SCOUTS-L

VIRUS ALERTS

Date: Sat, 24 Jun 1995 23:12:07 -0400 (EDT)
From: "Michael F. Bowman" <mfbowman@capaccess.org>
Subject: Re: VIRUS ALERT
To: Bill Case <billcase@romulus.ncsc.mil>

Bill,

Thanks for the comeback. Now you really have my attention - I am an AOL user and recently updated WINCIM with one of their mailed disks. Sounds like I could be in trouble. Please advise of the virus again and symptoms, cures, etc. to the extent that you know.

Speaking only for myself in the Scouting Spirit, Michael F. Bowman
Prof. Beaver, Nat. Capital Area Council, BSA mfbowman@CAPACCESS.ORG

Date: Tue, 27 Jun 1995 00:26:54 -0400 (EDT)
From: "Michael F. Bowman" <mfbowman@capaccess.org>
Subject: VIRUS ALERT - ABOUT THE RUMOR

Two people recently alerted the list to a suspected virus on disks being distributed by an online service, providing only sketchy details, prompting requests for more information. The rumor they were responding to was that disks distributed by America Online (AOL) were contaminated with a "Burp" virus.

I checked with AOL's Telecommunications/Security Forum for information. Two users related that friends had experienced a virus on software distributed by AOL. In both cases the users were alleged to have regularly checked their disks for viruses (some stealth viruses disable Central Point and Microsoft V-Safe, which means that the checking may not have been reliable), and that both users after booting, entering windows, and accessing AOL were presented with a large AOL Icon just before their systems locked up. When they rebooted, they allege that their systems were wiped out. All of this is second hand information and there has not been independent confirmation.

AOL has responded to inquiries on this subject by saying that it has tried to verify this information, but that so far all they can find are rumors. AOL is aware of the rumor, but maintains that it has not been able to find

this virus on its system, in its files or in distributed disks. AOL also advises that it checks all of its files and disks for viruses. They do caution that they cannot check files users download via e-mail or through internet connections provided by AOL (where AOL does not control the files).

Now before anyone jumps all over the two members of our list who related the rumor to us, remember that they were acting out of genuine concern for
the computer health of their fellow Scouters - trying to alert us to what might be a problem. They were sketchy in their descriptions, because they had been told they could be sued for naming names. I'm not sure this is much protection, as the other online services could also be affected by a non- specific rumor and have the same reason to be aggravated. Fortunately most services are eager to track down viruses, are concerned not to ship contaminated products, and just as eager to stop rumors that could hurt their businesses. Once a rumor gets circulated it can cause them just as much damage as a virus. Of course, if you are on the receiving end, it gets a little more personal when your computer dies and its a little late to find out at that point. AOL will continue to check into this one. At this point all that can be confirmed is that there is a rumor and that it has not yet been substantiated by first hand knowledge.

Information concerning this rumor can be found on AOL's tele-communications/security forum. For those who are on AOL and have concerns, please use that forum to check for information or to relate information.

For those new to this list and new to computers, this might be a good time to suggest that it is always a good practice to keep a backup of critical files (even if you still have the original program disk); e.g. .ini, .grp, and other files that you have customized or added in windows and your other primary programs. Similarly, it is a good practice to use an anti-virus program to check all new stuff that you add to your hard drive before you run it.

Speaking only for myself in the Scouting Spirit, Michael F. Bowman
Prof. Beaver, Nat. Capital Area Council, BSA mfbowman@CAPACCESS.ORG

From mfbowman@CapAccess.org Fri Nov 24 01:53:55 1995
Date: Fri, 24 Nov 1995 01:53:53 -0500 (EST)

From: "Michael F. Bowman" <mfbowman@CapAccess.org>
To: SCOUTS-L - Youth Groups Discussion List <SCOUTS-L@TCUBVM.IS.TCU.EDU>
cc: Multiple recipients of list SCOUTS-L <SCOUTS-L@TCUBVM.IS.TCU.EDU>
Subject: Information on "Good Times" Virus & AOLGOLD
In-Reply-To: <Pine.A32.3.91.951123223004.8593E-100000@voyager.bxscience.edu>
Message-ID: <Pine.SUN.3.91-FP.951124014404.6144A-100000@cap1.capaccess.org>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII
Status: RO
X-Status:

