

# 迈克·史密斯

目前公司：太子集团旗下某公司

目前职位：研发工程师

工作年限：5年以下

## 基本资料

年 龄：28

性 别：男

微 信：undef\_future

目前状态：在职

婚姻状况：未婚

邮 箱：binlife.me@gmail.com

Telegram:

所在地点：柬埔寨 金边

## 职业意向

期望行业：计算机软件

期望方向：安全、游戏

期望地点：无要求

入职时间：尽快

期望年薪：面议

目前年薪：3.3\*13

## 工作经历

2019.6 - 至今 柬埔寨太子集团旗下某公司

公司性质：民营

公司规模：1000-3000 人

公司行业：

工作地点：金边

担任职位：逆向开发工程师

所在部门：研发支持中心

时 间：2019.5 - 至今

薪酬状况：33000 元 / 月

下属人数：0

2017.3 - 2018.11 北京天融信科技股份有限公司

公司性质：民营·上市企业

公司规模：2000-5000 人

公司行业：网络安全

工作地点：北京

担任职位：研发工程师

所在部门：安全开发部

时 间：2017.3 - 2018.10

薪酬状况：20000 元 / 月

下属人数： 0

2014. 05-2017. 2      **安徽省奥创科技有限公司**

公司性质： 私营 • 民营企业

公司规模： 50-99 人

公司行业： 计算机软件

工作地点： 合肥

担任职位： 开发工程师

所在部门： 研发组

时      间： 2015. 05-2017. 2

薪酬状况： 8000 元 / 月

下属人数： 0

担任职位： 开发工程师

所在部门： 研发组

时      间： 2014. 05-2016. 5

薪酬状况： 6000 元 / 月

下属人数： 0

2010. 05-2013. 5      **中国电信**

公司性质： 国有企业

公司规模： 500-1000 人

公司行业： 通信

工作地点： 兰州

担任职位： 维护工程师

所在部门： 综合维护部

时      间： 2012. 11-2013. 11

薪酬状况： 3000 元 / 月

下属人数： 0

担任职位： 实施工程师

所在部门： 综合维护部

时      间： 2010. 11-2012. 11

薪酬状况： 2800 元 / 月

下属人数： 0

担任职位： 客服

薪酬状况： 客服部

时      间： 2010. 5-2010. 11

所在部门： 2500 元 / 月

下属人数： 0

教育经历

培训机构（ 2013.05 - 2014.05 ）

专业名称： 分析开发工程师      学历： 大专      是否统招：

否青岛拓谱信息工程学院（ 2006.02 - 2009.02 ）

专业名称： 物流管理      学历： 大专      是否统招： 否

## 项目经历

### 私服相关（金边）

项目职务： 游戏开发/逆向

项目描述： 协助脚本组和运营组解决日常中客户端和服务端出现的bug等。

项目业绩：

1. 修复客户端崩溃bug若干，包括但不限于同步官方资源、新加代码、编码、网络等等引起的崩溃
2. 修复服务端崩溃
3. 编写简单反外挂，缓解打金问题
4. 其他游戏相关工具和插件编写  
如：GM工具编译、改写、增加功能如：对接H5游戏插件编写

### 样本分析

项目职务： 安全研究员

项目描述： 分析 Windows、Linux、安卓下恶意样本，有时只鉴定黑白。Windows 占 80%，Linux 占 10%安卓10%。

项目业绩：

1. Linux 下XorDDOS 变种分析，给出清理方案，并帮助三家客户手动清理
2. 若干 Linux 样本，可以手动清理的给出清理方案，不能清的理形成分析报告
3. 少量安卓样本（有混淆、无壳）

### 漏洞相关

项目职务： 安全研究员

项目描述： 包括漏洞复现、分析、挖掘。

项目业绩：

1. 针对 CVE-2019-0708的热补丁demo(个人)
2. 挖掘某款云存储设备命令注入漏洞（0day），通用性50%，通过zoomeye搜索关键字可发现全球 600 万台设备
3. 挖掘 Windows 下某款 PCB 设计软件本地代码执行漏洞（0day）
4. MS17-010 复现，使用泄露工具和 MSF 验证，并给出缓解方案
5. 针对 CVE-2018-7886 分析、复现并编写弹出计算器的 poc

### 其他安全研究

项目职务： 安全研究员

项目描述： 安全工具开发，针对国内某个人云摄像头安全研究。一些安全工具开发。

项目业绩：

1. 针对系统远程桌面登录组件，编写获取密码工具
2. QQ聊天记录获取（本机，非协议）
3. 多款 Browser 的历史记录获取
4. 研究国内某厂商云摄像头，发现未授权访问缺陷，并研究半自动植入方案
5. 编写ring3 shellcode若干

## 网站漏洞批量检测

项目职务： 安全研究员

项目描述： 根据输入的关键字结合爬虫程序提取URL，批量检测struts2 框架漏洞模块，并预留接口以支持更多版本检测。

项目业绩：

1. 谷歌、百度爬虫（谷歌有验证码）
2. 支持 http/https 协议
3. 支持 Windows 和Linux（Linux 只有控制台版本）
4. 支持关键字分组

