Top Threat: Windows Hacktivation

May 5 2007

A clever Trojan tries to steal your credit card information by posing as the Windows activation interface.

Symantec is reporting on a Trojan horse that mimics the Windows activation interface.

What they are calling Trojan.Kardphisher doesn't do most of the technical things that Trojan horses usually do; it's a pure social engineering attack, aimed at stealing credit card information. In a sense, it's a standalone phishing program.

Once you reboot your PC after running the program, the program asks you to activate your copy of Windows and, while it assures you that you will not be charged, it asks for credit card information. If you don't enter the credit card information it shuts down the PC. The Trojan also disables Task Manager, making it more difficult to shut down..

Running on the first reboot is clever. It inherently makes the process look more like it's coming from Windows itself, and it removes the temporal connection to running the Trojan horse. The program even runs on versions of Windows prior to XP, which did not require activation.

This is not an attack that will sneak by you. The executable is nearly 1MB large. But if you find yourself in this situation you should be able to disable it in Windows Safe mode by removing the registry keys described in the Symantec writeup and deleting the program it points to. Updated antivirus software should also be able to remove it.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: Top Threat: Windows Hacktivation (2007, May 5) retrieved 20 March 2024 from https://phys.org/news/2007-05-threat-windows-hacktivation.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.