University of Mississippi

eGrove

Newsletters

American Institute of Certified Public Accountants (AICPA) Historical Collection

11-1995

AOLGOLD Trojan Program; Technology Alert, Vol. 95, No. 7, November 1995

American Institute of Certified Public Accountants (AICPA)

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_news

 Part of the Accounting Commons

TECHNOLOGY ALERT

© 1995 AICPA Information Technology Membership Section

Vol. 95 No. 7
November 1995

AOLGOLD Trojan Program

The following excerpts come from a bulletin (November 16, 1995: Number G-03) issued by the Computer Incident Advisory Capability (CIAC) organization in the U.S. Department of Energy. It provides a detailed description of the reported vulnerabilities, and the proposed solutions. The U.S. Department of Energy (DOE) established the CIAC in 1989 to provide various computer security services free of charge to employees and contractors of the DOE. CIAC is located at Lawrence Livermore National Laboratory in Livermore, California, and is part of its Computer Security Technology Center. This Alert is to inform Information Technology Section members about a trojan program that is being distributed through America Online and other networks called AOLGOLD.ZIP. When the INSTALL.EXE file of this program is executed, almost all of the files on the users C: drive are deleted.

The AOLGOLD Trojan program was recently discovered on the America Online (AOL) online service. An e-mail message is being circulated that contains an attached archive file named AOLGOLD.ZIP. A README file that is in the archive describes it as a new and improved interface for the AOL online service. AOL has stated that there is no such program as AOLGOLD. IT Section members are reminded that simply reading an e-mail message or even downloading an included file will not do damage to your machine. The downloaded file must be executed to release the Trojan and have it cause damage.

If you unzip the archive, you get two files: INSTALL.EXE and README.TXT. The README.TXT file again describes AOLGOLD as a new and improved interface to the AOL online service. The INSTALL.EXE program is a self-extracting ZIP archive. When you run the install program, it extracts 18 files onto your hard drive: MACROS.DRV; VIDEO.DRV; INSTALL.BAT; ADRIVE.RPT; SUSPEND.DRV; ANNOY.COM; MACRO.COM; SP-NET.COM; SP-WIN.COM; MEMBRINF.COM; DEVICE.COM; TEXTMAP.COM; HOST.COM; REP.COM; EMS2EXT.SYS; EMS.COM; EMS.SYS; and README.TXT.

If you stop at this point and do nothing but examine the unzipped files with the TYPE command, your machine will not be damaged. The Trojan program is contained in the following three files: MACROS.DRV; VIDEO.DRV; and INSTALL.BAT. The remainder of the files included in the archive appear to have been grabbed at random to simply fill up the archive and make it look official.

The Trojan program is started by executing the INSTALL.BAT file. The INSTALL.BAT file is a simple batch file that renames the VIDEO.DRV file to VIRUS.BAT and then runs it. VIDEO.DRV is an amateurish DOS batch file that starts deleting the contents of several critical directories on your C:
drive, including: c:\; c:\dos; c:\windows; c:\windows\system; c:\qemm; c:\stacker; and c:\norton.

It also deletes the contents of several other directories, including those for several online services and games, such as: c:\aol20; c:\prodigy; c:\aol25; c:\mmp169; c:\cserve; c:\doom; and c:\wolf3d.

When the batch file completes, it prints a crude message on the screen and attempts to run a program named DoomDay.EXE. Bugs in the batch file prevent the DOOMDAY.EXE program from running. Other bugs in the file cause it to delete itself if it is run from any drive but the C: drive. The programming style and bugs in the batch file indicates that the Trojan writer appears to have little programming experience.

Recovery

WARNING Do not copy any files onto your hard disk before trying to recover your hard drive.

The files are deleted with the DOS del command, and can be recovered with the DOS undelete command. The files are still on your disk, only the directory entries have been removed. If you copy any new files onto your hard disk, they will likely be written over the deleted files, making it impossible to recover the deleted files.

If you have delete protection installed on your system, recovery will be relatively easy. If not, the DOS undelete command can be used, but you will have to supply the first letter of each file name as it is recovered. In many cases, you will probably want to restore the directories by reinstalling them from the original installation disks, but do that last. You must recover any unreplaceable files first using undelete and then replace any others by copying or reinstalling them from the distribution disks.

To recover the system:

1. Boot the system with a clean, locked floppy containing the recovery program for the recovery files you have installed, or the DOS UNDELETE.EXE program if you do not have recovery files installed.

2. Type the VIRUS.BAT file to get a list of the directories the Trojan tried to delete. Ignore any directories that don't exist on your machine.

3. Run the recovery program and recover your files. You may have to help it find the recovery files, such as MIRROR, which will be in the root directory. You may have to recover the MIRROR file first and then use it to recover the other files.

   If you are using only the DOS undelete command, type:

   ```
   undelete directory
   ```

   where directory is the name of the directory to examine. To undelete the files in the dos directory, use:

   ```
   undelete c:\dos
   ```

   The undelete program will present you with a list of deleted files with the first letter replaced with a question mark. Without delete protection, you will have to supply this letter in order to undelete the file.

4. After you have restored as many files as you want or can using the UNDELETE command, replace any others by reinstalling them using the original installation disks.