

Interpretation of SavedLegacySettings

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.networks/2005-05/msg00205>

- *From:* Andrew Aronoff <NOSPAM_WRONG.ADDRESS@xxxxxxxxxx>
 - *Date:* Mon, 16 May 2005 23:26:35 +0200
-

We are investigating malware that changes the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings value. The value is altered, but we see no change in Control Panel | Internet Options | Connections (tab) | Settings...

Several malware species that change this value have been reported:
W32.MyDoom.AB: <http://tinyurl.com/47fv8>
VP Killer trojan: <http://tinyurl.com/82frk>

We've looked at the Microsoft documentation about SavedLegacySettings (<http://tinyurl.com/b3po9>) but it's paltry explanation.

What does this value do exactly? Why does malware change it? How can the binary value be interpreted? Can the value be changed via the GUI? If so, how? If not, why not?

regards, Andy

—

Please send e-mail to: usenet (dot) post (at) aaronoff (dot) com

To identify everything that starts up with Windows, download "Silent Runners.vbs" at www.silentrunners.org

.

- Prev by Date: [*Re: socket arguments*](#)
- Next by Date: [*Re: Service & network drive letters*](#)
- Previous by thread: [*Detecting Closed COnnections*](#)
- Next by thread: [*How can I do with Visual C++ 6.0 for run on Windows NT Server 3.51*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)