

13 May 2008

By: Bogdan Popa, Security and Search Engines Editor



Rootkits can prove to be extremely difficult to remove
askbobrankin

[New Rootkit Tricks the Operating System, Sits in Computer's Memory](#)

A new type of rootkit in the labs

TechWorld reported today that a new type of malware that could be impossible to detect by the anti-virus technologies currently on the market has been developed by security researchers and will be demonstrated at the Black Hat security event scheduled for August in Las Vegas. The same source adds that the new rootkit could prove to be incredibly hard to detect first of all due to the fact that it stays in a "protected part of the computer memory".

The rootkit installs in System Manager Mode (SMM) and could allow a potential attack to track the whole computer activity. The worst thing about it is that due to the fact that it is installed in a protected sector of the memory, the rootkit is entirely invisible to the operating system, which makes the detection and the removal quite impossible with the technologies currently existent on the market. The malicious code was developed by two security engineers, Shawn Embleton and Sherri Sparks, from Clear Hat Consulting, who also created similar rootkits a few years ago.

Rootkits have always been used by attackers as simple methods to break into the vulnerable systems and remain anonymous while conducting illegal activities but today's anti-virus solutions provide protection for a large number of rootkits. However, in case a rootkit manages to deploy its files into the computer memory, the anti-virus protection becomes quite useless and affected users must turn to other technologies in order to clean the computer, a method that usually requires advanced computer skills and knowledge.

"Rootkits are going more and more toward the hardware. The deeper into the system you go, the more power you have and the harder it is to detect you", Sherri Sparks of Clear Hat Consulting, the security company that built the rootkit, told [TechWorld](#).