

By: ~~October 2006~~, Technology News Editor

Microsoft Bulletproofed Vista Against the Blue Pill Rootkit

Or didn't it?

Back in August, at the Black Hat conference in Las Vegas, security expert Joanna Rutkowska from the Singapore-based firm COSEINC, had bypassed Windows Vista 64-bit edition's Patch Guard and performed a malware code injection. That malware code was none other than the Blue Pill rootkit. Well, Rutkowska herself revealed that Windows Vista is no longer vulnerable. "I had a chance to download Vista RC2 x64 and test it against the pagefile attack... It quickly turned out that our exploit doesn't work anymore! The reason: Vista RC2 now blocks write-access to raw disk sectors for user mode applications, even if they are executed with elevated administrative rights," stated Rutkowska. The image on the left clearly illustrates Rutkowska's statement. Rutkowska has presented three potential mitigations for the pagefile attack: 1. Block raw disk access from usermode. 2. Encrypt pagefile (alternatively, use hashing to ensure the integrity of paged out pages, as it was suggested by Elad Efrat from NetBSD). 3. Disable kernel mode paging (sacrificing probably around 80MB of memory in the worst case). According to Rutkowska, disallowing raw disk access was not the most comprehensive approach as it would generate incompatibility issues without actually resolving the problem. Why? Because legitimate kernel drivers designed to deliver compatibility with Vista to, let's say, a disk editor, could be geared toward malicious purposes involving accessing raw disk sectors via a pagefile attack. "The point here is, again, there is no bug in the driver, so there is no reason for revoking a signature of the driver. Even if we discovered that such driver is actually used by some people to conduct the attack! But it seems that MS actually decided to ignore those suggestions and implemented the easiest solution, ignoring the fact that it really doesn't solve the problem" concluded Rutkowska.