Cleaning Windows with Linux and ClamAV

by Robert Spotswood

Version 1.01

Introduction

Once a computer is infected with malware, you need special ways to clean it. Just installing some anti-virus (AV) software and telling it to clean will get some products, but not all. With malware employing rootkit technology, such as hooking into the Explorer process and therefore becoming completely invisible to Windows and the programs the run on top of Windows, such as AV software. Another trick is to have two processes which watch each other and restore one if the other is killed, or restore files if deleted.

There is a need to be able to scan a Windows machine while being absolutely sure no malware is active. One method is to pull the hard drive, put it into a known clean machine with AV software, and then scan the hard drive. It works, but is time consuming, and you have to have a clean machine handy.

There has to be a better way, and there is. It involves using a Live Linux CD and a flash drive with ClamAV.

Preparation

Thanks to -- StephenGran for the static compliation instructions. You need static compliation to reduce library version conflicts.

1. ./configure --enable-static --disable-shared --without-curl --prefix=/mnt/usbdisk
2. make LDFLAGS='-all-static'
3. Copy the binaries freshclam and clamscan to your flash drive.
4. Make an etc directory on the flash disk. This and steps 5-7 only have to be done once.
5. Copy the clamd.conf and freshclam.conf to the etc on the flash disk
6. For freshclam.conf:
    a. Comment out the example line
    b. Change DatabaseDirectory option to /mnt/usbdisk

c. Change DatabaseMirror to db.us.clamav.net for those in the US. See the docs for the correct value for other countries.

7. For clamd.conf:
   a. Comment out the example line
   b. Change DatabaseDirectory option to /mnt/usbdisk

Usage instructions

Optional, but recommended:

1. Have a good backup. It's possible the malware can sabatoge your computer so that removing it causes damage.
2. Do a disk cleanup. Every file you delete is one you don't have to scan. That means the scan takes less time and deleting is quicker than scanning.
3. Clear you Internet caches. This includes IE, Firefox, and Opera. Again, every file you delete is one you don't have to scan.
4. Disable system restore. Viruses are often backed up here and there can be a significant number of files to scan. However, this does limit your ability to repair some types of damage, so use this recommendation with caution.

Doing the Scan

1. Boot off a modern live CD. The CD must have NTFS-3G drivers. Tested CD's so far:
   a. Knoppix 5.1.1
   b. Insert 1.3.9b
   c. Xubuntu 7.10 Desktop – right now this my preferred CD
2. Open up two root prompt terminals
3. You must have a clamav user. Use the following command to create one if it doesn't exist: `useradd clamav` Ignore any errors, if any, that the user already exists.
4. Get the uid and gid of the clamav user. Check by using the following command: `grep clamav /etc/passwd` For example: `clamav:x:119:129::/var/lib/clamav:/bin/false` Here the uid is 119 and the gid is 129. Often the numbers are the same.

5. Now mount plug in the flash drive. Do not plug it in while booting. A few computers have problems booting off a live CD if a flash drive is inserted. I have seen this with Sony computers especially.
6. Ignore any auto mount operations. Cancel them. They will cause problems later.
7. Find out where the flash drive is, and the where the hard drive to be scanned is. Run the following command: `fdisk -l` as root. Usually it is /dev/sd?1 where the ? is often an "a". This command also tells you where the hard drive is.
8. Make the mount points for the flash drive and hard drive (if necessary). At the very least, you need to run the following command: `mkdir -p /mnt/usbdisk`
9. Mount the flash drive with clamav as the owner. This is particularly important if the flash drive is formatted as FAT or FAT32. Clam will no run unless the binaries are owned by clamav and with the FAT's, the mount options are the only way to make this happen. You will need the uid and gid noted above in step 4. Using step 4 as an example and assuming the flash drive is at /dev/sda1, the mount command would be: `mount -t auto -o uid=119,gid=129 /dev/sda1 /mnt/usbdisk`
10. Now, assuming you have internet connectivity, run the following command: `cd /mnt/usbdisk`. Next run freshclam: `/mnt/usbdisk/freshclam` If you get errors about `/mnt/usbdisk not locked` it means that the flash drive is also mounted somewhere else. Unmount ***all*** instances of it and re-run the mount command in step 9. As the definitions are stored on the flash drive, this step can be done ahead of time if you know, or suspect there will be internet connectivity issues. Just do it as close to the actual scan as possible.
11. While step 10 is running, in the other root prompt window, mount the hard drive partition(s). Usually, but not always, it is /dev/hda1 or /dev/sda1. If it is NTFS, a very common occurance, you need to issue the following command: `mount -t ntfs-3g /dev/hda1 /mnt/hda1` This command assumes you want to mount it at /mnt/hda1 and the mount point exists.
12. Delete or rename any old log.txt files on the flash drive.
13. Once step 10 is finished, now run the clamscan. See the clamscan man page for all the options, but here are the options I use. This assumes the hard drive is mounted on /mnt/hda1: `/mnt/usbdisk/clamscan -l log.txt -r -i --database=/mnt/usbdisk/ /mnt/hda1`

14. Generally you should just delete infected files. The paranoid can rename them and move them to another directory instead of deleting them. However, you need to use common sense as there may be false positives. If the computer has AV software, there will likely be false positives in the AV directory. If in doubt, and you have web access, you can try uploading the file to http://www.virustotal.com or http://virusscan.jotti.org/ to see what other virus scanners think of the file. Use sparingly though. They are s--l--o--w. Also, even if the file comes back squeaky clean, there are still no guarantees.
15. In case you notice a difference in the number of sigs reported by freshclam and clamscan, they are PUA (Potentially Unwanted Applications) sigs and they're not loaded by default. You can enable them by passing --detect-pua to clamscan or activating DetectPUA in clamd.conf but beware the high false positive rates!
16. Now if you reboot into Windows, you might want to re-install your AV software and do a full scan. ClamAV does not clean up the registry, although with the program files gone, the malware should be non-functional at this point.