# 免杀学习

恶意软件

分类

病毒、木马、蠕虫、键盘记录、勒索软件、僵尸程序、流氓软件

- 用户非自愿的情况下执行安装
- 出于某种恶意目的

防病毒手段(事后手段,发展落后于病毒)

- 杀毒软件/防病毒软件
- 文件/数据流

目前主流恶意程序检测原理

- 基于二进制文件特征签名的黑名单检测方法
- 基于行为的分析方法(启发式)

免杀技术

修改二进制文件中的特征字符

- 替换\修改\擦除

加密技术

- 通过加密使得特侦字符不可读,从而逃避AV检测(AV防病毒软件)
- 运行时分片分段的解密执行,注入进程或AV不检查的无害文件中

防病毒软件的检测

- 恶意程序本身的特征字符
- 加密器crypter的特征

恶意检测网站

- https://www.virustotal.com/

免杀思路

代码混淆、代码洞、定制编码