



Windows安全工程师

基本信息

姓名：魏星宇

出生日期：1998.12.13

住址：浙江省绍兴市

2020 届本科毕业

联系方式

QQ: 1013503897

手机: 17629281378

邮箱: 1013503897@qq.com

教育经历

长安大学

电子信息类

2016 年 -2017年

计算机科学与技术

2017 年 – 2020年

个人技能

- 熟悉 C/C++ 编程开发;
- 熟练运用 OD、IDA、WinDbg 等调试器进行代码调试和逆向分析;
- 熟悉 Windows 系统原理、Windows 驱动开发, 掌握 PE 文件格式;
- 掌握多种 Windows 平台的 HOOK 注入方法;
- 熟练掌握 x86/x64 汇编语言;
- 了解通信模型与协议;
- 了解Python/Java编程开发;

项目经历

安全卫士

基于MFC实现的安全卫士, 功能如下

1. PE文件分析, 模仿CFFExplorer界面, 解析PE文件, 支持快捷方式、32/64位PE文件等, 包含快速反汇编分析、HexEditor功能。
2. 进程枚举与分析, 模仿火绒剑界面, 枚举进程并可获取线程、内存、句柄、堆等相关信息。
3. 钩子扫描查找, 模仿火绒剑界面, 扫描指定进程的IAThook、EAThook与InlineHook, 扫描Windows消息钩子, 扫描SSDT hook, 并可进行简单的恢复。
4. 加载驱动并遍历系统的驱动模块信息, 通过IoControlCode与本程序通信。
5. 借助微软Detour库, 实现指定进程的常用API监控功能。
6. 文件分析与清理, 实现文件树控件, 遍历文件夹, 显示文件信息, 删除指定后缀文件。
7. 服务信息的遍历与操作。
8. 通过注册表操作实现启动项管理和软件卸载功能。
9. CPU与内存占用的实时显示, 内存与CPU占用释放功能。
10. 通过文件的MD5值与特征码实现病毒查杀, 可以增删改查本地病毒库。
11. 云病毒查杀, 编写服务器与客户端通过IOCP与OPEN-SSL进行加密通信, 服务器通过MySQL数据库保存病毒样本的MD5值、样本文件路径等数据, 客户端可进行样本文件上报/删除, 对指定路径进行扫描。
12. 窗口信息的遍历与操作。
10. 各种安全技术相关的功能模块, 包括快速反汇编, 注入工具, 一键开关机, 文件捆绑与分割机, 驱动加载器等等。

(Github: <https://github.com/1013503897/WxySecurityGuard>)

逆向分析勒索病毒 “WannaCry”

1. 逆向分析勒索病毒 WannaCry 本地部分的加解密文件与释放病毒的过程。
2. 包括了图片文件、加解密程序和多国语言包等, 运用资源函数进行导出; 导出并使用动态库中的函数进行加密操作;
3. 创建多个线程定期检测有无新文件, 通过后缀名加密指定类型文件, 并伴随创建临时文件夹, 修改注册表等行为。检测有无密钥, 有就进行解密;