SearchSecurity.com

Benevolent Nachi worm doing more harm than good

While the Nachi worm have been described by some as an antidote to the Lovsan worm, it comes with some nasty side effects such as clogging local networks with trash traffic.

Nachi, also known as the Welchia worm, emerged on Monday. It targets the same RPC vulnerability that allowed Lovsan to infect more than one million computers last week. However, Nachi then tries to kill Lovsan on infected systems and downloads a patch from Microsoft to prevent against future infection.

Also, it has emerged that Nachi also targets the Windows WebDav vulnerability, which was discovered in March when it was exploited on a Web site run by the US Army. The vulnerability is deep within Windows but can be exploited on Windows 2000 machines running IIS 5.0. The vulnerability is also found in Windows XP and NT 4.0 but it's not believed that Nachi can exploit the flaw on those platforms.

In a way, Nachi is probably a week too late. Many systems susceptible to the vulnerability have probably been patched, else Lovsan would have infected them. But experts agree that getting hit by a purported benevolent worm to protect against bad ones is not a good security plan.

Nachi doesn't do a great job removing Lovsan. It does stop the Lovsan process and delete the file associated with it. It also goes out and downloads the RPC patch and installs that. But the worm doesn't remove the registry key dropped by Lovsan. Moreover, having a worm install a patch is not an advisable practice.