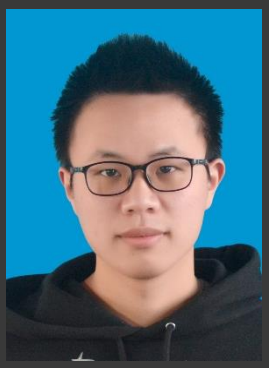

安全开发工程师

基本信息

姓名：魏星宇

出生日期：1998.12.13

住址：浙江省绍兴市

2021 届本科毕业

联系方式

手机：17629281378

邮箱：weixingyu@360.cn

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-2021年

实习经历

安全开发工程师

360企业安全集团-漏洞研究院

2020.7.6-至今

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 Winodws 系统原理、Winodws 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/C#编程开发；

项目经历

基于MFC的Windows平台安全卫士

1．PE文件分析，模仿CFFExplorer，包含反汇编分析、HexEditor功能。

2．进程枚举与分析，模仿火绒剑，枚举进程并可获取线程、句柄等信息。

3．钩子扫描查找，模仿火绒剑界面，扫描IAThook、EAThook与InlineHook。

4．通过文件的MD5值与特征码实现病毒查杀。

5．服务信息的遍历与操作。

6．通过注册表操作实现启动项管理和软件卸载功能。

7．安全技术相关的功能模块，包括快速反汇编，注入工具，驱动加载器等。

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

基于进程注入的Linux平台端口复用

1. 加载自定义.so文件，注入SSH/Apache2等端口通信进程。
2. Inline Hook accept/read/write等函数。
3. 识别自身流量，并劫获套接字。
4. 复用对方服务端口，加密转发自身流量，实现反弹Shell、文件传输等功能。

（ Github：https://github.com/1013503897/port_resue ）

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；