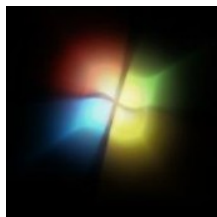


17 February 2010

By: Marius Oiaga, Technology News Editor

Windows 7
Microsoft

[Attackers Upgrade Rootkits Causing Windows Blue Screens of Death](#)

After Security Bulletin MS10-015 (KB977165) is applied

At the end of the past week, following the monthly release of Microsoft security patches, Windows users started reporting that their PCs crashed with a Blue Screen of Death error and were rendered un-bootable after applying [Security Bulletin MS10-015 \(KB977165\)](#). Microsoft immediately pulled the patch, and started investigating the issues. Also last weekend, the company offered an initial conclusion of its analysis indicating that malware infections were in fact responsible for the Windows BSOD crashes and not the security patch. Attackers have indirectly confirmed the software [giant's findings](#) when they started upgrading a piece of malicious code they authored, which failed to play nice with MS10-015 (KB977165).

"On last Tuesday Microsoft released a number of Windows updates, some of them critical because they fixed a 17 years old bug. After some users updated their Windows operating systems, they got a scaring and really annoying blue screen of death. Most of those users were angry with Microsoft, but the problem this time is not related to Microsoft," revealed [Marco Giuliani](#) from Pervx.

Responsible is a rootkit that goes by many names, including TDL3 or TDSS or Tidserv. The malware takes a numbers of precautions to both hide itself from the user and security solutions, but to also prevent its removal. TDL3/TDSS is not compatible with MS10-015 (KB977165), and its authors obviously did not expect Microsoft to make a kernel level change which would render infected computers useless.

"When the rootkit dropper is run, the infection calculates the RVA offsets of some Windows kernel APIs and hard code them so that at every restart the portion of the rootkit loader injected inside the infected driver can use these offsets to immediately calculate the address of the wanted functions," Giuliani explained. "This worked well until the MS10-015 update, when Microsoft updated Windows NT kernel. This update changed those offset values and consequently broke the rootkit code. When the update procedure is finished, system is restarted. At system restart, the rootkit code tries to call a non-valid address and this causes the BSOD."

However, attackers have moved fast and worked to upgrade their rootkit in order to make it compatible with Microsoft's security patch. Obviously, the malware's authors want to continue owning the machines their malicious code infected, not have them break down. In just a few hours, an update version of the TDL3/TDSS rootkit was offered to infected computers, a refresh which would no longer cause problems when MS10-015 is deployed.

The next move belongs to Microsoft. Security bulletin MS10-015 has managed to draw the attention on infected computers, and the Redmond company, along with members of the security industry need to now work together in order to make sure that the TDL3/TDSS is wiped out.