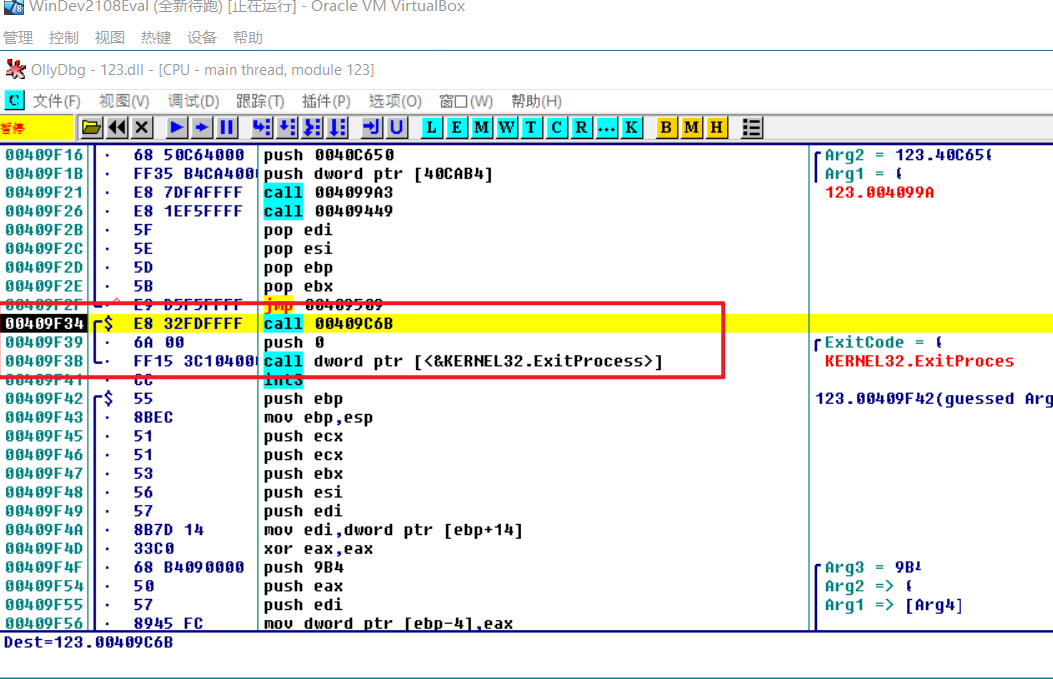
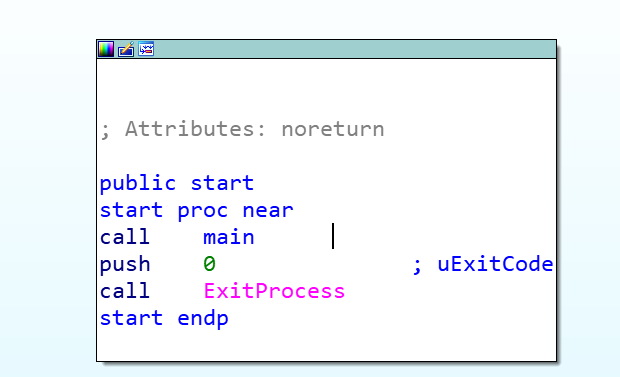
探索过程

已经对该病毒文件有了初步的了解, 开始配合动态调试判断每个函数的大致作用.

在进入ida时, 能看到一个start函数, 猜测它将要调用的就是main函数 , 使用ollydbg也验证了这就是main函数.





