

AppInit_DLLs revisited

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-12/0007.html>

From: Andrew Aronoff (*nbugtraq_at_AARONOFF.COM*)

Date: 12/06/04

Date: Mon, 6 Dec 2004 20:06:18 +0100
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Hello,

On September 30, I posted to NTBugTraq (<http://tinyurl.com/5657n>) about adware that infects the AppInit_DLLs (AID) registry value.

Here's an excerpt:

Per MSKB 197571, a .DLL listed there is "loaded by each Windows-based application running within the current logon session." IOW, any ad-ware found here runs concurrently with *_every_* program launched. It is truly astonishing that such a registry location exists.

In that submission, I warned that "AppInit_Dlls is a gaping security hole" and in a subsequent reply to the thread (<http://tinyurl.com/3thhc>), I opined that "there should be special vetting, perhaps against an MS-approved white list, before an app can write there."

A much better answer, though, was safely right in front of me --- SAFE MODE.

MS has made Safe Mode virtually startup-program-free and relatively service-free, but it blithely lets any AID-worker launch. (Anyone know why?)

If a user could boot into Safe Mode without any AID, this spyware bastion could be handily defeated.

MS should disable any AID-worker in Safe Mode and it should do it ASAP for *_all_* O/S's in the NT4 family.

regards, Andy

P.S. to Russ: pushing the non-proportional font button when browsing the NTBugTraq archives makes the web server burp the following error: "StartIndex cannot be less than zero." Too bad. I really like that button but I hate negative numbers even more. ;-)

NT-Bugtraq: Applnit_DLLs revisited

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

--
Editor's Note: The 43rd Most Powerful Person in Networking says...
Register today to take the TruSecure ICSCA exam by 12/31/04 at
<<http://www.2test.com>> , use promo code "CT1204" and you will pay just
\$221.25 US Dollars for domestic exam delivery and \$296.25 US Dollars
for international delivery.
Visit <<https://ticsa.trusecure.com>> for complete details regarding the
TICSA credential and to take the free sample exam.
--