# 恶意代码沙箱规避行为检测分析系统

闫佳 黄桦烽 杨轶 刘青芳 苏璞睿
{yanjia,purui}@iscas.ac.cn

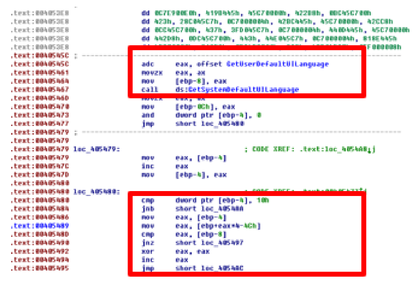
APT攻击中高对抗样本通过各类技术手段规避动态沙箱检测，导致样本行为触发不充分，攻击检测和机理分析困难。本系统针对该问题，提出基于高精度数据流分析技术对恶意软件的环境探测行为进行检测，进而基于执行环境地主动构造，实现恶意软件多路径分析，提升特种恶意软件的行为触发能力和机理分析能力。

规避卡巴斯基的动态检测

```
v0 = CreateToolhelp32Snapshot()
while(Process32Next(v0, &pe))
   if(strnicmp(pe.szExeFile,”avp.exe”,4)==0)
       return 1;
}
return 0;
```

在特定语言环境下才激活攻击行为

```
v0 = GetSystemUILanguage()
if(v0 == 0x419 || v0 == 0x422)
       return 1;
}
return 0;
```



解决的技术问题包括：

1）错误标记：程序中正常的依赖外部环境的路径分支条件；

2）编码、加密函数的识别和绕过：此类函数会导致路径条件求解困难；

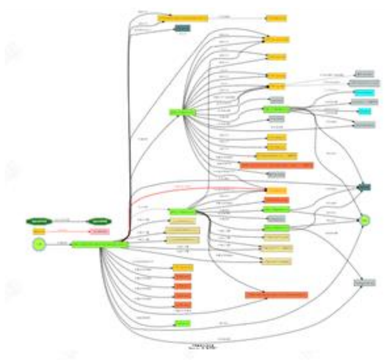
3）个别路径执行条件无法求解，难以构造执行环境；

本系统基于所在团队AOTA系统和金刚系统实现，采用了高精度污点分析和启发式行为分析方法，基于纯硬件层数据恢复沙箱规避行为上下文依赖条件，进而基于硬件模拟技术环境操控优势，在虚拟硬件层修改特定数据，直接干预程序运行，通过强制条件翻转和依赖环境修复触发更多恶意行为。

- 实现了15种规避行为的检测和特征抽取，以及基于规避特征的执行环境主动构造。
- 针对150个样本，平均分析耗时是 3分钟左右（记录Trace： 120秒，污点分析+符号执行+规则匹配： 62秒)。
- 针对CNCERT提供的大规模测试数据集，恶意代码关键行为触发率较未使用前至少提高57%以上。

| 序号 | 反沙箱探测行为 |
|---|---|
| 1 | 指定目录是否存在 |
| 2 | 磁盘类型检测 |
| 3 | 指定文件是否存在 |
| 4 | 内存大小检测 |
| 5 | 互斥量存在检测 |
| 6 | 指定注册表键是否存在 |
| 7 | 系统界面语言探测 |
| 8 | 指定URL是否可访问 |
| 9 | 指定标题窗口是否存在 |
| 10 | 指定名称进程是否存在 |
| 11 | 当前样本路径检测 |
| 12 | 注册表键值是否包含某特定字符串 |
| 13 | 当前用户是否是指定用户名 |
| 14 | 计算机主机名检测 |
| 15 | 主机CPU核数检测 |

原始报告行为



创建互斥量 ___PasswordList___

环境探测行为

| 进程 | 行为信息概要 |
|---|---|
| b5085d1c9b420e3 : 1636 | MUTEX_EXIST(“_x_X_UPDATE_X_x_”) != 183 |
| b5085d1c9b420e3 : 1636 | MUTEX_EXIST(“***MUTEX***_PERSIST”) != 183 |
| b5085d1c9b420e3 : 1636 | HANDLE_OF_FILEPATH(\\.\NTICE) == 4294967295 |
| b5085d1c9b420e3 : 1636 | MUTEX_EXIST(“_x_X_PASSWORDLIST_X_x_”) != 183 |
| b5085d1c9b420e3 : 1636 | MUTEX_EXIST(“_x_X_BLOCKMOUSE_X_x_”) != 183 |
| b5085d1c9b420e3 : 1636 | MUTEX_EXIST(“***MUTEX***”) != 183 |
| b5085d1c9b420e3 : 1636 | HANDLE_OF_FILEPATH(\\.\SICE) == 4294967295 |

1 到第 1 页 确定 共 7 条 10 条/页

重新配置环境并上传

主动构造环境后行为