图中main函数为我重命名函数结果。

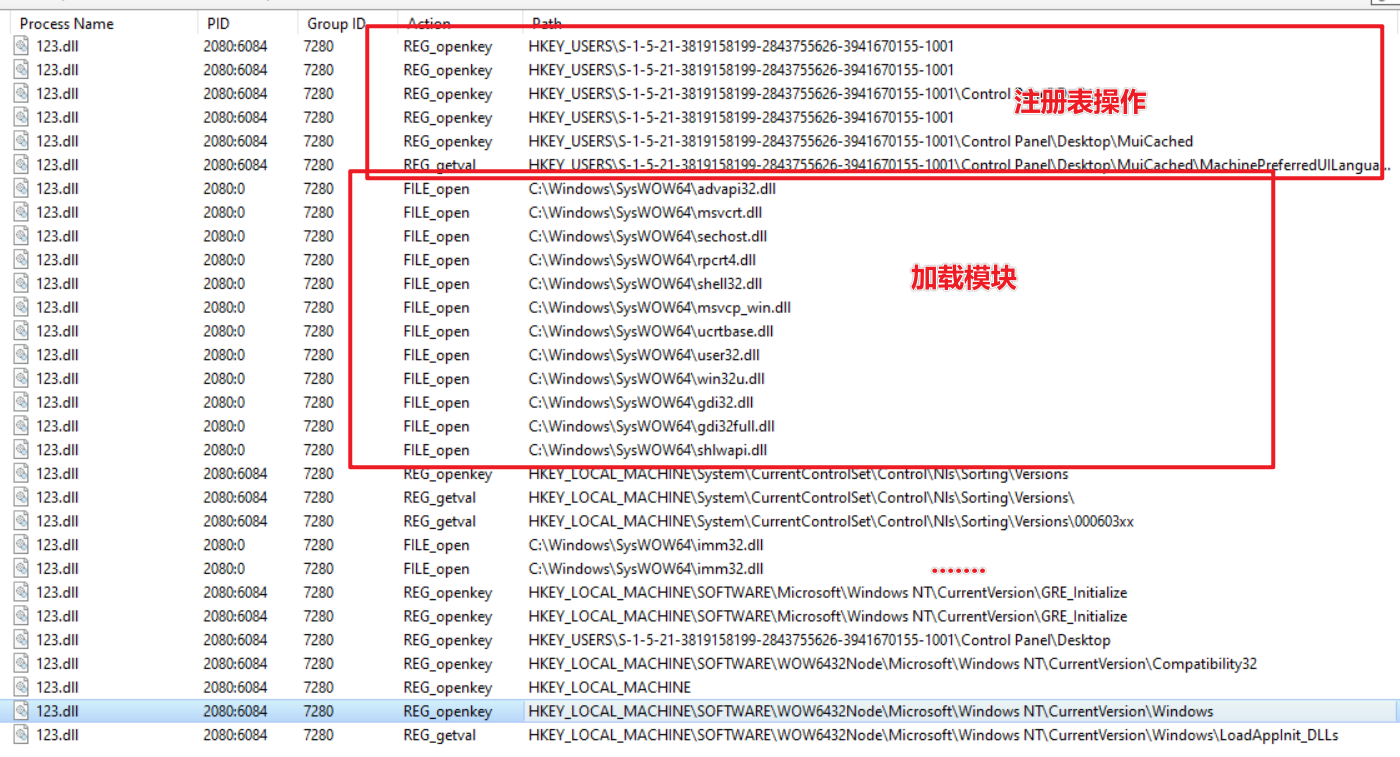
接下来则是探索main函数

若代码可读性良好则直接猜测估计作用（如此处的malloc，calloc），否则则根据动态跟踪的过程判断该函数的作用。

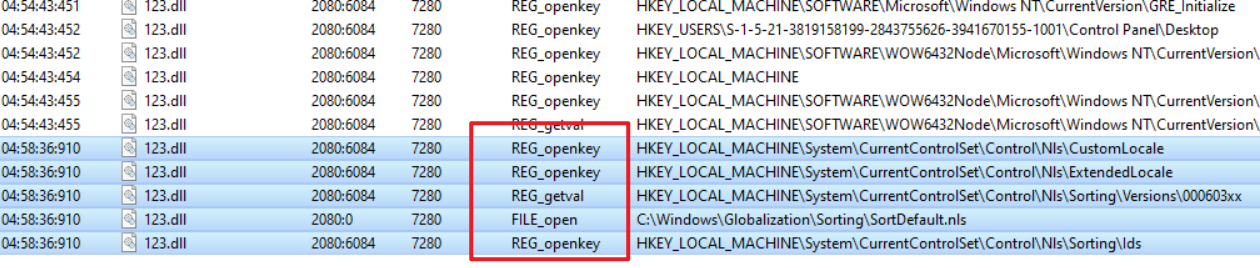
在main函数涉及的函数前都打上断点，开始运行

