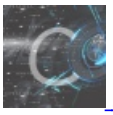
TCTF2017 线下赛 ——Wanacry writeup

原创

ddd0ng 于 2017-06-11 20:24:21 发布 1110 收藏

分类专栏： 二进制 文章标签： windows xp wannacry rsa

本文链接：https://blog.csdn.net/axiejundong/article/details/73065035



TCTF2017 线下赛 ——Wanacry writeup

这道题给了一些被用 wanacry 程序加密后的图片文件，一个 RSA 公钥文件，一个 windows xp 的内存 dump 文件。很明显，这是要去利用 windows xp 调用加密函数之后没有将相关内存清0的 bug 来从内存中恢复出私钥并解密文件，flag 就藏在解密后的文件中。具体原理可以参照这篇文章

github 上也有现成的工具 wanakiwi 可以下载（后来才发现 github 上除了源代码，同时也有了 release 版的exe文件，自己太蠢了才去手动编译）

跑偏的思路

但是这个工具根据作者的 readme 来看只能指定某个进程，然后搜索这个进程的整个虚拟内存地址空间，而题目给的是一个 内存dump 文件。一开始思路跑偏了，想去改这个工具的源码，以为改源码会比较简单，后来发现这个程序写的还蛮复杂的，而且调用了一大堆 windows 的 API，读懂源码就很费劲了，更别提修改了。

读源码的过程中发现这个工具有很多选项作者没有在 readme 里面说明（作者太坑了啊！），例如加上 `/mdmp:xxx.mdmp` 选项可以分析某个 dmp 文件，但是程序限制了这个 dmp 文件必须要是 `.mdmp` 后缀的。这个后缀的 dmp 文件是一种 windows 下的特殊 dmp 格式，有特定的文件头，包含了一些除了内存镜像以外的特殊信息。不能直接处理题目给的 vmem 后缀的文件，而 vmem 根据文件大小512M（512的整数倍）来判断 就是直接把内存给 dump 下来的文件。

正确的思路

一开始的思路走不通，突然想到既然改源码很麻烦，那把文件用程序整个 load 到内存里不就行了。一开始试了010Editor， 但是没有搜索到私钥。然后试着自己编写程序，想到可以把文件整个 map 到内存里面，使用了一些 windows 的 api， 但是还是不行。经@许晟杰 提醒，调用任务管理器查看内存占用，发现程序竟然只占用了300多 k 的内存，推测可能是这种方法并没有真正把文件加载到内存里，只是 map 到了虚拟地址空间，采用了 lazy load 的方法，实际去访问文件的时候才会把文件真正加载到真实内存里，并建立起真实内存和虚拟内存的映射。

又 google 的一番，发现最笨的方法我们竟然没有想到，就是用 malloc 在堆上分配512M 空间，然后用 fgets 读入文件。一开始想当然的认为这么大的文件malloc 应该分配不了这么大的文件，实际试了之后发现是可以的。所以任何事不要想当然。

之后就顺理成章了，指定 pid，用 wanakiwi搜索内存，然后找到私钥，解密文件，找到 flag。