attachment in a known hoax wouldn't cause a problem. Therefore, they end up executing the attachment out of curiosity, which results in the execution of a virus. Recently there have been hoaxes that instruct users how to check for and remove a virus from their system. In fact the "infected" files were important system files. It is essential that IT personnel as well as all e-mail users stay informed about Internet hoaxes and how they operate, as well as the potential damage these hoaxes can cause. Users will then be better equipped to spot new hoaxes and respond to them appropriately.

The Hoaxes

Below are some examples of hoaxes that have come out over the years:

Goodtimes

In Late 1994, the Goodtimes virus hoax was sent out warning users about a message that if downloaded and read, would cause damage to their system. Other incarnations of the Goodtimes virus hoax included claims that the FCC was originating the warning. Many corporate & academic email servers crashed in 1995 because this hoax turned into a major chain letter.[1]

Below is the original text from the Goodtimes Hoax message:

> Here is some important information. Beware of a file called Goodtimes. Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by e-mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friends. It may help them a lot.[2]

Some concerned users forwarded the message to numerous users while others replied back to everyone with questions. One thing that is typical of many virus hoaxes is that something impossible is claimed which in this case was that simply opening the message and reading it would infect the users system. This type of impossible claim makes many hoaxes easy to spot but what we see start to happen in later years is that these impossible claims start to be replaced with claims that are somewhat possible. This hoax has been reincarnated several times over the years and is still a threat today.

AOL4FREE

This Virus hoax was started in early 1997. Users were informed that a virus was being spread in a message with the subject "AOL4FREE" which, in certain versions of the hoax, claimed that reading the message would trigger the virus. Other versions of this hoax claimed an attachment contained the virus. This hoax was compounded by publicity about a real program called "AOL4FREE" hack program, which exploited the AOL network into giving extra online time to users. Later that same year, a Trojan was released as AOL4FREE.COM. AOL4FREE.COM deleted files from hard disk of infected systems.

Below is the text of the AOL4FREE hoax message:

> VIRUS ALERT!!!
> DON'T OPEN E-MAIL NOTING "AOL4FREE"
>
> Anyone who receives this must send it to as many people as you can. It is essential that this problem be reconciled as soon as possible. A few hours ago, I opened an E-mail that had the subject heading of "AOL4FREE.COM". Within seconds of opening it, a window appeared and began to display my files that were being deleted. I immediately shut down my computer, but it was too late. This virus wiped me out. It ate the Anti-Virus Software that comes with the Windows '95 Program along with F-Prot AVS. Neither was able to detect it. Please be careful and send this to as many

> people as possible, so maybe this new virus can be eliminated. [3]

As is typical with Virus hoax chain letters, many users forwarded this mail message but once some of the hysteria died down, a non-hoax Trojan was released in a similar message. The potential danger in this example is that any hoax warning related to a threat could be a precursor to a real attack with a real virus. Users might be lulled into a false sense of security that the attachment isn't a threat. Accordingly, they could execute the attachment out of curiosity, which would infect their system.

ELFBOWL.EXE

In late 1999, a game called Elf Bowling circulated the Internet. I received this game and decided to play it after I had scanned it for viruses. It was a whimsical game where Santa Clause used elves as bowling pins. I didn't think much of the game after that until I got the warning from the person that originally sent it to me that the game was infected with a virus. I did some checking and found that the virus warning was in fact a hoax. However, this made me think of the AOL4FREE hoax. If word got out that this game was in fact not infected with a virus, e-mail users might take their guard down and run the ELFBOWL.EXE without bothering to check it. This could make the ELFBOWL.EXE warning a good target for a real trojan or virus.

Sulfnbk.exe

In May of 2001, a Virus Hoax was sent around the Internet advising people that the sulfnbk.exe file was a virus. The hoax further advised those users to search their system for this file and remove it if it existed. The hoax letter even contained step by step instructions for users to follow. Some variants of the hoax also urged users that found this file on their systems to send the warning to anyone they have ever sent e-mail to in the past because they could have been infected also.