每个函数都打断点会出现一个问题，因为不是所有的函数都只被调用一遍的，在mian函数中对每个函数都断点会很复杂很麻烦，所以只选取几个进行断点跟踪。

在ollydbg加载该程序的时候，火绒剑就已经发现了部分行为，如图所示

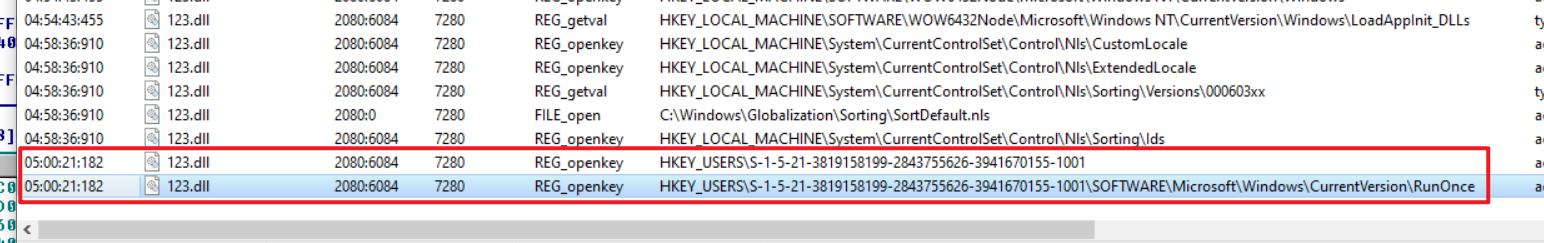


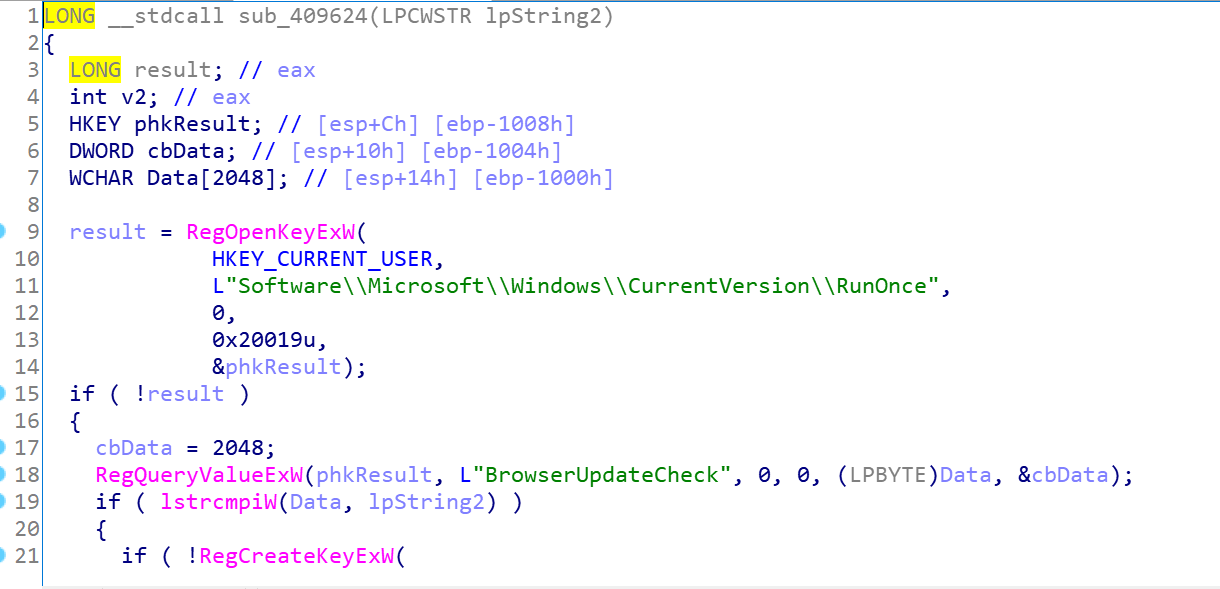
在sub409624的前后打上断点，在跳转到409624处时，该程序有下图所示行为



