Global Information Assurance Certification Paper

Chris Couture
GSEC Version: 1.4

How Much Do Virus Hoaxes Really Cost?

Abstract

The purpose of this paper is to demonstrate the real cost associated with virus hoaxes. Unlike viruses, hoaxes do not cause any physical damage to your PC. All damage that occurs is by the hands of the end users. This self-inflicting damage is the result of tricking users into deleting system files. Restoring these deleted system files can become quite costly for an organisation. Since hoaxes do not contain malicious code, they cannot be detected anti-virus software. The most effective way organisations can protect themselves against this threat is through security awareness programs, enforcing effective security policies and content filtering.

Introduction

Most security professionals have protected their networks with anti-virus software and have established methods to ensure the virus definitions are updated at regular intervals. While this may protect their systems against viruses, a primitive form of social engineering can defeat most networks. The social engineering being referred to takes the form of a virus hoax. Two hoaxes have recently used simple yet effective techniques to persuade users into deleting legitimate windows system files. These hoaxes were quite successful in persuading user to delete the files sulfbnk.exe and jdbgmgr.exe because these files supposedly contained a virus. Although these files were not critical, the technique was quite effective in having users self-inflict damage. Someone with basic computer knowledge could very easily modify one of these hoaxes to cause severe damage by simply changing the file name to a critical system file. All major anti-virus companies classify this type of threat as a hoax. These types of hoaxes fall into the same category with false virus warnings and jokes even though they have the potential to cause serious damage.

Most hoaxes are annoyances or warnings of non-existent threats. Hoaxes are often over looked as being practical jokes and harmless. It is just a matter of time before what is labelled as a hoax causes some real damage to an organisation. Security awareness programs and corporate policies should include sections on how to deal with these types of hoaxes and educate users to minimise this potential threat.

A Brief History of Virus Hoaxes

According to www.hoaxbusters.ciac.org, a division of the US department of Energy, computer virus hoaxes have been circulating since about 1988.[1] One of

[1]Hoaxbusters

the first virus hoaxes that began to appear was called 2400 Baud Modem Virus. This hoax claimed modems would cause virus infections. (See appendix) By 1994, the Good Times Hoax (See appendix) began to appear and was very successful. It would resurface somewhat modified every 3 to 6 months and still can be seen today. This hoax was responsible for creating mayhem on mail servers and IT personnel.[2] Since the Good Times hoax all major anti-virus manufactures have included a section of their anti-virus libraries to include a section exclusively for hoaxes.

Many more hoaxes had appeared but all with the similar warnings of fake viruses. Theses all appeared on the hoax listings provided by anti-virus vendors. By early 2001, the first sightings of the Sulfbnk.exe hoax began to appear. This hoax had a different twist and started a new trend. It tempted unsuspecting users to cause self-inflicted damage to their PC's.

The next hoax worth noting that was similar to Sulfbnk.exe hoax was Jdbgmgr.exe hoax, which began to appear in multiple languages almost a year later. This hoax basically accomplished the same thing, which was having users delete system files.

How are Viruses Different from Hoaxes

A virus is defined by Sophos as "The difference between a computer virus and other programs is that viruses are designed to self-replicate (that is to say, make copies of themselves). They usually self-replicate without the knowledge of the user." [3] A PC that contains an active copy of a virus is considered infected.

On the contrary, a hoax does not replicate itself, it requires user intervention to be sent to others and therefore doe not self-replicate. The user has full knowledge of sending it out to all their contacts and usually believes they are being helpful. Hoaxes rely on the users gullibility and their need to help others. One major difference is usually a hoax pleads and warns of a supposed infection while viruses actually infect the users PC without warning and announcing it's presence.

How to Identify a Hoax?

F-secure states "Hoax warnings are typically scare alerts started by malicious people – and passed on by innocent users who think they are helping the community by spreading the warning."[4] Usually IT Professionals can easily identify most of the hoaxes that have been widespread by their tell tale signs. Common hoaxes warning have similar characteristics that a trained eye can detect quite easily. A few of these very common traits are:

[2] Jones, FAQ
[3] Theriault, 1999
[4] F-Secure

- Statements such as send this to everyone you know
- Multiple words in caps and multiple exclamation points
- Stating that McAfee and Norton DO NOT detect this virus
- Claims to be the most dangerous virus ever

A great website which explains how to recognise a hoax in much more detail is: http://www.rbs2.com/choax.htm. [5]

The majority of hoaxes are just bogus warnings meant to waste people's time, waste bandwidth, and use up system resources. The Wobbler hoax, which was quite wide spread, began to appear in October 1999. This hoax warned of the fictional virus Wobbler, which was apparently much worse than the real virus Melissa. At the time the Melissa virus had a lot of media attention and was well known for mass-mailing and infecting word documents. The hoax went further to mention the announcement game from IBM in an attempt to sound genuine.

