

Being Emphatic

PRINT

Written by Matt Brunk

Jun 20, 2006

It was several years ago when a publicly traded company was splitting a key asset and the result was a separate company that left a lot of stockholders very happy. But the roller coaster ride and inflated stock wouldn't last long. "Sell Mom."



Later, my mother stated that I wasn't "emphatic enough" to convince her to sell that stock.

Now keep that thought. What should you be concerned about regarding your IP voice networks security?

Rootkits.

As reported in February at the RSA Security conference held in San Francisco, Microsoft security experts stated "Be Afraid, Very Afraid" when it comes to rootkits. When your computers or servers become infected with rootkits and you are running a converged IP network you may very well feel more than a pinch from infected machines. According to the report in Computer World- Mike Danseglio of Microsoft's Security Solutions Group said the only sure way to remove kernel rootkits is to completely erase an infected hard drive and reinstall the operating system from scratch.

Detecting rootkits isn't easy either. We are using RootKit Revealer, which is one of several available tools that identifies hidden rootkits. There aren't many tools out there yet that I'd hang my hat on and you probably won't find any single cure offering to clean rootkits completely from infected machines. **Preventing rootkits** varies in force with the tools you use too.

The overhead traffic produced by rootkits may be just enough to affect or disrupt voice quality not to mention breaching security in a big way. In our recent experience with a client network that we are building we found existing rootkit infections on more than 80% of their PCs and that was after several weeks of work adding new antivirus clients, malware and registry scans and hours of packet tracing. We estimated that about ten percent of the traffic we are seeing on the customer network is generated by these hidden monsters after matching the firewall logs against the web traffic reports and then looking at the oddities of traffic on sequential TCP ports. Okay, so that's our best guess. The disturbing thing about rootkits is that we may not be seeing all the traffic since some rootkits can piggyback on valid connections and remain stealth. Now that is scary.

As bandwidth is a precious commodity, procuring more isn't a solution but improving how we use it, manage it and secure it is. Time spent today chasing the 10 percent may prove worthwhile tomorrow and the preventive measures invested in now- once we agree on which one to adopt, I believe will pay off long term.

Microsoft and a few others have stated that there haven't been many detections- seemingly to imply that they are too small to worry about. But that was the left hand of Microsoft talking while the right hand says, "be afraid, very afraid." **Recognize and understand what rootkits are** and you'll at least be in the know. While rootkits may appear as a small deviation in the number of incidents "reported" you can count on seeing more of them. For something that can remain hidden so well, rootkits deserve your attention.

Okay, now for all the Moms: I'm being emphatic- be wary, very wary of rootkits.

Comment on this article

Leave your comments (Show/Hide Form)

Other Visitors Comments

There are no comments currently....

Close Window