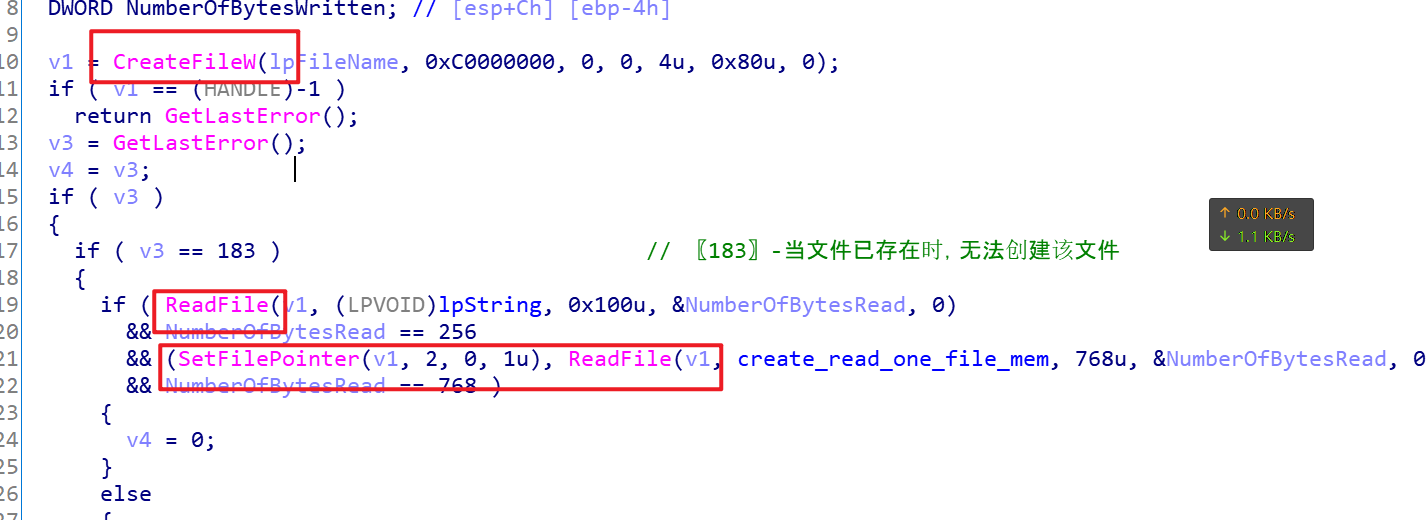
都是些注册表相关的行为。

运行完409624发现增加两条注册表操作

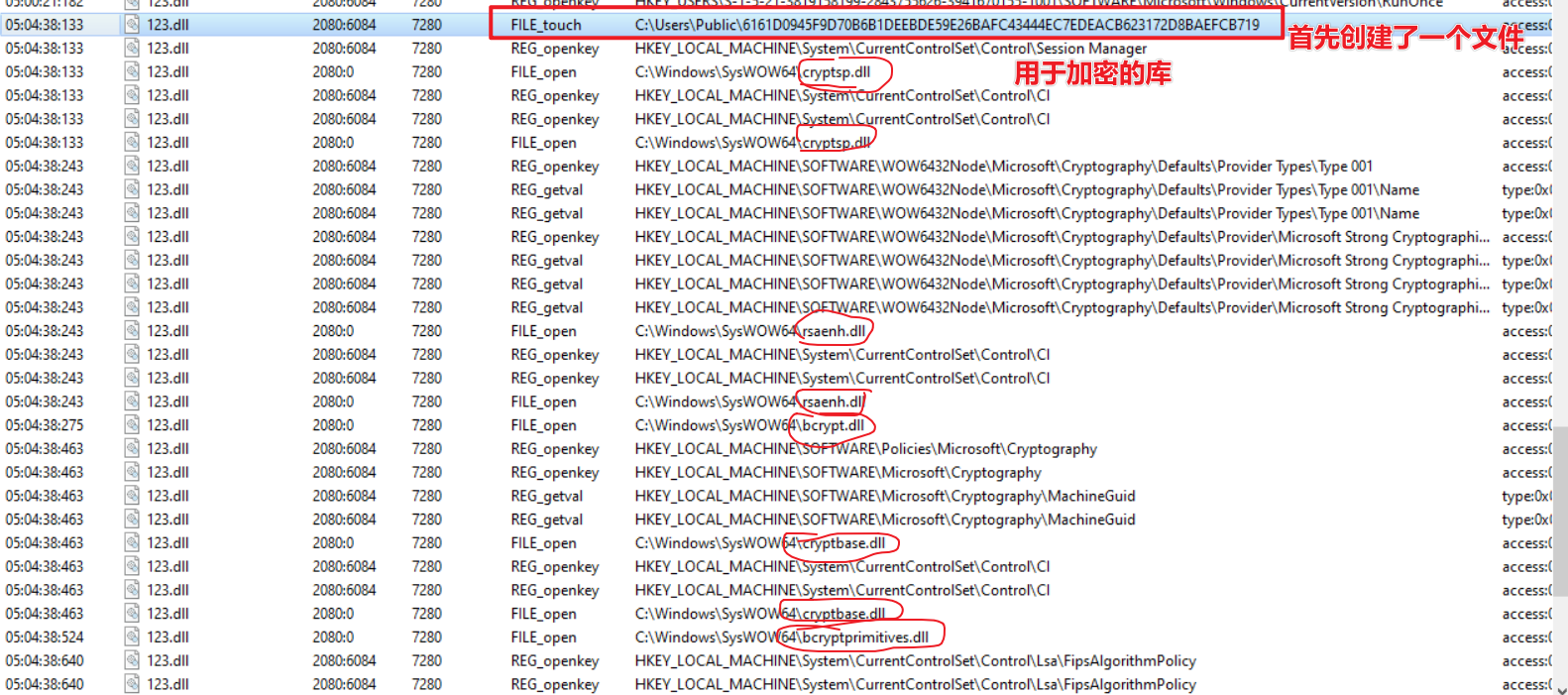


这与ida反汇编静态分析看到的代码一致。

