# Tssk.sys分析报告

该驱动主要用于防止各类已知rootkit驱动的攻击，有很多恢复系统函数的操作，具体过程不详细介绍，看idb即可。

目录

[Tssk.sys分析报告 1](#_Toc433295717)

[一、 基础库 2](#_Toc433295718)

## 基础库