Below is the text from the Sulfnbk.exe hoax message:

> Subject: BAD virus - act quickly!!
> Date: Tue, 29 May 2001 21:57:22 -0400
>
> Subject: Please Act Urgently
> VIRUS COULD BE IN YOUR COMPUTER

> It will become activate on June 1st and will delete all files and folders on the hard drive. No Anti-Virus software can detect it because it doesn't become a VIRUS until 1/6/2001. It travels through the e-mail and migrate to your computer.
> To find it please follow the following directions:
> Go To "START" button
> Go to "Find" or "Search"
> Go to files and folders
> Make sure to search in drive C
> Type in; SULFNBK.EXE
> Begin Search
> If it finds it, highlight it and delete it
> Close the dialogue box
> Open the Recycle Bin
> Find the file and delete it from the Recycle Bin
> You should be safe. The bad part is you need to contact everyone you sent ANY e-mail to in the past few months. Many major companies have found this virus on their computers. Whatever you do, DO NOT open the file. [4]

As with many hoaxes, this hoax has the potential to clog up mail servers and bandwidth when it is forwarded. This hoax should also serve as a warning of a new threat in the area of hoaxes. When hoaxes warn of viruses, they frequently make claims that just are not possible. For example, "if you read the e-mail, you will be infected with a virus." However, in this case, the recipient is warned that they may have a virus and if they check, they can find out for sure. Typically, users that check find a file which provides undue credibility to the hoax e-mail. What also helps the credibility of this hoax is the fact that Any executable file has the potential to be infected by a virus and some viruses, like W32.Magistr.24876@mm, which can infect any Windows Portable File, with the exception of .dll files. Future hoaxes could target more critical files, urging users to delete them, thus causing problems just as if a real virus had hit. In other words, Hoaxes may soon be featuring malicious payloads deliberately executed by the unsuspecting user. [5]

The "Hoax" is an attack in much the same way a virus is an attack. While a virus or trojan have machine executable code, hoaxes have user executable "code" in the form of instructions for the user to follow. Most of the time, it is an urgent plea to "forward this e-mail to everyone you know." Recently it was step by step instructions on how to disable (clean) their systems. The attackers go to great lengths to get users to execute the code. Attackers are very convincing and since many hoaxes were forwarded by someone that the users knew, more credibility might be given to the warning than otherwise would.

Defense

It would be helpful if Anti-Hoax software was as readily available as Anti-Virus software. Since hoaxes attack the unsuspecting, uninformed and gullible e-mail users, it is essential that IT personnel inform them about hoaxes so they will know to suspect these types of e-mails. Visit sites like http://www.vmyths.com/, http://www.hoaxkill.com/, and http://hoaxbusters.ciac.org/, which are great sources for more information about Hoaxes. Spotting the hoax isn't too difficult since they frequently use the same type of language:

> -**"THIS IS NOT A HOAX"** (A message that proclaims it is not a hoax should be considered suspect).
>
> -Any language that prompts the recipient to forward the message to many people like "forward this to everyone you know."
>
> -Lots of CAPS as well as multiple exclamation points!!!!!!
>
> -Any lack of outside sources that corroborate the claims in the message. I have seen many hoaxes as well as legitimate virus warnings. The legitimate warnings always have links to major Anti-Virus websites like McAfee.com.

Read this article, http://www.sans.org/infosecFAQ/securitybasics/hoaxes.htm, from the SANS Institute Information Security Reading Room, which provides valuable information related to spotting a virus hoax.

