

12 May 2007

By: Marius Oiaga, Technology News Editor



Windows XP
Profession 'of Life :
ش ;

[Microsoft Confirms the Windows Activation Trojan Horse](#)

Video demonstration

Microsoft has confirmed Symantec reports related to the spreading of a Windows product activation Trojan horse. The malicious code, identified by the Cupertino-based company as Trojan.Kardphisher, is designed to attack Windows XP users, by masquerading as Microsoft's Windows Genuine Advantage tool. According to Symantec, the malicious code in itself is only a minor threat, but the problem resides in the fact that the Trojan asks users to enter their credit card credentials. The social engineering aspect of this attack is quite well thought out and put together, as you will be able to see from the video embedded at the bottom, courtesy of Symantec. "While not a technically sophisticated approach, this Trojan relies on a social engineering tactic to trick consumers into providing credit card and other personal data. Because of situations like this Microsoft recommends that people be very cautious about revealing personal and financial information online," revealed Alex Kochis, senior licensing manager on the WGA team. Symantec's Takashi Katsuki posted the following instructions detailing the process users need to undertake to remove Trojan.Kardphisher:

1. Reboot the infected machine. You can do that by simply clicking the "No" and "Next" buttons, or by doing a good-old fashioned hard reboot.
2. While Windows is starting, press the function 8 key (F8 key) to enter Safe Mode.
3. Click Start > Run.
4. Type regedit
5. Click OK.
6. Navigate to and delete these subkeys:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runsoft2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
CurrentVersion\Policies\System\DisableTaskMgr (If it exists)
7. Exit the Registry Editor.

Users also have the possibility to introduce fake information in order to access their computer. You will be able to enter virtually any combination of letters and numbers for the email address, phone number, expiration date, credit card number, CVV2 code, ATM PIN and name on card, as long they resemble genuine ones. Next, make your way to this registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runsoft2.