Another example of a common hoax is the Guts to Say Jesus hoax. This hoax appeared in many different languages and warned of a virus that not many people new about. This time they mentioned IBM and AOL as the authorities that allegedly discovered this fictional virus. It was suppose to erase everything on your hard drive.

These hoaxes warned of false threats and had users forward them to their colleagues. The latest trend seen in virus hoaxes is a little more on the damaging side. Hoaxes have evolved from false warnings to social engineering. This evolution creates a new threat.

SULFBNK.EXE Hoax

On April 17th, 2001, reports of this hoax began to surface. This hoax was first reported in Brazil. The hoax warned of a terrible payload that would remain dormant until June 1st 2001.The hoax encourages users to delete the file sulfbnk.exe because it is supposedly infected with a virus. The file is actually a valid system file. Sulfbnk.exe is a Microsoft Windows 95/98/Me utility that is used to restore long file name.[6] This file is not a critical system file and therefore your operating system will run normally without it installed.[7] The hoax also claimed that no anti-virus software would detect it and of course to email all your friends. For further information, read the Microsoft Knowledge Base article: Description of Sulfnbk.exe and How to Replace the Program File (Q301316)

[5] Stadler, 2002
[6] Symantec
[7] Microsoft

JDBGMGR.EXE  Hoax

Reports of a similar hoax appeared on April 8th, 2002. This one persuaded users into deleting the file Jdbgmgr.exe. Once again this was a valid system file, thankfully not a critical one. The file JDBGMGR.EXE is the Microsoft Debugger Registrar for Java and deleting may cause some Java applets not to run properly.[8] As per Microsoft " If a user has Visual J++ 1.x installed but JDBGMGR.exe is missing, the net result would be that some Java programs wouldn't run. In all other cases, there would be no effect from deleting this file."[9] The unusual icon of this file was a teddy bear (as seen above), made the user feel more confident that this was indeed an infected file. More information on this hoax read the Microsoft Knowledge Base article: Virus Hoax: Microsoft Debugger Registrar for Java (Jdbgmgr.exe) Is Not a Virus (Q322993).

JDBGMGR.EXE Revisited

With all the media attention surrounding and the outbreak of the legitimate virus W32/Bugbear, the jdbgmgr.exe hoax began to resurface on October 8th, 2002. The hoax has been slightly modified and takes advantage of the teddy bear icon. The hoax writer is playing on the name bugbear and associating it with the teddy bear icon. The hoax contains an apology for infecting the user with the bugbear virus and advises the user to delete the file jdbgmgr.exe to eradicate the virus.

The actual W32/Bugbear virus executable has a generic icon  typically associated with EXE files.[10] It is the same hoax but this time it is taking advantage of the confusion and unawareness of the user community surrounding real viruses.

How Are These Two Hoaxes Different

Why would someone spend time writing a virus when they can simply convince users to inflict damage themselves? Both of these hoaxes had naive users delete system files. This form of social engineering preys on people's fear of computer viruses. This differs from the fake virus warnings, which usually just ask the user become a mass mailer. This is achieved by having the user send an email of the false threat to everyone they know. Both the above hoaxes requested users mass mail as well but also included detailed instructions on how to remove specific files. These two hoaxes simulate the behaviour of some common viruses today, except there is absolutely no programming involved. The user community innocently performs all the tasks that a common virus would.

[8] Symantec
[9] Microsoft
[10] NAI

Since no program is executed to spread these the difficulty in slowing the spread of these hoaxes becomes tricky. Many users are also to embarrassed to admit they were fooled by a hoax and are not easily willing to admit deleting system files which actually hinders recovery time.

