No. 124, June 2005

THE COMPUTER CORNER

No. 124. Rootkit: Malnews

- by Stan Kaplan, WB9RQR
105 Martin Drive
Port Washington, WI 53074-9654
(262) 284-9346
skaplan@mcw.edu

Most of us think we have our computing environment pretty much under control. We use a virus scanner to keep our machines clean, and we update the virus definitions regularly to make sure we are ready to meet the latest threats. Many of us use additional software to keep our machines free of spyware – programs that can collect personal information without our consent and send it back via the web to unscrupulous individuals or companies that seek to rob us or otherwise make a dishonest profit. Viruses, spyware, key loggers, trojan horses – all are lumped together under the general definition of malware. Mal comes from the Latin word *malus*, which means badly. In English, mal- is a prefix meaning bad. Virus writers can be considered to be maladjusted individuals!

Well, I have some malnews. There is a malware mechanism or technique that is rearing its head and may cause many of us difficulties. It is not really new; some viruses used similar techniques at least 20 years ago. However, it is being revived. Called Rootkit, it can be used with any kind of virus, trojan, spyware and so on. Indeed, commercial key loggers are using it right now – key loggers are programs you can purchase that will log every keystroke on a machine for later perusal of the user's activities by the person who installed the key logger software.

Let us use an example to illustrate. Suppose a conventional virus infects your machine. It is what is generally known as a "well written" virus since it does no harm other than what the writer intended. Its payload consists of writing the words SAVE THE TREES in 72-point type on your screen every Friday at 9:00 a.m., if the machine is on at that time, and the words reappear on every boot each Friday. Lets call this pretend virus (I just made it up) the Tree Virus. A scan by Norton or another virus scanner can find and delete it from your machine. It is not a rootkit virus.

However, the author rewrites the Tree Virus to include rootkit techniques. It is now called the Rootkit Tree Virus. So what is the rootkit technique? It hides itself from system management utilities, spyware blockers and antivirus scanners! They can't see it! How can Norton Antivirus spot and delete or disinfect a virus if it cannot see it? How can Webroot Spysweeper detect and quarantine a spyware program if it cannot see it? The simple answer is: they cannot. Guess what? That includes you. If you use Explorer to examine a folder with a rootkit virus in it, you will not see its filename!

How does it do this? In the old DOS days, when we wanted to see the files in a folder (subdirectory), we issued a DIR command. Instantly a list of file names, extensions, size and date/time stamps would appear as a column on our screens. Now days, when we use Explorer to examine the contents of a folder, we see much the same (though you may well see only icons unless you select **View** and **Details** to see the output in column format). Rootkit malware simply intercepts the information before it gets to the screen or printer, and removes itself from the listing! Well now, virus scanners also use the system calls that Explorer uses to view the contents of a folder. So the virus scanner also gets misled, because it cannot see the file containing the virus, so it doesn't scan it. Devilishly clever!

What I am saying, folks, is that some people have a virus on their machine that is not being detected by the best commercial virus scanner software on the market today! Fortunately, there are relatively few rootkit malware programs out "in the wild" at present – just a handful. And the antivirus software makers are busy at work preparing programs that can find and kill rootkits. Microsoft is preparing a commercial program, "Strider Ghostbuster" as I write this (22Apr05). There are two free scanners available at this time: "RootkitRevealer" (www.sysinternals.com), and "Blacklight" (www.f-secure.com, free only to

1Jul05). Everything available now is in beta format – the companies are preparing to hit the market with full-fledged tools later, after their products are polished.

How do they do it? The rootkit scanners do two scans. The first is a complete scan of the system at the highest level – just like Explorer, or even you when you (the human user) use a Command Prompt window to execute a DIR command. Next it does another scan at a very low level – the raw contents of a file system volume or registry hive (the registry's on-disk storage format). Then it displays the difference. Anything showing up in the difference tally is at least suspect (but there may indeed be false positives). False positives should be less of a problem in the future as the technology learns to ignore system files that really should be hidden in the high level scans. At present, it is left up to the user to delete the positives or not.

Well, you read about it here first! Happy Computing!