QGIS Application - Bug report #14140
Crash in QgsGeomColumnTypeThread stopping connection scan

2016-01-19 03:48 AM - Sandro Santilli

Status:	Closed		
Priority:	Normal		
Assignee:	Sandro Santilli		
Category:	Data Provider/PostGIS		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	
Crashes QGIS or corrupts data:	Yes	**Copied to github as #:**	22142

Description

I just got a segfault with current master (670ded3d0622811f8e0ba50b3f3fd5e783742044) by clicking on "stop" in the "Add PostGIS Layer" dialog, while it was scannign a database.
Backtrace:

```
(gdb) bt
#0  0x00007fa6eb4ec12c in QString::QString (this=0x7fa6d98c8b40, other=...) at /usr/include/qt4/QtCore/qstring.h:725
#1  0x00007fa6eb510273 in QgsPostgresConn::connInfo (this=0x0) at
/usr/src/qgis/qgis-master/src/providers/postgres/qgspostgresconn.h:308
#2  0x00007fa6eb510387 in qgsConnectionPool_ConnectionToName (c=0x0) at
/usr/src/qgis/qgis-master/src/providers/postgres/qgspostgresconnpool.h:25
#3  0x00007fa6eb510c2a in QgsConnectionPool<QgsPostgresConn*, QgsPostgresConnPoolGroup>::releaseConnection (
   this=0x7fa6eb75ed50 <QgsPostgresConnPool::sInstance>, conn=0x0)
   at /usr/src/qgis/qgis-master/src/providers/postgres/../../core/qgsconnectionpool.h:264
#4  0x00007fa6eb5304aa in QgsGeomColumnTypeThread::run (this=0x2337220)
   at /usr/src/qgis/qgis-master/src/providers/postgres/qgscolumntypethread.cpp:115
#5  0x00007fa787bd132f in ?? () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#6  0x00007fa78005c182 in start_thread (arg=0x7fa6d98c9700) at pthread_create.c:312
#7  0x00007fa7866be47d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111
```

It's still the QgsGeomColumnTypeThread...

Associated revisions

Revision 69cb0c4e - 2016-01-19 01:15 PM - Sandro Santilli

Fix double-release of postgresql connection on table retriveal stop

Also breaks earlier out of loop and print a different status
message on "stop" (rather than "complete").

Fixes #14140

History

#1 - 2016-01-19 03:53 AM - Sandro Santilli

```
==1984== Thread 11 QgsGeomColumnTypeThread:
```

```
==1984== Invalid read of size 8
==1984==    at 0x8355B12C: QString::QString(QString const&) (qstring.h:725)
==1984==    by 0x8357F272: QgsPostgresConn::connInfo() const (qgspostgresconn.h:308)
==1984==    by 0x8357F386: qgsConnectionPool_ConnectionToName(QgsPostgresConn*) (qgspostgresconnpool.h:25)
==1984==    by 0x8357FC29: QgsConnectionPool<QgsPostgresConn*, QgsPostgresConnPoolGroup>::releaseConnection(QgsPostgresConn*) (qgsconnectionpool.h:
264)
==1984==    by 0x8359F4A9: QgsGeomColumnTypeThread::run() (qgscolumntypethread.cpp:115)
```

#2 - 2016-01-19 03:56 AM - Sandro Santilli

Got it, ColumnTypeThread handling of "stopped" (mStop) is not thread-safe.

#3 - 2016-01-19 04:15 AM - Sandro Santilli

- Status changed from In Progress to Closed

Fixed in changeset commit:"69cb0c4ed3174946c82e32dad4af5a12275079fc".