The Potential Threat

All major Anti-virus companies classified the two hoaxes this paper focuses on in the same category as all the other hoaxes. The classification of these two threats as a hoax is quite misleading. McAfee warns ”virus hoaxes are more than mere annoyances, as they may lead some users to routinely ignore all virus warnings, leaving them vulnerable to a genuine, destructive Virus.”[11] While this may very well be true, a hoax is usually just a false warning of a non-existent virus. These hoaxes while taking using up email resources and taking away from user and IT personnel productivity still are not destructive by nature. When users start deleting files on there own is when the danger begins. Could you imagine the impact of users being instructed to delete critical entries in the registry? The most common anti-virus software programs search for virus signatures to determine if files are infected, while this works effectively in detecting viruses when virus signatures are up to date, they do not protect against hoaxes. When a threat is labelled as a hoax the perception of the seriousness of the threat is greatly reduced. Hoaxes are usually just false alarms or jokes and not normally thought of as a form social engineering causing real harm.

The Cost of Hoaxes

It appears that no valid metrics have been in place to measure the full impact and cost virus hoaxes can have to an organisation. Statistic such as www.Hoaxbusters.ciac.org claim outrageous expenses generated by hoaxes with the following formula:

“If everyone on the Internet were to receive one hoax message and spent one minute reading and discarding it, the cost would be something like

50,000,000 people *1/60 hour * $50/hour = $41.7 million”[12]

There are obvious flaws in this formula, not everyone reading email is at the office and getting paid while they read emails. The estimate if 1 minute per email is also a little high. This calculation was used more to illustrate the potential cost that hoaxes could generate if everyone forwarded them to everyone in their address book. Most IT Professionals should be able to see a hoax without looking it up should be on list supplied by vendors. It is the time answering the calls and emails of concerned user, which consumes the time of

[11] NAI
[12] Hoaxbusters

the IT Professional.

Using the Spam calculator found at www.cmsconnect.com although not perfect for hoaxes can make a more reasonable calculation. When the following data was enter in the calculator: 100 employees, 230 working days, 25$ average salary, 2 Spams received daily, 5 seconds wasted per Spam.
The results were:
Cost to Corporation: $1597.22 yearly, $6.94 daily, 101.39 hours wasted yearly
Cost for each employee: $15.97 yearly, $0.07 daily, 1.01 hours wasted yearly[13]

This could represent the cost associated with user dealing with hoaxes although it does not include the cost of restoring deleted files.

What are the real cost of hoaxes? As stated earlier an IT Professional should be able to filter out most hoaxes without looking them up in Anti-Virus vendor websites. Most IT professionals who work with Anti-Virus products are on or should be on a mailing list provided by the vendor which provide a list of all new virus threats which also includes hoaxes. The time wasted by IT staff looking up potential virus threats is minimal.

Cost begins to be a factor when help desks begin to receive calls from user who have deleted files as seen in the two hoaxes described earlier. In the early stages it is unknown to most the full impact of having deleted certain system files. Until some testing is completed, restoring the files can be costly. If an organisation does not have software solutions to push files to workstation, a technician must be sent to the workstation to restore the files. This is where cost start to add up in most cases. Usually with 24- 48 hours the full impact of deleting the files mentioned in the hoax is understood by the vendors. It 's usually only the first day when cost will be generated restoring files.

Another cost that can occur from hoaxes being forwarded to customers is to ones reputation and credibility. Graham Cluley, senior consultant at the Anti-Virus firm Sophos states, " a company's name is often tarnished if it is linked with a hoax email". [14] There is a cost associated to a company's integrity when a virus hoax is forwarded from one of its email addresses.

Educating Users to Reduce Costs

The first step in fighting hoaxes is to establish a security awareness program. If one already exists it is important to have a section dedicated to hoaxes. An effective security awareness program should have a number of different methods to get the message out. Effective programs include entertaining and mandatory sessions. Having a marketing campaign with videos, posters and employee rewards for attending can be effective. It is also important that the

[13] Computer Mail Service
[14] Sophos

information being distributed is up to date and revised often to ensure it is still relevant. Security briefings should at least be given every quarter to make certain the information is still fresh and in the minds of the user community. Creating an effective security awareness program is beyond the scope of this paper, more information on poster, videos, screen savers, and effective security awareness can be found at www.securityawareness.com.[15] Below are some hoax related solutions that can cut cost and be incorporated into an awareness program.

One way of reducing cost is to have a central location for user to verify hoaxes themselves. This can be accomplished by setting up an intranet site with common virus hoaxes listed. This can contain links to other hoax sites that the majority of the anti-virus vendors have on their websites. Most anti-virus vendors allow their virus and hoax libraries to be mirrored. Be sure to verify with your vendor before doing so. This way the email is not sent out to IT personnel and the users stop the hoax themselves.

