

22 April 2008

By: Bogdan Popa, Security and Search Engines Editor

Troj/Dloadr-BKU - Yet Another EXE Downloader

One more dangerous infection in the wild



Trojan horses have always been a problem
Waynecounty

Finding malicious websites on the Internet or receiving emails with infected files is something usual these days so it's pretty important to have an up-to-date antivirus which would be able to block these threats. However, new infections are born every day so, if you really want to keep your system clean, you must keep an eye on the advisories released by security companies. One of the recently spotted infections is Troj/Dloadr-BKU, a Windows Trojan horse which installs its files into the registry and attempts to drop more malware on the affected computer. What's worse is that recovering and repairing a computer infected with this Trojan horse requires the user to restore the mlang.dll file from the Windows CD, even if your antivirus manages to clean the whole system. According to a security report published by Sophos, the Trojan horse drops three executable files on the affected systems, namely 1.exe, 2.exe and 3.exe. Sophos states that 1.exe was detected as Mal/EncPk-DI while 3.exe is said to be a sample of Troj/Dloadr-BKU. The 2.exe executable file can be safely deleted as it doesn't harm the computer. In addition to the mentioned files, the Trojan horse also creates and executes a BAT file, namely a.bat, which, according to Sophos, is detected as Troj/Dloadr-BKU, exactly the Trojan horse we're talking about. "Troj/Dloadr-BKU installs itself as a browser helper object which sends information about the infected system and downloads updates," the security company explained. Since most antivirus products have already released protection against this threat, it's recommended to run an update and apply the latest patches provided by the security vendor. Also, extra care is advisable as well as a full computer scan in case of suspicious activity spotted on the system.