接下来看409b4b，该函数从代码来看显然要创建并写入一个文件，打上断点并且运行

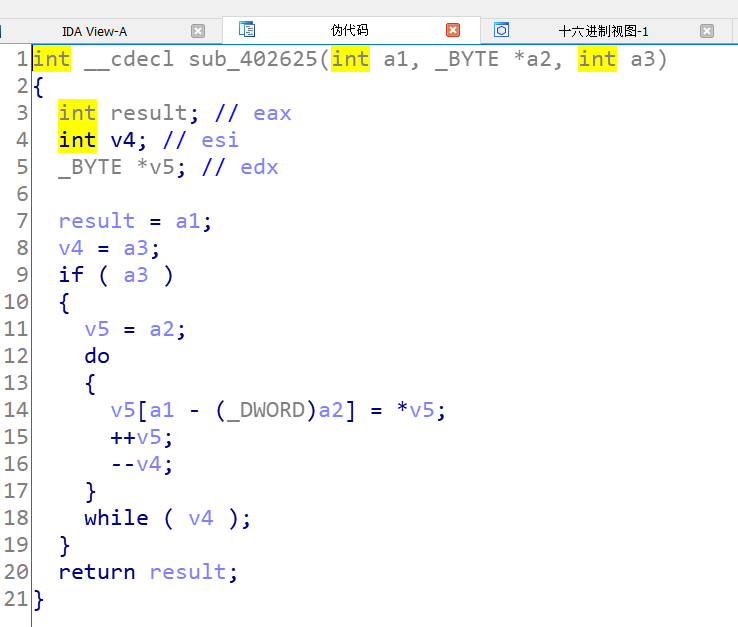


此次的行为很多



在C:\Users\Public\下创建了一个文件，然后调用了很多加密相关的库，然后写入并保存了该文件。猜测此处创建了一个文件，并且存储公钥或私钥等敏感内容，用于勒索。