Another method is to set up a centralized mailbox and have all users send virus warnings and hoaxes to one location. More than one person can monitor this mailbox reducing emails being sent to the entire IT department. Sharing in the task of responding to theses emails is also shared and form letters can be created to answer them eliminating some of the time wasted answering the same type of email over and over. The response can also include the link to the intranet site to encourage users to look them up on their own.

An additional effective way of reducing users from deleting files is to have a general broadcast system in place. If a new threat is discovered, a broadcast can be sent out to all users requesting them not to start deleting files. This may create some email traffic itself by sending the warning of the hoax to everyone, but at least users will be use to having the notification of threats come from one authority and not anyone who sends them an email. The users soon begin to realise if it is a real threat IT would have already warned them and would be taking corrective actions to minimise the damage.

If an intranet site is available, educating users how to spot a virus hoax can be helpful. By making information on how to spot a hoax public to everyone in the company, this would greatly reduce the calls and emails to IT personal t have to answer. The more information made available to the user community the better. Once the user is educated on the common characteristics seen in most virus hoaxes, the productivity loss is reduced to just a user deleting an email.

Using Software to Reduce Costs

Relying on people alone to reduce the cost generated by virus hoaxes, due to human nature is not effective enough. There are several ways that software can be used to eliminate virus hoaxes and viruses for that matter. The initial cost of purchasing software may be expensive but often they can be used to address

[15] Security Awareness

different issues, such as Spam.

One method often recommended by anti-virus vendors is to protect the network at multiple levels. If the mail gateway is scanning for viruses, it also may be able to content filter. Blocking emails containing the text sulfbnk.exe will not disrupt legitimate business email. No business related email would contain the text string sulfbnk.exe that I am aware of. Even if the content filtering is restricted to the subject line, you could filter out quite a few by blocking common subject lines. Even if the mail gateway is not scanning for viruses, some email gateways have some form of content filtering as a feature. It just may not be being used or is not turned on.

Commercial content filtering programs are widely available. These programs will not only filter out virus hoaxes from entering your network but also a lot of Spam. This alone may justify the cost of purchasing content filtering software. Calculations done with the Spam calculator show reasonable costs associated with reading and deleting Spam. By reducing the amount of Spam you could easily eliminate your hoaxes from being circulated as well.

Another method is to lock down workstations protecting them against the user causing unnecessary damage. Depending on the environment a couple of options exist. If Group Policies can be applied then setting folder permission on Windows 2000 and XP workstations can be applied. This would eliminate the users ability to delete system files. If windows NT is being used a script can be written and activated with the logon script to change the folder permissions to protect key system folders such as the c:\winnt folder. If an older operating system is in use with limited security functionality, selecting “hide files of these types” in the options of windows explorer will hide files with certain extensions. This will not eliminate the problem completely but may prevent the user deleting system files they cannot see.

Security Policy

The best way to handle hoaxes is to include a section on them when addressing viruses or email in the security policy. This way the actions and procedures are available to everyone in the company and all the ideas above can be implemented into the security policy. Users can be referred to the policy for such issues and free up the IT personnel for duties. Security policies should be able to encompass all the cost saving techniques discussed. A security policy needs to be seen to be enforced. It is important that the security policy be part of any awareness program. Many papers on writing and deploying effective security policies can be found in the SANS reading room.

Conclusion

Although no accurate metrics exist to determine the cost of hoaxes have on companies, this paper clearly points out some areas where costs can occur. Settings up an effective security policy and security awareness program are

essential to reduce the cost encountered when dealing with virus hoaxes. If the trend continues and social engineering is causing users to self inflict damage cost surrounding hoaxes will only rise. The next time a hoax is posted by an Anti-Virus vendor, take the time to read it, it may just be instructing your user to delete key files and end up costing more than any virus infection. Be aware that hoaxes are sometimes more than just a joke or false alert.

