From: Kenneth R. van Wyk (The Moderator) <krvw@CERT.SEI.CMU.EDU>
Errors-To: krvw@CERT.SEI.CMU.EDU
To: VIRUS-L@IBM1.CC.LEHIGH.EDU
Path: cert.sei.cmu.edu!krvw
Subject: VIRUS-L Digest V4 #76
Reply-To: VIRUS-L@IBM1.CC.LEHIGH.EDU

VIRUS-L Digest Tuesday, 7 May 1991 Volume 4 : Issue 76

Today's Topics:

VIRUS-L is a moderated, digested mail forum for discussing computer virus issues; comp.virus is a non-digested Usenet counterpart. Discussions are not limited to any one hardware/software platform - diversity is welcomed. Contributions should be relevant, concise, polite, etc. Please sign submissions with your real name. Send contributions to VIRUS-L@IBM1.CC.LEHIGH.EDU (that's equivalent to VIRUS-L at LEHIIBM1 for you BITNET folks). Information on accessing anti-virus, documentation, and back-issue archives is distributed periodically on the list. Administrative mail (comments, suggestions, and so forth) should be sent to me at: krvw@CERT.SEI.CMU.EDU.

Ken van Wyk

Date: Mon, 06 May 91 10:43:37 -0500
From: <BDANIEL@USCN.BITNET>
Subject: Found Tester Virus [TV] still... (PC)

Thanks for the many helpful messages. I downloaded the new McAfee programs from 130.160.20.80 in /pub/ibm-antivirus:
VSHIELD 3.6V77, VSHEILD1 VSCRC 0.2, NETSCAN V77, SCAN 7.2V77, CLEAN 7.2V77
To my knowledge, these are the latest versions on these programs. The only program that finds the alledged virus is still NETSCAN. SCAN and CLEAN both tell me there is no virus. My only reason for running NETSCAN is because it wont goof up on my server's protected files. Does this mean it doesn't scan those files for viruses or does it by-pass the file security?

As for 'LOG.COM', its from PC-Magazine and its been sitting on my hard disk and on the server in the utils directory for years and I haven't run mine in a long time and I doubt LOG.COM on the server was infected with the Read Only Sharable flag. No other file has been flagged as having the virus.

Oddly, CLEAN V76 cleaned the virus by erasing the file and CLEAN V77 finds no virus. (Note: I kept a copy of LOG.COM on a floppy..)

Enough of beating on this, I'd like to UUENCODE the file and send it direct thru E-MAIL to McAfee. What Bitnet address do I send it to?

- _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ -

The note above contains my personal views and ideas. The above should not be considered in any way a view of Columbus College.

- _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ - _ -

Brian Daniel @ Columbus College, Computer Center, Woodall Hall Rm 113
BDaniel@USCN Cougar Court, Columbus GA 31993-2399 (404)568-2063

Date: Mon, 06 May 91 11:45:55 -0400
From: "Christopher T. Anderson" <CANDERSO@uga.cc.uga.edu>
Subject: re: help with mac "virus"? (Mac)

> recently, we've come across a problem with one of the macs in our lab.
> we really don't know if it's a virus or not, but it does act something
> like one. anyway, here are the symptoms:
>
> - - the mac has a 40 meg hard disk
> - - there is only about 16 meg of software installed
> - - both the finder and mactools report 38 meg used, 2 meg free
> - - disinfectant can't find anything, and neither can virus detective
> - - there are no hidden files anywhere on the disk (if there are, neither
> mactools nor resedit can find them)
> - - the "virus" hasn't spread to any of our other macs
>
> what we really want to know is: is this some sort of new virus, or is
> our mac just confused?"

This problem is not necessarilt indicative of a virus, but an otherwise corrupted Directory (or possibly Desktop). You could try rebuilding your Desktop, but probably should defrag/optimize the drive. This would rebuild your directory. For this I reccomend Disk Express II, it has always worked wonders for me.

- ---

Name: Christopher T. Anderson (Chris)
Mail Address: Computer Services Annex Electronic Addresses:
University of Georgia Bitnet: CAnderso@uga
Athens, GA 30602 Internet: CAnderso@uga.cc.uga.edu
Telephone: Work (404) 542-5162 EasyLink: 74730.3306@compuserv.com
Home (404) 549-8958 America Online: CTAnderson

C A R P E D I E M ! ! !

- ---

Date: Mon, 06 May 91 15:08:43 -0400
From: padgett%tccslr.dnet@mmc.com (A. Padgett Peterson)

Subject: re: What's so bad about self-extracting archives?

>From: Murray_RJ@cc.curtin.edu.au

>The other objection I have with self-extracting
>archives is that you're stuck with extracting the whole lot, even if
>you only want to find out what the !@#$%^&*() thing does.

This is not a generic case. I mostly use Phil Katz' excellent PKZIP (plug) and while it can create self-extracting files using an included utility, there is nothing that requires you to use the self-extracting feature. The file can still be viewed and selectively extracted using PKUNZIP just like a regular .ZIP file. The only difference is that you must completely specify the file as PKZIP defaults to the .ZIP extension.

