Freeciv - Bug #768386

Threaded AI crash at can_unit_do_activity_targeted_at()

Status: New
Priority: Normal
Assignee: Marko Lindqvist
Category:
Sprint/Milestone:

Description
This is with 68a3f97be1fec3f26b36d8ad1f89c0497624c2e from master with number of later bugfixes backported to it.

Thread 2 "freeciv-server" received signal SIGSEGV, Segmentation fault.
(Switching to Thread 0x7ffffffee3700 (LWP 32734))
can_unit_do_activity_targeted_at (punit=0x555555618ee30, activity=ACTIVITY_BASE, target=0x555555af9270 <extras+3440>, ptile=0x5555557caf20) at ../../src/common/unit.c:786
786   if (is_build_activity(tunit->activity, ptile)
tunit pointer seems garbage.

Backtrace:
#0  can_unit_do_activity_targeted_at (punit=0x555555618ee30, activity=ACTIVITY_BASE, target=0x555555af9270 <extras+3440>, ptile=0x5555557caf20) at ../../src/common/unit.c:786
#1  0x00005555556cdaf7 in tai_city_worker_requests_create (ait=ait@entry=0x555555af5ee0 <ai_types+608>, pplayer=0x555555ee8460, pcity=0x5555557d5150) at ../../../src/ai/threaded/taicity.c:218
#2  0x00005555556c4750 in tai_check_messages (ait=ait@entry=0x555555af5ee0 <ai_types+608>) at ../../../src/ai/threaded/taiplayer.c:121
#3  0x00005555556c4827 in tai_thread_start (arg=0x555555af5ee0 <ai_types+608>) at ../../../src/ai/threaded/taiplayer.c:121
#4  0x00005555556cc4827 in tai_thread_start (arg=0x55555af5ee0 <ai_types+608>) at ../../../src/ai/threaded/taiplayer.c:85
#5  0x00007fffff4a04f2a in start_thread (arg=0x7ffffffee39700) at pthread_create.c:155
#6  0x00007fffff4937edf in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95

The crash is inside unit_list_iterate() for a tile, and tunit is the unit received from that iteration, so it seems likely that main thread has changed the list at the same time.