Vmyths.com recommends that you put something fun in an employee newsletter and they even authorize the use of the following:

> Which of these things is not like the others?
>
> 1. *Win a Holiday* computer virus alert
> 2. *Returned/Unable To Deliver* computer virus alert
> 3. *Join the Crew* computer virus alert
> 4. *Word.Concept* computer virus alert
> 5. *Penpal Greetings* computer virus alert
>
> Answer: (4). The *Word.Concept* virus is real. The rest are hoaxes designed to frighten you. Don't panic about a virus alert -- especially if you receive the alert on April Fool's Day. Visit http://hoaxbusters.ciac.org and http://Vmyths.com for more information about computer virus hoaxes. [6]

Hoaxes used to be easy to identify because of the impossible things they frequently claimed. Now some hoaxes make claims that are possible therefore, IT personnel should keep current with the latest hoaxes. IT personnel should also keep e-mail users informed with periodic information about current hoaxes as well as instructions all virus alerts should be forwarded to IT personnel so that it can be verified and acted upon. New employees should also be informed about the virus hoax threat in conjunction with education about virus threats as well.

Conclusion

While most hoaxes seem to be little more than annoying chain letters, which absorb bandwidth as the message propagates around the Internet, there is a threat that shouldn't be overlooked. Hoaxes sometimes carry "payloads" in the form of instructions for unsuspecting users to execute. Hoaxes also can carry "payloads" in the form of real viruses that users might not suspect since it is attached to a "known" hoax. Uninformed E-mail users are typically the targets of these hoaxes. The spread of potentially crippling viruses can be stopped by keeping these users better informed about hoaxes.

References:

[1] Author Unknown, Vmyths.com "Good Times virus." 25 January 2001. URL: http://vmyths.com/hoax.cfm?id=14&page=3 (4 June 2001).

[2] Author Unknown, Hoaxbusters web site. "Malicious Code Warnings: Good Times Virus Hoax." section undated. URL: http://hoaxbusters.ciac.org/HBMalCode.shtml#goodtimes (12 June 2001).

[3] Author Unknown, Hoaxbusters web site. "Malicious Code Warnings: AOL4FREE." section undated. URL: http://hoaxbusters.ciac.org/HBMalCode.shtml#aol4free (12 June 2001).

[4] Author Unknown, Hoaxbusters web site. "Malicious Code Warnings: SULFNBK.EXE Hoax." May 2001. URL: http://hoaxbusters.ciac.org/HBMalCode.shtml#sulfnbk (12 June 2001).

[5] Author Unknown, Vmyths.com "sulfnbk.exe virus." 31 May 2001. URL: http://vmyths.com/hoax.cfm?id=257&page=3 (4 June 2001).

[6] Author Unkown, Vmyths.com "Resources | Reduce the virus hoaxes inside your company ." undated. URL: http://vmyths.com/resource.cfm?id=20&page=1 (12 June 2001).

Author Unknown, Vmyths.com “AOL4FREE Trojan/virus.” 11 November 2000. URL: http://vmyths.com/hoax.cfm?id=31&page=3 (3 June 2001).

Author Unknown, CIAC “H-47a: AOL4FREE.COM Trojan Horse Program Destroys Hard Drives.” 17 April 1997. URL: http://ciac.llnl.gov/ciac/bulletins/h-47a.shtml (4 June 2001).

Les Jones “Goodtimes Virus Hoax Mini Faq.” 12 October 1995. URL: http://www.umich.edu/~wwwitd/virus-busters/hoaxes/goodtimes.html (4 June 2001).

Jeff Henning. “Internet Hoaxes: The Truth is Out There.” 4 September 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/hoaxes.htm (4 June 2001).

Author Unknown, Mcafee.COM website. “AOL4FREE Hoax or What?.” 20 January 2000. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=10558& (4 June 2001).

Mary Landesman. “Sulfnbk.exe, When hoaxes harm.” 16 May 2001. URL: http://antivirus.about.com/compute/antivirus/library/weekly/aa051601a.htm (5 June 2001)

Author Unkown, Sophos.com website. “Virus Info: Elf Bowling.” URL: http://www.sophos.com/virusinfo/hoaxes/elfbowl.html (5 June 2001)

Author Unknown, Symantec website. “W32.Magistr.24876@mm. “ 4 April 2001 URL: http://www.symantec.com/avcenter/venc/data/w32.magistr.24876@mm.html. (5 June 2001)