QGIS Application - Feature request #14914
Add a warning to Plugin manager

2016-05-27 10:53 PM - Paolo Cavallini

Status:	Closed		
Priority:	High		
Assignee:	Borys Jurgiel		
Category:	Plugin Manager		
Pull Request or Patch supplied:	No	**Resolution:**	
Easy fix?:	No	**Copied to github as #:**	22866

Description

Users should be warned that external plugins may contain even serious errors and malicious code.

Related issues:

Related to QGIS Application - Feature request # 17349: Sort out the trusted/u...	**Closed**	**2017-10-28**

History

#1 - 2016-05-27 10:56 PM - Paolo Cavallini

- Operating System set to All

- Category set to Plugin Manager

#2 - 2016-05-27 11:25 PM - Alexander Bruy

Where is the best place for such warning? We can put in at the plugin description page shown on the right side of the Plugin Manager. E.g. under plugin title and description.

Also we need to agree about text of this warning. It can be something like "This is 3rd party plugin and QGIS team has no relation to it. Plugin may have bugs or even malicious code. Use at own risk". Or just simple "Use at own risk".

#3 - 2016-05-27 11:28 PM - Paolo Cavallini

@tim, could you please suggest the best wording here?

#4 - 2016-05-28 03:45 AM - Tim Sutton

"*Please Note:* Whilst the QGIS project provides a platform for creating and sharing plugins, we make not assertions as to the quality and security of these plugins. Plugins in the repository are developed by third parties and may have bugs, be non-functional or even contain malicious code. We recommend that you carefully review which plugins you install. You should understand that the use of contributed plugins is entirely at your own risk. If you wish to report an issue with any plugin, please contact us at plugins@qgis.org"

#5 - 2016-05-30 04:08 AM - Alexander Bruy

Where this warning should be shown: on each plugin page or somewhere else?

#6 - 2016-05-30 04:10 AM - Paolo Cavallini

- Subject changed from Add a warning to Plugn manager to Add a warning to Plugin manager

#7 - 2016-05-30 04:12 AM - Paolo Cavallini

IMHO it is OK to add it to the setting tab of the plugin manager, besides the new option "Only trusted plugins", so users are warned before turning the option off.

#8 - 2016-05-30 07:14 AM - Tim Sutton

I think we need to display it on the web site too since you can download them from there.

#9 - 2016-05-30 07:58 AM - Harrissou Santanna

Tim sutton wrote:

> *If you wish to report an issue with any plugin, please contact us at plugins@qgis.org*

Isn't there a risk to have people reporting issue about plugin functionnality (i mean simple bug reports) to plugins@qgis.org instead of plugin author?

#10 - 2016-05-30 10:34 PM - Paolo Cavallini

Harissou, fully agreed, this is a big risk, who can lead to an unsustainable situation for the plugins manager

#11 - 2016-05-31 01:20 PM - Tim Sutton

Hi Harissou

Yes - on the other hand it is common for sites to have a way to report issues with the content on the site. If you are trying to report a malicious plugin, writing to the plugin author obviously isn't the way to go and there should be some mechanism to do it. We could use the ticket system, but I think that just transfers the same problem somewhere else.

Do you have any alternative suggestion that might work?

Regards

Tim

#12 - 2016-05-31 02:31 PM - Harrissou Santanna

Hi,
I realised after Paolo's message that i should have come with a solution. Tim, I'm ok with asking them to report to the plugin site if there's a malicious or no source provided with the plugin. What I meant was about the wording. With

> *If you wish to report an issue with any plugin, please contact us at plugins@qgis.org*

some people may report all kind of issues. Our warning should imho emphasize/be more precise on the kind of issues (malicious code, source not provided, something else?) we're expecting the report.

#13 - 2016-05-31 02:50 PM - Tim Sutton

Hi Harrison

Ok thanks for your input! How about this revised text?:

"*Please Note:* Whilst the QGIS project provides a platform for creating and sharing plugins, we make not assertions as to the quality and security of these plugins. Plugins in the repository are developed by third parties and may have bugs, be non-functional or even contain malicious code. We recommend that you carefully review which plugins you install. You should understand that the use of contributed plugins is entirely at your own risk. If you wish to report an issue with any plugin that you believe may be a security issue, or that creates a poor experience for users in other ways, please contact the plugin creators directly. If you do not receive a response from the plugin author or you do not believe the author intends to correctly address a serious issue, please contact us at plugins@qgis.org and we will consider delisting the plugins if needed."

#14 - 2016-05-31 04:01 PM - Harrissou Santanna

LGTM. And sorry for my first unclear reaction.

#15 - 2016-05-31 09:58 PM - Paolo Cavallini

Seems reasonable to me, thanks.

#16 - 2016-06-01 05:11 AM - Harrissou Santanna

A side note about the warning: Does it mean that QGIS project no longer checks quality of the plugins?
Around me, I often praise the completeness of QGIS using (also) features, fiability, openness of its plugins infrastructure (Core or not). Every body is aware that bugs are inherent to a software project but malicious code is another thing.
I'm afraid that given that few people among QGIS users are able/willing to dig into plugins code and identify malicious code, the expression "malicious code" scares them and give a negative image of the QGIS plugin repo.

I remember a call from Paolo about an automatic tool from devs to check that side of the plugins. Couldn't that be in the Todo list and financed by QGIS.ORG (or did I miss something)?

#17 - 2016-06-01 07:17 AM - Paolo Cavallini

Please use the mailing list for longer discussions.
Yes, same quality check in place, unchanged.

#18 - 2017-04-05 05:02 AM - Borys Jurgiel

- Assignee set to Borys Jurgiel

#19 - 2017-05-01 12:46 AM - Giovanni Manghi

- Easy fix? set to No

#20 - 2017-10-27 06:41 PM - Borys Jurgiel

See https://github.com/qgis/QGIS/pull/5484

#21 - 2017-10-28 11:24 AM - Borys Jurgiel

- Status changed from Open to Closed

Superseded by #17349

#22 - 2017-10-28 11:25 AM - Borys Jurgiel

- Related to Feature request #17349: Sort out the trusted/untrusted plugins/authors stuff added