Uri,
You have been the victim of a hoax that has taken in Government agencies and many corporations, that should have known better. Just as destructive as a virus are the efforts of twisted minds that perpetrate these hoaxes aimed at harming the public confidence in a particular online service and which costs untold financial losses from lost subscribers. Most of these hoax type messages are passed without any verification information, which should be a clue. In any case, the only responsible way to handle such postings is to check them out, before passing them on to large groups.

America Online (AOL) and Compuserve maintain excellent information on virus problems that can be accessed by the keyword "virus" and I suspect that Prodigy does as well. I checked with AOL to see what I could find. The following was copied directly out of AOL's Virus Information Center and pertains to the "Good Times" Hoax and the real AOLGOLD Virus. At the end there is a contact point for Symantec Corp. where anyone can call for virus information for free.

——-----

The Good Times email virus is a hoax!
If anyone repeats the hoax, please show them the FAQ.

Good Times Virus Hoax

Mini FAQ

by Les Jones
macfaq@aol.com
lesjones@usit.net

October 12, 1995

A FAQ, if you're new to the Internet, is a document that answers Frequently Asked Questions. This Mini FAQ is a summary of, and a reference to, the full FAQ, which has much more information about this and other hoaxes. Instructions for retrieving the full FAQ are at the end of this message. The Mini FAQ is short enough for faxes, message boards, company memos, and people with short attention spans.

Is the Good Times email virus a hoax?

Yes. It's a hoax.

America Online, government computer security agencies, and makers of anti-virus software have declared Good Times a hoax. See Online References at the end of the FAQ.

The hoax has been around since at least November of 1994. Since that time, no copy of the alleged virus has ever been found, nor has there been a single verified case of a viral attack.

I'm new to the Internet. What is the Good Times virus hoax?

The story is that a virus called Good Times is being carried by email. Just reading a message with "Good Times" in the subject line will erase your hard drive, or even destroy your computer's processor. Needless to say, it's a hoax, but a lot of people believed it.

Some of the companies that have reportedly fallen for the hoax include AT&T, CitiBank, NBC, Hughes Aircraft, Texas Instruments, and dozens or hundreds of others. There have been outbreaks at numerous colleges.

The U.S. government has not been immune. Some of the government agencies that have reportedly fallen victim to the hoax include the Department of Defense, the FCC, and NASA.

The full Good Times Virus Hoax FAQ has more information about the origins of the hoax, and variations on the text of the hoax.

What was the CIAC bulletin?

On December 6, 1994, the U.S. Department of Energy's CIAC (Computer Incident Advisory Capability) issued a bulletin declaring the Good Times virus a hoax and an urban legend. The bulletin was widely quoted as an antidote to the hoax. The original document can be found at the address in Online References at the end of the mini FAQ, and is included verbatim in the full FAQ. CIAC issued another bulletin on April 24, 1995 to reiterate that Good Times is a hoax.

Online References

CIAC Notes 94-05 95-09, and especially 94-04

FTP to ciac.llnl.gov and look in the pub/ciac/notes directory. The URL is ftp://ciac.llnl.gov/pub/notes/

The URL for the CIAC home page on the World Wide Web is http://ciac.llnl.gov/ciac/

America Online's official statement

Keyword "virus2" on America Online

Where can I find the complete Good Times Virus Hoax FAQ?

Via FTP:
FTP to usit.net and look in the pub/lesjones directory. The URL is
ftp://usit.net/pub/lesjones/good-times-virus-hoax-faq.txt
ftp://users.aol.com/macfaq/good-times-virus-hoax-faq.txt

On the World Wide Web:
http://www.tcp.co.uk/tcp/good-times/index.html -- excellent hypertext
http://www.singnet.com.sg/staff/lorna/Virus -- lots of virus info
(Note: the V must be capitalized.)