(e.g. PKUNZIP [-v|-n|etc] SELFEXTR.EXE)

The biggest difference is that the .EXE is about 10k longer than the bare .ZIP but is handy when the DE doesn't have PKUNZIP.

Warmly,
Padgett

Date: 06 May 91 18:56:32 +0000
From: fisherjm@iris.ucdavis.edu (John M. Fisher)
Subject: Disk Killer Virus (PC)

We have had one of our hard disks encrypted with the Disk Killer virus. Supposedly there is a decryption package known as RestOgre and a detection package known as AntiOgre. Would anyone have any information about this virus, and known where I can find these programs? Any help would be greatly appreciated!

Thanks,
John

Date: 06 May 91 14:24:00 -0600
From: "William Walker C60223 x4570" <walker@AEDC-VAX.AF.MIL>
Subject: Re: Tester Virus [TV] in LOG.COM (PC)

Brian Daniel (BDANIEL@USCN.BITNET) writes:
> Question#1: Why does NETSCAN find the virus & SCAN not find the virus?
> . . .
> Question#4: Why is it only the LOG.COM file from PC-Magazine tht I've had
> for several years that shows up and infected?

I reassembled LOG.COM from the original source (I use a modified version of it) on a known clean machine and ran both SCAN (v76C) and NETSCAN (v76) on it. My results were comparable with Brian's.

Apparently, SCAN and NETSCAN are using two different search strings for the Tester Virus. Also apparently, a portion of the code in LOG.COM coincidentally matches the string NETSCAN uses to identify the Tester Virus. I guess it was only a matter of time before this type of thing occurred (or has it occurred before???). Aryeh Goretsky may wish to verify these findings (many apologies if I spelled your name wrong).

BTW, NETSCAN also found the Tester Virus in my modified version of LOG.COM, and the v77 versions of SCAN and NETSCAN give the same results as the v76 versions. I don't have the Tester Virus search strings to try Norton Antivirus on those files.

Bill Walker (WALKER@AEDC-VAX.AF.MIL) |
OAO Corporation |
Arnold Engineering Development Center | "I'd like to solve the puzzle, Pat"
M.S. 120 |
Arnold Air Force Base, TN 37389-9998 |

Date: Mon, 06 May 91 09:11:31 +0300
From: eldar@lomi.spb.su (Eldar A. Musaev)
Subject: Viruses in the USSR (PC)

By the information of the moscow AV researcher and developer of the AIDSTST (one of the soviet analogs of SCAN) Dmitry N.Lozinsky there are approx. 130 viruses in the USSR, including rare, very rare and exotic. Again, only 20-30 of them are really active.

Newly published book of Kiev AV researcher Nikolai N.Bezrukov contains references to approx. 10-15 soviet viruses (Voronezh group, Hymn group), though Lozinsky state that there are much more ones now and the wave of the soviet viruses is coming after the wave of the Bulgarian ones. I could not confirm or deny these data - I've seen only three ones, and it seems to be so that there are no more in Leningrad this time.

Eldar A.Musaev, researcher, Ph.D. eldar@lomi.spb.su
Mathematical Instituite of the Soviet Academy of Sciences, Leningrad, USSR

Date: Mon, 06 May 91 15:23:53
From: microsoft!c-rossgr@uunet.uu.net
Subject: re: F-PROT and FluShot problems

>Date: Fri, 03 May 91 17:10:20 +0000
>From: umbc3!umbc3.umbc.edu!cs106132@uunet.UU.NET (cs106132)
>
>.... It happened when a variant of 4096 was active.
>...., the virus infected the system files (IBMBIO....), the result
>was a non-bootable hard disk. This indicates [it] can actually
>contribute to the spread of this kind of viruses. This is not a bug

>type of thing, it is a design flaw!
> I repeated the same test using FluShot+ (1.81), the same thing
>happened in a slightly different manner. But the system again became
>impossible to boot from the hard disk. I had to run SYS C: to restore
>the sanity of the system. Any comments?

Obviously I have a comment! :-)

Please let me know more about this varient on 4096 and I'll fix it up
in the next release of FLU_SHOT+ (Current release, by the way, is
version 1.82, released 4/7/91...next release is due out shortly).

Ross M. Greenberg
 Author, FLU_SHOT+ & Virex-PC

Date: Mon, 06 May 91 23:08:37 -0700
From: p1@arkham.wimsey.bc.ca (Rob Slade)
Subject: Virus lists for misc machines

scott@hsvaic.boeing.com (Scott Hinckley) writes:

> If you know of/have a list of viruses affecting various machines (Mac,
> IBM, AMIGA, UNIX, etc). I would be interested in getting it. I am not
> looking for the code persay, merely a list of names and the machine(s)
> they can infect. A description of their effects would be appreciated,
> but by no means necessary for this compilation.

