United States - English [Change]

CA Security Advisor Research Blog

Find out what our research team is saying about the latest security threats in the CA Security Advisor blog

Identifying and Removing AntiVirus 2009 and Rootkit

On November 10 of this year in a blog titled Emerging Threat: AntiVirus 2009 I explained that our Support and Research teams were seeing a jump in the number of AV 2009 infections (we first saw copies of AV 2009 in June of this year). Well, this threat is well beyond 'emerging'. Over the last 4 weeks we have seen a jump in the use of rootkits to hide, protect, and keep the AV2009 infection resident. Of course, the use of rootkits is nothing new and the rogue software AntiVirus 2009 is nothing new, but over the last 4 weeks our Support team has seen an explosion of the two working in tandem. To learn more about rootkits, read here.

The Silent Infection Indicators (quite difficult to identify)

This infection is comprised of two very different components that work toward one cause, getting your money. Your money is the bottom line! First, you have the trojan element. It consists of a variety of files, some include rootkit elements. This component of the infection is not easily visible and is intent on staying hidden, running silently in the back ground, protecting itself and related files and downloading the rogue product. The rootkit consists of a system driver located in the driver folder at C:\windows\system 32\drivers\TDSS****.sys (not viewable without special tools). The file name appears to be semi-random. The first half of the driver name is fairly consistently "TDSS". The second half, represented here with an asterisk (*) varies from install to install. For example, across three installs, I had three different filenames: TDSSmxst.sys, TDSSliqp.sys, and TDSSosvn.sys – same file, different names. This rootkit recently has been accompanied by the file brastk.exe which shows up in two locations: C:\WINDOWS\system32\ and C:\WINDOWS. This file is not randomly named and stays generally static (for now). In some instances, this infection prevents common anti-rootkit tools from running. The infection makes a lot of registry changes, like: "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\tdssdata".

The Noisy Infection Indicators (the easily visible aspects)

Second, the other component of this infection relates to the rogue security product. This component is in your face and repeatedly pops up and nags at you. You will often find links to it on your desktop and in you Program Files. It is generally very easy to remove. The infection opens a warning from the system tray on regular intervals (see the box numbered B, in the image below). The sample I tested opened this warning every three minutes and would leave the window open for 16 seconds before closing. If you click on the window, it will automatically begin downloading a rogue security product. The rogue product can vary (and most assuredly will change in the future), but can include AntiSpywareXP 2009, AV2009, AntiVirus 2009, AV 2008, AntiVirus 2008 and other related variants (see the box lettered A below). If you close the installation window, it will open the window again and continue downloading – this process will repeat indefinitely (and cause you big headache). There is a white "X" that stays resident in the system tray (see icon labeled C).