CERT Incident Note IN-99-03: CIH/Chernobyl Virus

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

CIH/Chernobyl Virus

Thursday, April 22, 1999
Friday, April 23, 1999 -- Updated vendor information
Monday, April 26, 1999 -- Updated vendor information, added FAQ

Overview

We have received a number of information requests about a computer virus named CIH. Anti-virus vendors have given this virus the following names: CIH, Win95.CIH, PE_CIH, Win32.CIH, and W95/CIH.1003. The virus has also been called the Chernobyl virus. Some versions of the CIH virus become active on April 26, 1999 which is the 13th anniversary of the Chernobyl disaster.

In addition to this Incident Note please see the CIH FAQ (Frequently Asked Questions) document.

http://www.cert.com/tech_tips/CIH_FAQ.html

Description

The CIH virus infects executable files and is spread by executing an infected file. Since many files are executed during normal use of a computer, the CIH virus can infect many files quickly.

There are several variants of the CIH virus. Some activate every month on the 26th, while other variants activate just on April 26th or June 26th. Once the CIH virus activates, the virus attempts to erase the entire hard drive and to overwrite the system BIOS. Some machines may require a new BIOS chip to recover if overwritten by the CIH virus. CIH only affects Win95/98 machines.

More technical details about the CIH virus can be found at the following site.

http://www.virusbtn.com/VirusInformation/cih.html

Solutions

The following items will help to prevent the CIH virus from deleting your data or writing to the BIOS, but if your computer has already been damaged by the CIH virus the following will not help to recover. If your computer has been damaged by the CIH virus we recommend you contact your computer vendor or motherboard vendor to find out how to recover the system BIOS. The data on the hard drive might not be recoverable, but a data recovery service might be able to retore some portion of the data.

Many motherboards have a "jumper" that will enable or disable the ability to write to the BIOS. To prevent the CIH virus or any other program from writing to your computer BIOS, we recommend that you set the motherboard jumpers so that the BIOS can not be modified. Some motherboards vendors may ship with the jumper set in the writable/programmable mode for the BIOS.

This is a known virus and anti-virus vendors are able to detect the CIH virus. To detect and remove current viruses, you must update your scanning tools and anti-virus software with the latest virus signatures or definitions. To properly clean the CIH virus we recommend booting an infected computer from a clean floppy diskette (one that is not infected) and then run anti-virus software.

Vendor Information

Below is a list of anti-virus vendors that have futher infomation and tools relating to the CIH virus.

Computer Associates InoculateIT

http://www.cai.com/virusinfo/melissa_virus.htm#cih

Current Virus Signature Versions that Detect and Cure the CIH virus are as follows:

- Any version of InoculateIT signature file later than 4.15 will detect and cure CIH.
- Current version of InoculateIT signature file is 4.20.
  Any of the above virus signatures files can be downloaded at www.support.cai.com

Data Fellows F-Secure Anti-Virus

http://www.datafellows.com/cih/

Network Associates/McAfee

http://www.avertlabs.com/public/datafiles/valerts/vinfo/spacefiller411.asp

ProLand Software

http://www.pspl.com/faqs/cihfaq.htm
http://www.pspl.com/download/cleancih.htm

Sophos

http://www.sophos.de/companyinfo/pressrel/uk/19990310chernobyl.html

Symantec/Norton AntiVirus

http://www.symantec.com/avcenter/venc/data/cih.html
http://www.symantec.com/avcenter/kill_cih.html

TrendMicro

http://216.33.21.51/vinfo/virusencyclo/default3.asp?VCode=EN001344

Copyright 1999 Carnegie Mellon University.