扫雷的逆向思路

转载

weixin_34221775 于 2019-06-29 19:08:40 发布 478 收藏
文章标签： php 数据结构与算法
原文链接：http://www.cnblogs.com/fanzi2009/archive/2009/03/19/1417003.html

思路来源于看雪的一篇文章： http://bbs.pediy.com/showthread.php?t=55942

扫雷内部的数据结构肯定是n*m的一个动态数组。数组元素中不同的值代表不同的状态。
用spy++查看扫雷的窗体，发现那些小方格不是不是button，而是BitBlt画上去的。
因此在BitBlt下断点，发现有两处。一处位于一个2维循环中，于是在这里找突破口。
发现每个循环中的BitBlt的srcDC不一样，是存在一个数组中的，这个数组记录着雷、数字图形的DC。
修改汇编，可以轻松让满屏的都是雷、或者数字。
顺藤摸瓜，就知道m*n数组的位置，继续逆向分析，可以知道数组中不同数值的意义。