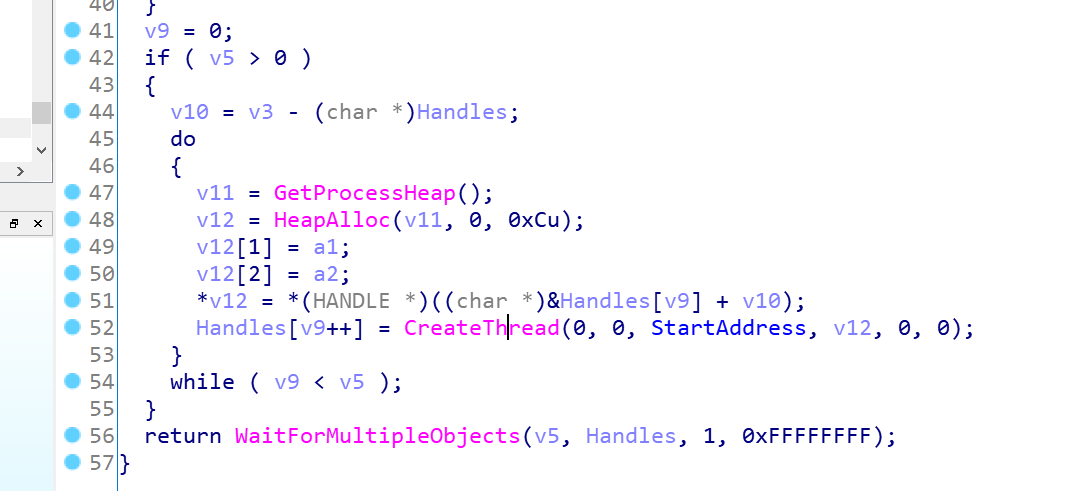
接下来看402625函数，该函数可读性很差



看代码并没有任何思路，因为只涉及运算，也没有调用其他内容，所以并没有任何异常行为。根据之前的经验，该函数会在很多地方被调用，所应该是进行某种常见运算。

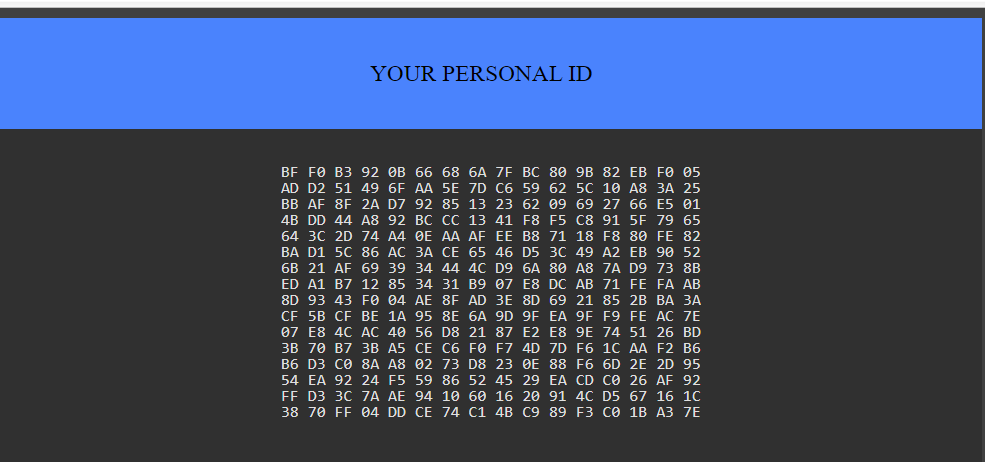
接下来看4099a3。

查看反汇编代码，有堆创建和线程相关的操作

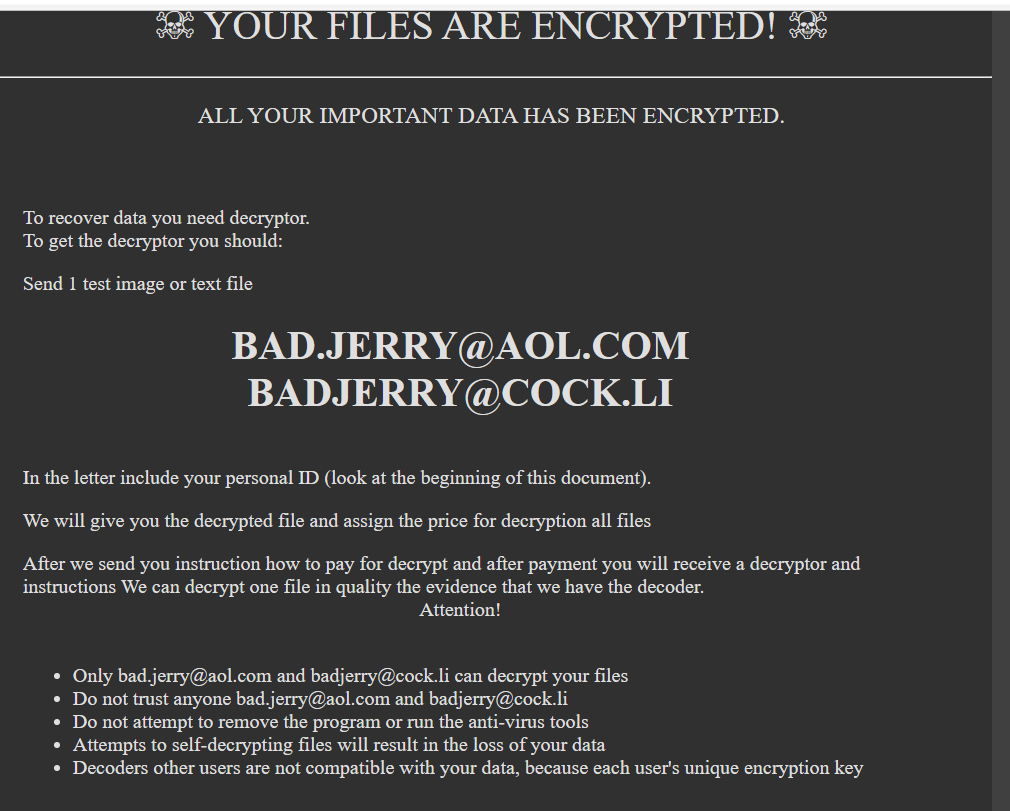


打断点查看行为，发现该函数是该恶意代码的主体，断点迟迟不结束，并且在行为处可以观察到有以下几个行为，首先是对注册表进行操作，然后遍历目录，打开C\Users\文件夹下的文件，并且对其进行修改和重命名。并且在特定的目录下释放了how\_to\_back\_files.html，用于告知受害者情况，并且提供解密的方法，进行勒索。