## 端游安全加固

项目职务： 游戏安全工程师

项目描述： 对端游客户端进行安全加固，包括客户端和网络封包加固。建立完善的加固和测试流程并文档化。

项目业绩：

1. 客户端自校验
2. DLL注入检测
3. 封包合法性检测，加入按装检

项目职务： 安全研究员

项目描述： 更新、维护原有代码，编写相关文档，并且将半自动全部为全自动。负责筛选新人并指导快速上手业务

项目业绩：

1. 加入19 款游戏，累计支持 58 款热门游
2. 封包合法性检测，加入按装检测
3. 加入获取机器码模块
4. 加强网络验证，增强客户端授权安全性
5. 验证服务器环境由 Windows+MFC 改为 Linux 下，由 MSSQL 改为 MySQL
6. 优化查询，改为纯内存查询
7. 指导新同事熟悉框架

## 多款页游半自动广告程序开发

项目职务： 开发工程师

项目描述：

1. 加入新功能，如检测好友在线状态、检测好友等级、邀请好友入帮、批量删除好友
2. 分析竞品实现竞品全部功能，如批量登录、自动移动、自动任务、自动加好友、自动消息等
3. 编写防破解相关代码，使用 VMP 加密客户端授权相关模块
4. 编写服务端验证代码，使用 MFC 异步选择模型+MSSQL 数据库，实现可承载 5000 左右连接服务端程序
5. 分析竞品实现其所有功能，并加入新的功能，独立实现客户端和服务端验证程序，主要功能为通过程序半自动实现在游戏中私聊、公聊广告的目的

项目业绩：

支持游戏以下：

火影忍者（腾讯平台）  
灵域（腾讯平台）

原始传奇 (51.com)  
仙魂 (腾讯平台)  
苍穹变 (腾讯平台)  
霸图 (4399.com) 等 39 款热门游戏

### 某端游自动化工具编写 (个人)

学习项目

项目职务: 学员

项目描述: 分析游戏关键数据及核心 CALL 调用并编写自动化工具进行游戏, 提升分析经验

项目业绩:

1. 完成地图怪物位置数据基址的定位
2. 完成游戏吃血 call, 攻击 call, 移动 call 的查找
3. 完成自动化程序编写, 通过本地回环进行通信, 将核心模块注入游戏进程, 获取关键数据信息
4. 回传控制端, 控制端进行判断并发送对应控制指令进行自动化打怪吃血等
5. 完成基本人物属性信息数据的基址定位 如血液 攻击力等

### windows 用户层调试器 (32 位)

学习项目

项目职务: 学员

项目描述: ring3调试器 支持 32 位程序的动态调试

- 完成调试器框架编码与设计
- 完成 T 命令. 单步步入
- 完成 P 命令. 单步步过
- 完成 G 命令 运行到指定地址, 如不带参数, 直接运行
- 完成 D 命令 显示指定地址的数据
- 完成 U 命令 反汇编指定地址的代码, 参数为空则反汇编当前 EIP 处的代码
- 完成 E 命令 修改某地址的数据, 可以修改为 16 进制值也可以修改为字符串
- 完成 MEM 命令 查看内存属性信息
- 完成 bp 命令 支持多断点 临时断点 永久断点
- 完成 bc 命令 清除断点 bc 指定断点 ID
- 完成 bl 命令 查看所有普通断点
- 完成 bh 命令 下硬件访问、写、执行断点 执行断点默认为 1 字节访问断点
- 完成 bh1 命令 查看硬件断点列表
- 完成 bhc 命令 删除硬件断点 参数断点序号
- 完成 bm 命令 内存断点 支持访问断点和写断点, 支持内存断点跨页, 支持多内存断点
- 完成 bml 命令 查看所有内存断点
- 完成 bmp1 命令 查看内存分页断点
- 完成 bmc 命令 删除内存断点 参数断点序号
- 支持对同一地址下内存断点硬件断点和普通断点
- 完成 r 命令 查看寄存器 带参数则修改指定寄存器的值
- 完成 mdl 命令. 显示加载模块列表
- 完成间接 call API 名称解析
- 完成间接 jmp [XXX] API 名称解析
- 完成 Trace 命令, 指定一段地址, 和 DLL 名称若 DLL 名称为空则跟踪从指定起始地址到结束地址的所有代码, DLL 不为空则只记录该地址段内对指定 DLL 的访问代码, 若无参数则跟踪地址为

主模块范围内的代码，遇见 CALL 进入是主模块的话执行 T，否则执行 P 命令

项目业绩： 深入了解调试器原理，有助于开发排错

### 学生信息管理系统(3 层架构)

学习项目

项目职务： 学员

项目描述： 学生信息管理系统 用来统计学生信息及考勤安排

项目简介：

1. 实现对学生信息，老师信息，课程信息进行管理，支持增、删、查、改。
2. 建立本地缓存池，避免每次都从服务器获取数据,有效缓解了服务端的压力
3. 三层架构模型，分层设计，分为客户端 中间层 和 服务端，提高程序安全性和扩展性
4. 采用连接池 和 缓冲池，预先开启合适数量的线程和数据库连接对象，减少高并发短连接时频繁创建线程关闭线程等操作带来的资源浪费问题
5. 支持安卓客户端

项目业绩： 独立完成编码、测试、优化工作

## 技能列表

开发技能：

1. 熟练掌握 Windows 开发
2. 熟练掌握 MFC 界面框架编程
3. 熟练掌握 STL
4. 熟练掌握网络编程、多线程、进程通信、Windows 程序性能优化
5. 熟练掌握 Windows 逆向

编程语言：

熟练掌握 C/C++、了解 Python 、Java

IDE：

熟练使用Virtual studio、了解 QT Creator

调试工具：

WinDbg、Wireshark、IDA、OD、Sysinternals Suite

## 个人描述

自我评价：

善于沟通、积极主动渴望学习新知识。

*对漏洞、木马、攻防有强烈兴趣，希望结识更多有意思的朋友*