References

About, "The Hoax that cried Virus"
http://antivirus.about.com/library/weekly/aa102300a.htm

About, "Excuce me, How much did your Virus cost?"
http://antivirus.about.com/library/weekly/aa100600a.htm

Computer Mail Services, "The Cost Of Spam"
http://www.cmsconnect.com/Marketing/spamcalc.htm

F-Secure, "Hoax Warnings" http://f-secure.com/virus-info/hoax/

Griffith, Eric, "How to Spot a Hoax" http://www.cliffsnotes.com/internet/virus.html

Heikkila, Pia, " Why Virus Hoaxes are No Joke"
http://www.silicon.com/DigitalBlunders/virus_hoaxes.htm

HoaxBusters , "Welcome to the CIAC Hoax Pages" 09/16/2002.
http://hoaxbusters.ciac.org/HoaxBustersHome.html

Hymes,Charles, "Anti-Hoax Advice"
http://www.nonprofit.net/hoax/advice/advice.html

Jones, Les ,"Good Times FAQ" 27/04/95. http://www.informatik.uni-trier.de/~bern/GoodTimes-Hoax/FAQ.html

Lee, Andrew, "Email Virus Hoaxes" http://www.claymania.com/hoaxes.html - cost

Microsoft, "TechNet - Hoaxes" http://microsoft.com/technet/

NAI, "Hoaxes" http://vil.nai.com/VIL/hoaxes.asp

Panda, "Hoax and Jokes" http://www.pandasoftware.com/library/hoax.htm

Security Awareness Inc. "Protect IT: End User Awareness Workshop"
http://securityawareness.com/protect.htm

Sophos, "Don't Fall for a Virus Hoax"
http://www.sophos.com/virusinfo/articles/hoaxes.html - cost

Stradler, B. Ronald "Computer Virus Hoaxes" 06/15/2002
http://www.rbs2.com/choax.htm

Sturgeon, Will, ”Resources Drained by Email Hoaxes” 04/09/02
http://zdnet.com.com/2100-1105-956504.html

Symantec, “Hoaxes” http://securityresponse.symantec.com/avcenter/hoax.html

Theriault,Carole, ”An Introduction to Computer Viruses” October 1999.
http://sophos.com/virusinfo/whitepapers/videmys.html

TruSecure, “Hype or Hot” http://trusecure.com/knowledge/hypeorhot/

Appendix 1 – Examples From Actual Email Hoaxes (taken from Nai.com)

2400 Baud Modem Hoax

SUBJ: Really Nasty Virus

AREA: GENERAL (1)

I've just discovered probably the world's worst computer virus yet. I had just finished a late night session of BBS'ing and file

treading when I exited Telix 3 and attempted to run pkxarc to unarc the software I had downloaded. Next thing I knew my hard

disk was seeking all over and it was apparently writing random sectors. Thank god for strong coffee and a recent backup. Everything was back to normal, so I called the BBS again and downloaded a file. When I went to use ddir to list the directory, my hard disk was getting trashed again. I tried Procomm Plus TD and also PC Talk 3. Same results every time. Something was up so Ihooked up to my test equipment and different modems (I do research and development for a local computer telecommunications company and have an in-house lab at my disposal). After another hour of corrupted hard drives I found what I think is the world's worst computer virus yet. The virus distributes itself on the modem sub-carrier present in all 2400 baud and up modems. The sub-carrier is

used for ROM and register debugging purposes only, and otherwise serves no othr (sp) purpose. The virus sets a bit pattern in one

of the internal modem registers, but it seemed to screw up the other registers on my USR. A modem that has been "infected" with

this virus will then transmit the virus to other modems that use a subcarrier (I suppose those who use 300 and 1200 baud modems

should be immune). The virus then attaches itself to all binary incoming data and infects the host computer's hard disk. The only

way to get rid of this virus is to completely reset all the modem registers by hand, but I haven't found a way to vaccinate a modem

against the virus, but there is the possibility of building a subcarrier filter. I am calling on a 1200 baud modem to enter this

message, and have advised the sysops of the two other boards (names withheld). I don't know how this virus originated, but I'm

sure it is the work of someone in the computer telecommunications field such as myself. Probably the best thing to do now is to

stick to 1200 baud until we figure this thing out.

Good Times

PLEASE READ THE MESSAGE BELOW !!!!!!!!!!!!

Some miscreant is sending email under the title "Good Times" nationwide, if you get anything like this, DON'T DOWN LOAD THE FILE!