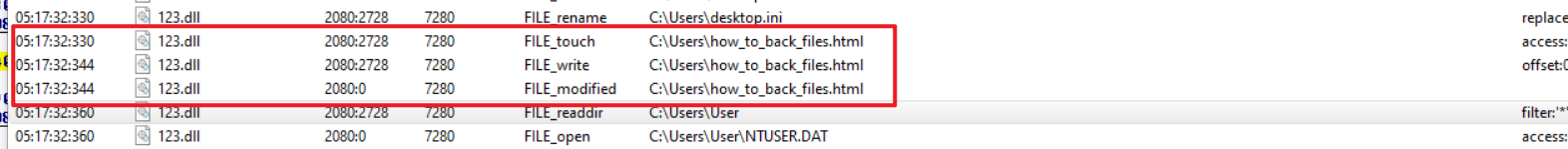
该文件打开后显示personal id



以及一些注意事项

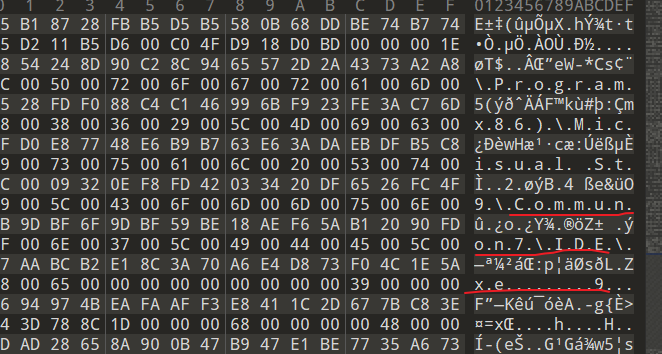


该文件在很多地方都有。释放文件的行为如下。

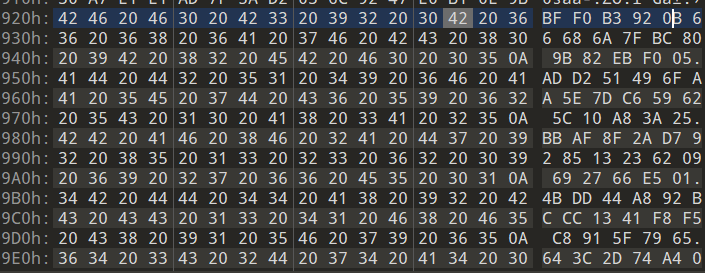


同时大部分文件被加密，少部分因为及时暂停，还没有被加密。

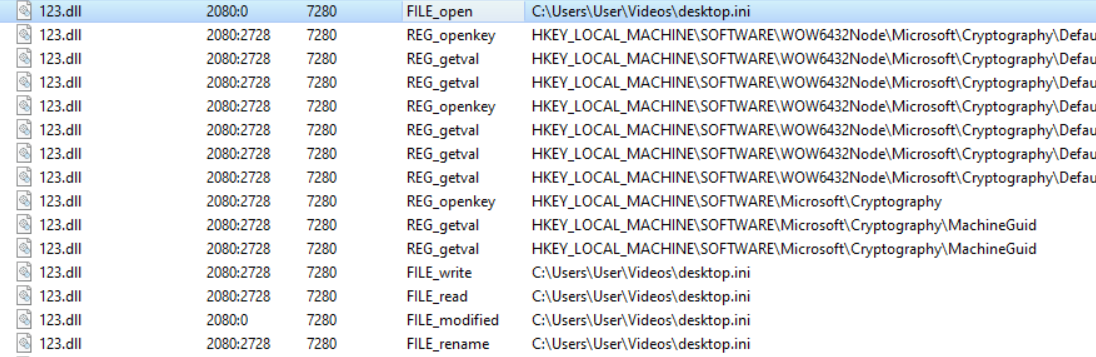
加密后的文件后缀名为xxx，用010编辑查看发现文件并非完全被加密，仍有部分原文件的特征，比如打开vs的快捷方式，发现在文件中仍有community字样，所以该加密算法不是每个字符都加密



并且在文件的最后，被添加了personal id



加密文件的行为如下



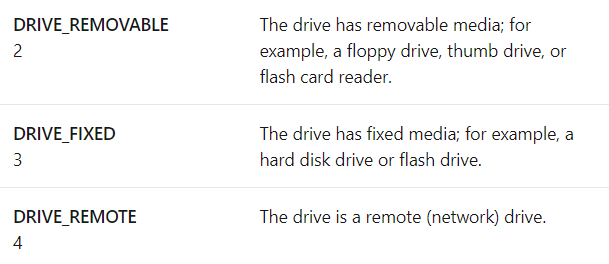
所以接下来对该函数进行进一步分析。

这个函数中有几个系统函数需要先了解一下。

GetLogicalDrives 用于获取当前所有的盘，并且按位映射