The Brunnstein Computer virus Catalog would be the best place to start.
The INDEX.291 (available on cert) would give you at least the names of
viri for most micro systems, and the catalogues themselves (less widely
available) have the descriptions.

==========
Vancouver p1@arkham.wimsey.bc.ca | "If you do buy a
Institute for Robert_Slade@mtsg.sfu.ca | computer, don't
Research into (SUZY) INtegrity | turn it on."
User Canada V7K 2G6 | Richards' 2nd Law
Security | of Data Security

Date: Tue, 07 May 91 09:10:34 +0100
From: Norman Paterson <norman@cs.st-andrews.ac.uk>
Subject: help with mac "virus"? (Mac)

billj@uop.uop.edu (Snugglupagus) (vol 4 issue 74): we have noticed a
similar effect but only on the 800 kb floppies. It seems that the
disc is fragmented and the missing space is recovered by drag copying
the old floppy to a newly initialised floppy.

I don't know if the hard disc software is more intelligent - I'd hope
so! But you might try connecting up a spare hard disc, initialising

it, and drag copying the old one onto it, to see if your space reappears. Effectively you are compacting your disc by this method.

Norman

Date: Mon, 06 May 91 17:32:48 -0700
From: p1@arkham.wimsey.bc.ca (Rob Slade)
Subject: Viri and the media (general)

Monday, May 6, 1991

Open letter to:
Editor, The Sun
Vancouver, BC
V6H 3G2

Dear Sir:

It is with considerable dismay that I read your reprint of the Canadian Press article on computer viral programs ("A Plague on the Government", High Tech, Wednesday, May 1st, 1991.) Although it is somewhat encouraging to see that the growing problem is receiving some coverage, I find it disheartening that the media is still mixing up information from various data security problems and failing to accurately inform the public.

The first problem is that of suggesting the problem is limited to the government. While government computers are being hit (and my own experience in government offices indicates that the figures published are at least an order fo magnitude too low), private companies and individuals are suffering as well. Certus International, a company specialising in antiviral and disk recovery programs, recently published a study in which 26% of responding corporations admitted to having been hit with a computer viral "infection" in January of 1991 alone. The study also indicates that the problem is growing at a rate of 160% per quarter. This suggests that by the end of this year, almost all large companies can expect to be hit with at least one infection every month.

The second problem is the sandwiching of paragraphs describing attempts by outsiders to access government mainframe computers between descriptions of the actions of microcomputer viral attacks. The structure of the article implies a relation between the "crackers" who are trying to break into computers through "public access" ports and links through "wide area networks" and the action of computer viral programs, most of which are only intended to spread as widely as possible through the microcomputer community. While the former are of concern only to large corporations, government and military, the latter can affect anyone who uses a microcomputer.

The third problem is the poor description of the viral programs themselves. What is the meaning of the statement that the "Eddie"

("Dark Avenger" is somewhat of a misnomer, being the name of the author, who has written a number of other viral programs) virus "attacks a system's main storage area"? It is true that the virus will, on occasion, overwrite random sectors on the hard disk of an infected microcomputer, and possibly corrupt files. Or the statement about the "so-called Stoned virus which destroys data." Why "so-called"? The Stoned virus, which is currently far and away the most common virus in North America, causes the least debate about its name, and any destruction of data it causes is unintentional and strictly limited to individual and special types of disks.

Comuter viral programs are certainly not the end of computers, as some have reported, but they definitely do exist. Viral programs present some risk to microcomputer users of all backgrounds, particularly when so few among the general population are well enough informed to take appropriate precautions. The problem of "viral illiteracy" is a matter of computer "public health". In the same way that healthy people are at greater risk when the general population is full of diseased "carriers", the average or even well-informed computer user stands a greater chance of being infected if most computer users around the individual may be infected and not know it.

Unfortunately, even the computer trade media is poorly informed on this issue. Lat year Computing Canada reported a story about a sophisticated extortion attempt that made use of a "trojan horse" program which pretended to be an AIDS information program while actually setting your system up to be "encrypted" in such a way that you would have to call upon the author's services. While there was never any indication that the program would reporduce itself in any way, it was reported as a virus, thus supporting the general myth that any type of computer problem is a virus.

Because correct information is so rare, myths about viral programs abound. One is that viral programs only come from "pirate" software, another that those who use only "commercial" software are safe. (Unfortunately, we have all to many examples of retailers, and even commercial software authors, distributing infected software.) Electronic bulletin board systems are often seen as a source (unlikely) and, astonishingly, many believe that the use of a modem itself is a means of infection (technically impossible.)

I wish to commend you on extending coverage of this important topic, but fervently hope that in future the information provided is more accurate.

==========

Vancouver p1@arkham.wimsey.bc.ca | "If you do buy a
Institute for Robert_Slade@mtsg.sfu.ca | computer, don't
Research into (SUZY) INtegrity | turn it on."
User Canada V7K 2G6 | Richards' 2nd Law
Security | of Data Security

End of VIRUS-L Digest [Volume 4 Issue 76]
****