Analysis of the bug

The `do_newarg()` function contains an integer overflow bug: a sufficiently large positive `num` will overflow the multiplication, producing a very small `size` (maybe even zero). This will lead to a situation where the program thinks it has allocated a very large number of `ArgObj` objects on the heap, but it has actually allocated just a few bytes.