

Re: MD5 Hash for WindowsXP-KB835935-SP2-ENU.exe

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-08/0042.html>

From: Jason Coombs PivX Solutions (jcoombs_at_PIVX.COM)

Date: 08/12/04

Date: Thu, 12 Aug 2004 00:00:00 GMT

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

-----Original Message-----

FROM: "Jason Coombs PivX Solutions" <jasoncoombs@tmo.blackberry.net>

Date: Wed, 11 Aug 2004 22:00:32

To: "Windows NTBugtraq Mailing List" <NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM>

Cc: PTCull@LBL.GOV

Subject: Re: MD5 Hash for WindowsXP-KB835935-SP2-ENU.exe

Pete Cull wrote:

> *Other companies are doing this.*

> *Should MS include md5 checksums?*

Yes.

That having been said, I have debated this point for some time with Microsoft and others, and the real answer is both 1) no, and 2) they already do include hash codes for the software they publish.

You probably know that Microsoft uses digital signatures. Their view is that these signatures are better than a list of known/expected hashes ... check the digital signature on the file, the argument goes, and you **are** verifying its hash code. You do so under Windows Explorer by right-clicking on the file.

Never mind that we all have our favorite trusted hashing utility, and our favorite trusted source like PTCull@LBL.GOV and NTBugTraq to confirm for us that we know what hash code to expect. Obviously, because the NTBugTraq posting is not itself digitally signed, an attacker who has planted a bad binary on your system is going to also watch all your incoming mail and replace the real hash code supplied by NTBugTraq with the right one for the malware. Or, the attacker will just DOS your inbox to prevent you from receiving the NTBugTraq posting that supplies the correct hash code.

This is the general argument against publishing hashes, the way all good software vendors do, and I still cannot comprehend it. Some people look at hashes or signatures as solely an integrity check, and perhaps you consider yourself to be in this camp? A checksum that tells you that your download has completed successfully is helpful, particularly when our file transfer tools are so poorly designed as to tell you neither how large the file was supposed to be nor that the file did not download completely.

But more than an integrity check, keeping track of known good hashes is also a security measure. Receiving a hash code from a trusted source that you can verify with a tool of your choice offers superior practical security

NT-Bugtraq: Re: MD5 Hash for WindowsXP-KB835935-SP2-ENU.exe

than does attempting to verify a digital signature with a tool provided by the software vendor.

Sincerely,

Jason Coombs
Director of Forensic Services
PivX Solutions, Inc.
<http://www.PivX.com/forensics/>

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.