On America Online:
the file libraries at keyword "virus"

by email:
send email to archive@xconn.com with REQUEST GT_VIRUS.TXT in the subject line.

Note: You can find the full FAQ in the "Miscellaneous Text" Library in the PC Telecom Forum (Keyword: PTC

____

AOLGOLD

November 14, 1995

Dear Member:

As you know, we strive to keep you informed on various issues regarding online safety.

We want to take this opportunity to remind you about potential computer viruses and Trojan horses and how to protect your computer. First, a virus is a program that is designed to spread and usually attaches itself to a program with the goal of spreading to other computers. A Trojan horse is a program that is intended to corrupt your computer but has to be activated before it can be executed. For example, a Trojan horse can be distributed as an attached file to an email but the file has to be downloaded and executed before harm is done.

If you receive email from unknown senders with an attached file, it is a good rule of thumb not to download the files. In addition, if you ever receive a file in email you believe could cause problems, please forward it immediately to TOSEMAIL1, and explain your concerns to our Terms of Service staff.

We have received recent inquiries regarding a Trojan horse that is sent as an attached file in an email message entitled "AOLGOLD" and "Install.exe". It is important to understand that no virus or Trojan horse can be passed along by simply reading email. However, we strongly urge that if you receive email with an attached file with this name not to download it.

Due to the private nature of electronic mail, we cannot scan files in email for viruses as we do with files in public areas of the service.

We have never had an occurrence of a virus or Trojan horse being spread through simply reading email. In order for one to spread to your computer, you would have to proactively select the attached file and download it to your hard drive. It is therefore advisable never to download attached files from an unknown sender.

AOL incorporates virus protection throughout the service and scans all posted software, text, and sound files in public areas. We also offer our members the Virus Information Center on AOL where you'll find information
about the latest virus or Trojan horse, along with updates to all the popular commercial, shareware, and freeware anti-virus tools. Keyword: VIRUS.

Thank you for taking an active role in maintaining a safe online environment.

Sincerely,
AOL Operations Staff

The AOLGOLD virus is a Trojan Horse virus that is intended to erase most of your system files. America Online's Terms of Service Department tested and verified it's capabilities, after a member who had received it reported it to us.

AOLGOLD.ZIP contains an install file, INSTALL.EXE, which when run,

expands into the following:

ADRIVE.RPT
ANNOY.COM
DOER.DO
DOOMDAY.EXE
INSTALL.BAT
INSTALL.EXE
SLOWER.ZZ
SUSPEND.DRV
VIDEO.DRV

When INSTALL.BAT is initialized (by rebooting your computer) it renames VIDEO.DRV to VIRUS.BAT. The next time the computer is rebooted, VIRUS.BAT
begins it's job of deleting all files on the computer's C:\ drive, in alphabetical and numerical order.

We recommend that ANY EMAIL YOU RECEIVE WITH THE AOLGOLD.ZIP FILE
ATTACHED BE FORWARDED TO THE TERMS OF SERVICE DEPARTMENT AT SCREEN NAME
"TOSEMAIL1", THEN IMMEDIATELY DELETED FROM YOUR "MAIL YOU'VE SENT" AND
"MAIL YOU'VE READ" MAILBOXES by selecting the "delete" button on your email list window.

PLEASE DO NOT DOWNLOAD OR EXECUTE THIS FILE. (The AOLGOLD FILE, not this
Scouts-L e-mail)

Subj: New Virus Hotline
Date: 95-11-21 20:42:12 EST
From: SymMichael

NEW ANTI-VIRUS HOTLINE SERVICE

The new Symantec Anti-Virus HotLine can be accessed for the price of a
phone call by calling (541) 9VIRUS9, (984-7879) Monday through Friday

between the hours of 7:00 a.m. and 4:00 p.m. PDT.

This revolutionary new service will place live anti-virus technicians at your finger tips to quickly and efficiently help you resolve those burdensome live virus infection situations, no matter what product you are using to detect the virus.

To help you in your fight against virus infections Symantec is proud to introduce the industry's first dedicated anti-virus hotline.
As computer viruses become more diverse and increasingly difficult to deal with without expert help, the amount of time and money spent on resolving viral infection situations is increasing.

