2021/05/21_x86逆向C++_第8课_病毒分析

笔记本: x86逆向-C++
创建时间: 2021/5/21 星期五 15:09
作者: ileemi

课前会议

```
00000000 _EH4_SCOPETABLE_RECORD struc ; (sizeof=0xC, align=0x4,
copyof_10)
00000000 ; XREF: _EH4_SCOPETABLE/r
00000000 EnclosingLevel dd ?    // 等级 代表数组下标
00000004 FilterFunc dd ? ; offset
00000008 HandlerFunc dd ? ; offset
0000000C _EH4_SCOPETABLE_RECORD ends
```

__try{}__except{} 也使用 SEH 异常（会注册SEH），表只有一个。没有数据类型一说，所有异常都会接收、处理。

__finally -- 每次抛异常需要执行的函数，由 ScopeRecord.HandlerFunc 决定。

病毒的种类

病毒：具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。计算机病毒的生命周期：开发期→传染期→潜伏期→发作期→发现期→消化期→消亡期。

> 感染型、远控型、家族型。附带型病毒、蠕虫病毒、可变病毒。

木马（Trojan）：是具备破坏和删除文件、发送密码、记录键盘和攻击Dos等特殊功能的后门程序。木马病毒其实是计算机黑客用于远程控制计算机的程序。

网络病毒：通过计算机网络感染可执行文件的计算机病毒。
文件病毒：主攻计算机内文件的病毒。
引导性病毒：是一种主攻感染驱动扇区和硬盘系统引导扇区的病毒。

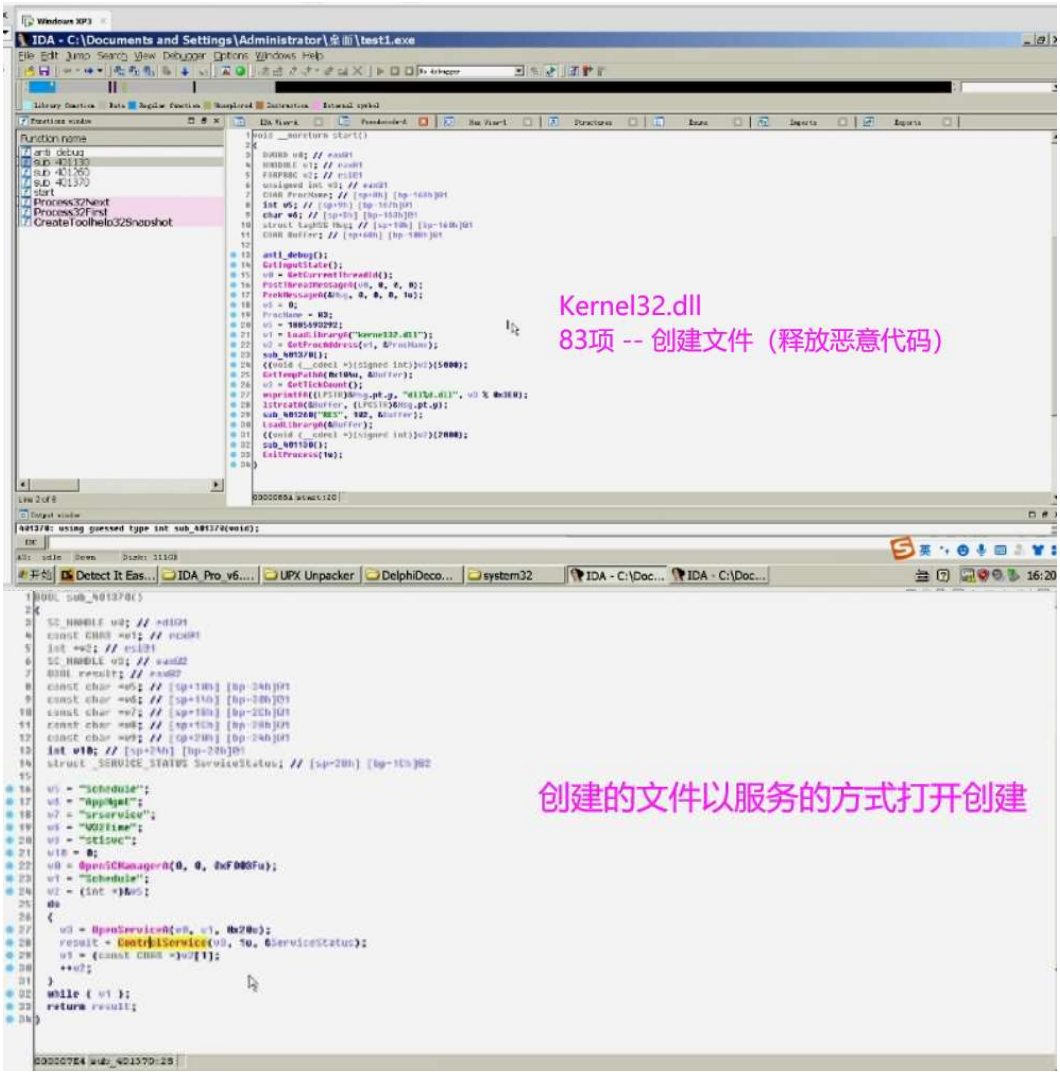
病毒自身没有恶意代码，启动程序会释放出可以代码，通常以服务方式运行。

病毒的分析

PEID原理：根据程序入口代码特征分析。PEID特征库较老，现在多使用DIE、Exeinfo等工具。

1. 分析病毒之前，安装分析、测试虚拟环境（win7最好，适合大部分分析工具）。
2. 查壳，确定可疑程序的开发语言以及编译器版本。根据程序对应的开发语言选择对应的反编译工具。（家族样本 -- autorun -- 9be5xxxx 为例）
3. 脱壳（可使用对应的脱壳工具）
4. 使用反编译工具分析代码流程（比如使用IDA分析是否由反调试代码）
5. 动态调试（结合IDA，定位反调试、加密等代码），获取释放的文件（存在可疑代码，母体程序中一般不会存在恶意代码），再次进行分析，如果依然存在释放文件，依然需要进行分析。
6. 编写详细的分析报告。

反调试代码：



格式化字符串，释放可疑.dll文件（LoadResource -- 可以代码可能存放在资源中，所以就需要通过资源句柄获取可以代码），之后加载.dll。

获取释放dll中释放的文件：

- 通过上下文API（CreateFileA为例）下断点（过反调试），等待目标文件释放，再次分析可以文件。

- 再测试环境由快照的情况下且dll中释放的文件名固定时，可直接运行可疑程序，搜索目标文件，找到后做备份，还原系统，分析目标文件即可。

dll中的反调试需要在 LoadLibraryA/W API出下断点，等待可执行程序加载目标dll，定位入口（直接修改EIP为dll的入口地址，会导致堆栈不平衡），再过反调试。

家族样本 -- autorun -- 9be5xxxx 为例：

xxx.exe
xxx.dll
xxx.sys -- Hook SDT表

> 使用软件行为监控工具可快速分析可疑程序是否是一个病毒程序（对于没有读写进程，没有操作文件、注册表、也没有产生网络行为的程序就不可能是一个病毒程序，也就不需要再进行静态分析）。

病毒对虚拟机的检测：简单做法就是扫描虚拟机进程是否存在。