If the function succeeds, the return value is a bitmask representing the currently available disk drives. Bit position 0 (the least-significant bit) is drive A, bit position 1 is drive B, bit position 2 is drive C, and so on.

GetDriveTypeA用于获取当前盘的属性，其中返回值为2，3，4意义如下，所以该勒索软件只对这三种类型的盘进行感染。

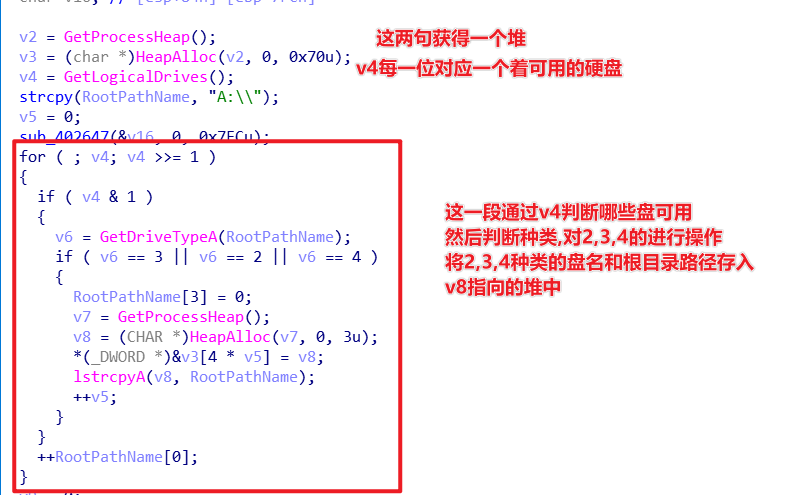


heapAlloc和GetProcessHeap共同使用用于申请当前进程的默认堆内存上的一个不可移动的空间，用法如下。

lpData = (LPData)HeapAlloc( GetProcessHeap(), HEAP\_ZERO\_MEMORY,sizeof(Data));

即在进程默认堆内存上申请了一个不可移动的空间，大小为sizeof(Data)的内存空间

所以分析代码如下。





看StartAddress函数

结构非常明确是, 遍历目录所有文件 , 然后对符合要求的文件进行加密，不全盘加密是防止系统不能正常运行。