W95.CIH | Symantec

Discovered: June 01, 1998
Updated: April 25, 2002 2:39:44 PM
Type: Virus
Systems Affected: Windows

W95.CIH, also commonly referred to as Chernobyl, is a destructive parasitic virus. It remains memory resident and infects other exe files when they are opened.

Due to decreased submissions, Symantec Security Response has downgraded this threat level to 2 from 3 as of March 30, 2004.

The CIH virus, also known as Chernobyl, was first discovered in June 1998 in Taiwan. According to the Taipei authorities, Chen Ing-hau wrote the CIH virus. The name of the virus derived from his initials.

CIH is a destructive virus with a payload that destroys data. On April 26, 1999, the payload triggered for the first time, causing many computer users to lose their data. In Korea, it was estimated that as many as one million computers were affected, resulting in more than $250 million in damages.

Although the virus is rather old, Symantec still believes the virus is in the wild and may cause damage to computer users who use outdated virus definitions, or who do not use antivirus software.

Antivirus Protection Dates

- **Initial Rapid Release version** June 28, 1998
- **Latest Rapid Release version** August 08, 2016 revision 023
- **Initial Daily Certified version** June 28, 1998
- **Latest Daily Certified version** August 09, 2016 revision 001
- **Initial Weekly Certified release date** June 28, 1998

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Writeup By: Motoaki Yamamura

Discovered: June 01, 1998
Updated: April 25, 2002 2:39:44 PM
Type: Virus
Systems Affected: Windows

CIH is a virus that infects the 32-bit Windows 95/98/NT executable files, but can function only under Windows 95/98 and ME. It does not function under Windows NT or Windows 2000. When an infected program is run under Windows 95/98/ME, the virus becomes resident in memory. To remove the virus, do one of the following:

- Recommended method: Use the Symantec Security Response CIH Removal Tool, which removes the virus from memory and prevents the need to reboot from a clean system disk.
- Reboot the computer from a Rescue Disk.
- Reboot the computer from the Norton AntiVirus (NAV) 2001/2002 CD, if your computer allows this option.

If this is not done, the virus will infect every file scanned with Norton AntiVirus or with any antivirus program.

Although Windows NT system files can be infected, the virus cannot become resident or infect files on a computer running Windows NT or Windows 2000. The virus does not function under DOS, Windows 3.1, or on Macintosh computers. Once the virus is resident, the CIH virus infects other files when accessed.

The files infected by CIH may have the same size as the original files, due to the unique infection mode of CIH. The virus searches for empty, unused spaces in the file. Next, it breaks itself up into smaller pieces and inserts its code into these unused spaces. When NAV repairs a file infected by CIH, it looks for these small viral pieces and removes them from the file.

As of April, 1999, three known, similar variants of this virus exist. CIH versions 1.2 and 1.3 have a payload that will trigger on April 26, commemorating Chernobyl, the Soviet nuclear disaster, which occurred on April 26, 1986. CIH version 1.4 has a payload that will trigger on the 26th of any month. The payloads of all the versions of CIH are the same.

The first payload overwrites the hard disk with random data, starting at the beginning of the disk (sector 0) using an infinite loop. The overwriting of the sectors does not stop until the system has crashed. As a result, the computer will not boot from the hard disk or floppy disk. Also, the data that has been overwritten on the hard disk will be very difficult or impossible to recover. You must restore the data from backups.

The second payload tries to cause permanent damage to the computer. This payload attacks the Flash BIOS (a part of your computer that initializes and manages the relationships and data flow between the system devices, including the hard drive, serial and parallel ports, and the keyboard) and tries to corrupt the data stored there. As a result, nothing may be displayed when you start the computer. A computer technician would need to fix this.

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
- For further information on the terms used in this document, please refer to the Security Response glossary.

Writeup By: Motoaki Yamamura

Discovered: June 01, 1998
Updated: April 25, 2002 2:39:44 PM
Type: Virus
Systems Affected: Windows

Removal using the CIH removal tool
Symantec Security Response has developed a removal tool to clean the infections of W95.CIH. Use this removal tool first, as it is the easiest way to remove this threat.

Manual Removal:

The following instructions pertain to all current and recent Symantec antivirus products, including the Symantec AntiVirus and Norton AntiVirus product lines.

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan.

For specific details on each of these steps, read the following instructions.

1. To disable System Restore (Windows Me/XP)
If you are running Windows Me or Windows XP, we recommend that you temporarily turn off System Restore. Windows Me/XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore, antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, a virus scan may detect a threat in the System Restore folder even though you have removed the threat.

For instructions on how to turn off System Restore, read your Windows documentation, or one of the following articles:

- How to disable or enable Windows Me System Restore
- How to turn off or turn on Windows XP System Restore

Note: When you are completely finished with the removal procedure and are satisfied that the threat has been removed, reenable System Restore by following the instructions in the aforementioned documents.

For additional information, and an alternative to disabling Windows Me System Restore, see the Microsoft Knowledge Base article: Antivirus Tools Cannot Clean Infected Files in the _Restore Folder (Article ID: Q263455).

2. To update the virus definitions
Symantec Security Response fully tests all the virus definitions for quality assurance before they are posted to our servers. There are two ways to obtain the most recent virus definitions:

- Running LiveUpdate, which is the easiest way to obtain virus definitions.
  If you use Norton AntiVirus 2006, Symantec AntiVirus Corporate Edition 10.0, or newer products, LiveUpdate definitions are updated daily. These products include newer technology.

  If you use Norton AntiVirus 2005, Symantec AntiVirus Corporate Edition 9.0, or earlier products, LiveUpdate definitions are updated weekly. The exception is major outbreaks, when definitions are updated more often.

- Downloading the definitions using the Intelligent Updater: The Intelligent Updater virus definitions are posted daily. You should download the definitions from the Symantec Security Response Web site and manually install them.

The latest Intelligent Updater virus definitions can be obtained here: Intelligent Updater virus definitions . For detailed instructions read the document: How to update virus definition files using the Intelligent Updater .

3. To run a full system scan

1. Start your Symantec antivirus program and make sure that it is configured to scan all the files.
   For Norton AntiVirus consumer products: Read the document: How to configure Norton AntiVirus to scan all files.

   For Symantec AntiVirus Enterprise products: Read the document: How to verify that a Symantec Corporate antivirus product is set to scan all files.

2. Run a full system scan.
3. If any files are detected, follow the instructions displayed by your antivirus program.

Important: If you are unable to start your Symantec antivirus product or the product reports that it cannot delete a detected file, you may need to stop the risk from running in order to remove it. To do this, run the scan in Safe mode. For instructions, read the document, How to start the computer in Safe Mode . Once you have restarted in Safe mode, run the scan again.

After the files are deleted, restart the computer in Normal mode.

Writeup By: Motoaki Yamamura