Speaking only for myself in the Scouting Spirit, Michael F. Bowman
DDC-Training, GW Dist. Nat Capital Area Council
mfbowman@CAPACCESS.ORG

Date: Fri, 22 Dec 1995 09:00:00 EST
From: "Smith Kevin S." <SMITHKS@WLMPO2.WILM.GE.COM>
Subject: Mail Bomb { A Reply}

I was just talking to some teachers at work today and was told that there is a new virus out that attacks through e-mail. Supposedly it is
worse
for Macs but it attacks IBM also and really trashes the memory. They have recommended downloading nothing and reading mail only from people you know.
Has anyone else heard this?!!!

Jim Deroba
ASM

This is a HOAX,
AOL has a team of software experts that have debunked this story several times this year. Also articles have appeared in the following magazines I-Way & NetGuide. Allaying the fears of Mail introduced Viruses, THEY ARE NONE EXISTENT.
Mail Bombing on the other hand is very common on AOL. Most AOL users have probably come across Hacker's using a program called AOHELL 3.1. that program is capable of sending up to 2000 pieces of mail to one user { it duplicates the original message } It takes forever to delete a mail bomb because it also disables the AOL Delete all function.

Other things to be wary of with AOHELL 3.1 users.,
They have the capability to duplicate your on-line Sign on Name.
They have access to your account info { Everything but your password }
NEVER give your Password out to anyone Especially any user who claims to be a
AOL staffer. AOL will never ask you for your password.

How to spot a AOHELL 3.1 user :
They are usually very Egotistical, they like folks to know they have the power to make your On-line time HELL. they use screen names like " YPAY2PLAY" <----------- Why Pay To Play. because they are charging time to someone else's account IT COULD BE YOURS.
They Scroll Continually. { AOHELL overrides the AOL 3 line limit }
They are always Abusive and they continually SHOUT { Type in CAPS }.

For those of you who have never encountered a AOHELL user this is what they can do to you in a Chat room.

CuBMasters : Greetings fellow Scouters
Scout123 : Hi Cubmasters how are you today
CuBMasters : Stick it up your BUTT WIMP. <----------- This line was not sent from CuBMaster it is an AOHELL user starting a Fight

As you can see from the above example the AOHELL user has just caused some major problems for CuBMasters. { if this happens to you IM the recipient of the Abuse, explain that you did not type the line , and then sign OFF.}

Sorry for this Long Post But I know a lot of you are AOL users

Kevin S. Smith
ACM Pack 234 Cape Fear Council NC

Date: Wed, 29 May 1996 00:07:15 -0400 (EDT)
From: "Jeffrey M. Schweiger" <jschweig@opnav-emh.navy.mil>
Subject: c4i-pro New Virus (fwd)

FYI.

Jeff

Date: Tue, 28 May 1996 15:36:18 -0400
From: Neal Pollock <pollockn@smtp-gw.spawar.navy.mil>
To: c4i-pro@azure.stl.nps.navy.mil
Subject: c4i-pro New Virus

pollockn@smtp-gw.spawar.navy.mil (Neal Pollock)
Subject: NEW VIRUS!
Importance: High

ATTENTION FOLKS!!
A new Windows virus has been reported.. It is called the "Tentacle" virus.
It apparently originated from the internet on the alt.cracks   newsgroup, attached to a posted file called DOGZCODE.ZIP. It is a direct   action virus which infects Windows programs.
Each time an infected program is run, one file in the current directory becomes infected, followed by two files in the Windows directory.
The payload acts between midnight and quarter past midnight. A program that becomes infected within this time has it's standard icon changed to an icon of a tentacle. This change is not immediately obvious. It is not until you attempt to change the icon, delete icons in the program group and attempt to replace them, or if you run and minimize the program
that the tentacle icon will display itself.
It is not know as of now whether the IBM Anti-virus program will detect (or clean) this virus. We are attempting to confirm this now. PLEASE DO NOT OPEN ANY FILE NAMED DOGZCODE.ZIP!!