

Windows® 7 Compatibility Checker turns out to be a Trojan

Author: Sabina Datcu

Date: 05/10/2010

A deceptive "help" message invites recipients to check their PCs' compatibility with Windows® 7 by downloading and running an altered version of Windows® 7 Upgrade Advisor concealing a Trojan.

Cybercriminals are well known for their predilection to spot and bank on people's interest in what's hot in the e-world. Operating systems and their latest developments are classic honey pots and it is practically impossible to miss their potential as baits for illicit gains.

With Windows®7, the latest version of [Microsoft® Windows®](#), reaching general retail availability on October 2009, it was just a matter of time before [malware](#) creators rose to the occasion, and exploited users' eagerness to install it on their PCs.

This kind of success stories cannot exclusively rely on sheer luck, so a little bit of planning is mandatory. Here's how the plot line goes this time: a "disinterested helping hand" type of e-mail reaches Windows users' Inboxes and recommends that they download Windows®7 Upgrade Advisor Setup. This piece of software supposedly allows them to see if their system resources could support the new OS. All they have to do is open the attached .zip file.

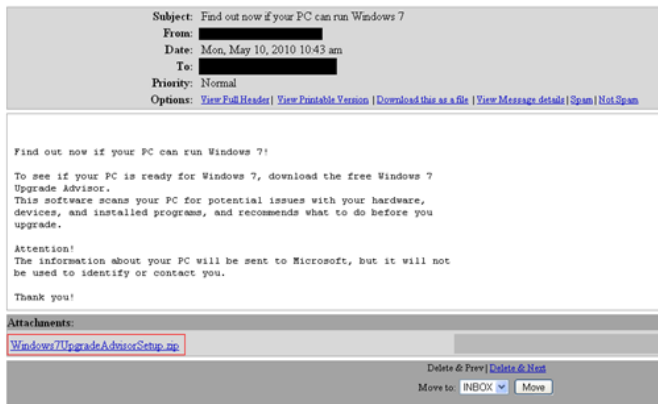


Fig. 1 The fake Windows® 7 compatibility check message

Instead of the promised compatibility checking tool, the zip file hides Trojan.Generic.3783603. This piece of malware contains malicious or potentially unwanted software which it drops and installs on the system. Frequently, it installs a backdoor which allows remote, clandestine access to the infected system. This backdoor may then be used by cybercriminals to upload and install additional malicious or potentially unwanted software on the captured system.

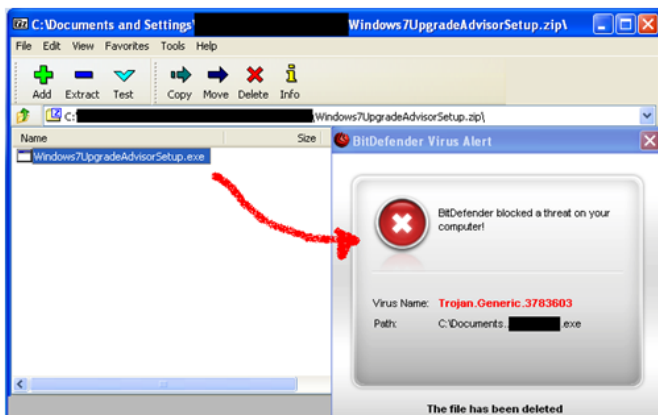


Fig. 2 Trojan.Generic.3783603 is exposed

The infection rates reflected by the [BitDefender Real-Time Virus Reporting System](#) indicate the beginning of a massive spreading of Trojan.Generic.3783603. Although this phenomenon has just started, it seems that it's just a matter of time before the cybercriminals control a huge number of systems. Infection rates are also expected to boom because of the effective social engineering ingredient of this mechanism, namely the reference to the highly popular Microsoft® Windows® OS.

In order to stay safe, BitDefender recommends that you never open the attachments coming from unknown contacts and that you install and update a [complete antimalware software solution](#). To always stay on the safe side of things, make sure you download the [software](#) you need from the official vendor's website.

All product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.