Grisoft Offers Free Rootkit Removal

April 11 2007

Grisoft, makers of the popular AVG Antivirus, today released a free tool specifically aimed at eliminating malicious software that hides itself using rootkit techniques.

Rootkits typically subvert the Windows file system and Registry so as to hide their files from the operating system and from security software that relies on the operating system when searching for traces of malware. Grisoft conducted six months of public beta testing before releasing AVG Anti-Rootkit, to ensure that it removes malicious rootkits without affecting legitimate hidden processes.

AVG Vice President Larry Bridwell explained that AVG Anti-Rootkit was developed to "detect and destroy rootkits effectively, without bothering users with false alarms." He noted that rootkits "were originally used by hackers to cover their tracks after unauthorized access to computers. Today, these techniques have been redesigned in order to mask the presence of malicious software used to gather and exploit personal information…."

I ran a quick test using a half-dozen rootkit-based malware samples. AAR cleaned up the first batch effectively using its ordinary "Search for rootkits" scan. It didn't report on hidden Registry data nor on every hidden file, but after its removal process all leftover files and Registry data were exposed for removal by ordinary antivirus software. As AAR frequently points out, for full protection you'll also need real-time protection against malware installation and a complete malware scan-and-clean tool.

One of the malware samples in the second batch resisted AAR's removal; either that or it managed to reinstall its rookit code immediately after removal. A double-check scan with Microsoft's RootkitRevealer confirmed the problem. Still, this handy freebie will be a nice addition to your security arsenal. Look for a full review shortly.