It has a virus that rewrites your hard drive, obliterating anything t. Please be careful and forward this mail to anyone you care about. Te FCC released a warning last Wednesday concerning a matter of major importance to any regular user of the Internet. Apparently a new computer virus has been engineered by a user of AMERICA ON LINE that is unparalleled in its destructive capability. Other more well-known viruses such as "Stoned", "Airwolf" and "Michaelangelo" pale in comparison to the prospects of this newest creation by a warped mentality. What makes this virus so terrifying, said the FCC, is the fact that no program needs to be exchanged for a new computer to be infected. It can be spread through the existing email systems of the Internet.

Once a Computer is infected, one of several things can happen. If the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop -which can severely damage the processor if left running that way too long. Unfortunately, most novice computer users will not realize what is happening until it is far too late. Luckily, there is one sure means of detecting what is now known as the "Good Times" virus. It always travels to new computers the same way in a text email message with the subject line reading "Good Times". Avoiding infection is easy once the file has been received simply by NOT READING IT! The act of loading the file into the mail server's ASCII buffer causes the "Good Times" mainline program to initialize and execute.

The program is highly intelligent - it will send copies of itself to everyone whose email address is contained in a receive-mail file or a sent-mail file, if it can find one. It will then proceed to trash the computer it is running on.

The bottom line is: - if you receive a file with the subject line "Good Times", delete it immediately! Do not read it" Rest assured that whoever's name was on the "From" line was surely struck by the virus. Warn your friends and local system users of this newest threat to the Internet! It could save them a lot of

time and money.

Could you pass this along to your global mailing list as well?

Guts to Say Jesus

VIRUS WARNING !!!!!!!

If you receive an email titled "It Takes Guts to Say 'Jesus'" do NOT open it. It will erase everything on your hard drive.

This is a new, very malicious virus and not many people know about it. This information was announced yesterday morning from IBM; please share it with everyone that might access the internet. Once again, pass this along to EVERYONE in your address book so that this may be stopped.

Also, do not open or even look at any mail that says "RETURNED OR UNABLE TO DELIVER."

This virus will attach itself to your computer components and render them useless. Immediately delete any mail items that say this. AOL has said that this is a very dangerous virus and that there is NO remedy for it at this time. Please practice cautionary measures and forward this to all your online friends ASAP

JDBGMGR.EXE

I found the little bear in my machine because of that I am sending this message in order for you to find it in your machine. The procedure is very simple:

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

The virus can be cleaned before it deletes the files from your system. In order to eliminate it, it is just necessary to do the following steps:

1. Go to Start, click "Search"

2.- In the "Files or Folders option" write the name jdbgmgr.exe

3.- Be sure that you are searching in the drive "C"

4.- Click "find now"

5.- If the virus is there (it has a little bear-like icon with the name of jdbgmgr.exe DO NOT OPEN IT FOR ANY REASON

6.- Right click and delete it (it will go to the Recycle bin)

7.- Go to the recycle bin and delete it or empty the recycle bin.

IF YOU FIND THE VIRUS IN ALL OF YOUR SYSTEMS SEND THIS MESSAGE TO ALL OF YOUR CONTACTS LOCATED IN YOUR ADDRESS BOOK BEFORE IT CAN CAUSE ANY DAMAGE.

SULFBNK.EXE

A VIRUS could be in your computer files now, dormant but will become active on June 1. Try not to USE your Computer on June 1st. FOLLOW DIRECTIONS BELOW TO CHECK IF YOU HAVE IT AND TO REMOVE IT NOW. No Virus software can detect it. It will become active on June 1, 2001. It might be too late by then. It wipes out all files and folders on the hard drive. This virus travels thru E-mail and migrates to the 'C:\windows\command' folder. To find it and get rid of it off of your computer, do the following.

Go to the "START" button.

Go to "FIND" or "SEARCH"

Go to "FILES & FOLDERS"

Make sure the find box is searching the "C:" drive.

Type in: SULFNBK.EXE

Begin search.

Wobbler

Thought you might be interested in this message. If you receive an email with a file called "California" do not open the file. The file contains the "WOBBLER" virus.

This information was announced yesterday morning by IBM. The statement says that ... "This is a very dangerous virus, much worse than 'Melissa' and there is NO remedy for it at this time. Some very sick individual has succeeded in using the reformat function from Norton Utilities causing it to completely erase all documents on the hard drive. It has been designed to work with Netscape Navigator and Microsoft Internet Explorer. It destroys Macintosh and IBM compatible computers. This is a new, very malicious virus and not many people know about it at this time."

"Please pass this warning to everyone in your address book and share it with all your online friends ASAP so that the destruction it can cause may be minimized."