

Re: Self Decrypting Archive Freeware?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2102.html>

From: Juuso Hukkanen (juuso929_at_tele3d.net)

Date: 04/29/05

Date: Fri, 29 Apr 2005 22:36:33 +0300

On Fri, 29 Apr 2005 09:00:06 +0200, Sebastian Gottschalk
<seppi@seppig.de> wrote:

>*The encrypted ZIP archive are _not_ portable. Please read the PKZIP
>specification;*

I agree that PKZIP 2.0 encryption is not portable not even secure. On the other hand portability is always a relative issue not even the C is not completely portable – nothing is. Mikes question wanted a "better than plaintext solution" which would allow him to access his now recorded files in 2015. Anyone is free to offer a solution, traditional PKZIP has some durability advantages due to its popularity. I suggested that and gave an extra hint for hardening its limited security a little bit.

> *AES encryption in WinZip is a proprietary incompatible nonsense.*

Yes, already a second AES – zip format and counting. PKWARE also has their AES – zip, I dont know if it is the same as win – zip's. Propably it is still too early to use them for storing purpoces above lets say 5 – 10 years and they are not the freeware answer which was required by OP. However somehow I think AES – zip could very soon become the dominant zip format, especially if MS would start to support it. I mean with similar magic MS always succeeds to force MS – office users into new word documet formats. Anyway independently of future zips, the 2.0 version will be supported atleast the required 10 years.

Mikes simple question did show the limits of systems predictability very well. Did you self have a better (than zip) ten – years – one – click – always – works – solution – to offer.

Juuso Hukkanen