赵建祖

男 · 36岁 · 工作13年1个月 · 保密 · 北京-海淀区 · 本科 · 其他

13011206207

276793422@qq.com

优势亮点

web版简历：http://sqlxss.com/job.html

（web版简历更详细一些，项目细节支持折叠，看着也更方便一点，部分点有图示说明）

擅长思考，擅于总结，有流程化思考的习惯。知识面较广，熟悉跨端、跨平台开发及产品架构设计。

熟悉Windows开发，熟练掌握C/C++语言，熟悉Python、Go、C#语言，了解Rust、JS 语言。

求职期望

在职，看看新机会

C++　50-70k×15薪 | 北京 | 计算机软件

工作经历

联想北京　2022/06-至今

dev

职责业绩：联想集团“设备互联”项目，底层功能解决方案提供，底层功能架构设计。
带领团队同事一起做底层功能代码研发。
带领团队同事一起做底层模块、设备的操作分析，做各种可能的优化。
从0 到1 的团队组建，从0 到1 的产品开发全流程参与，从0 到1 的SDL 融入组内。
于2024年8月18日换部门。在新部门任PC客户端资深开发岗位。
负责组建团队、底层开发、疑难问题攻坚、预装问题分析、BUG分析等众多高难度问题。

珠海豹趣科技有限公司　2020/06-2022/06

资深C++驱动开发工程师

职责业绩：负责针对金山毒霸的防御体系，对现有防御功能进行改进并使其增强。
产品新增功能开发。应急响应、处理相关开发工作。
应用层相关接口开发。Windows驱动开发。金山毒霸的资源、性能优化。
基于ATT&CK矩阵的数据收集模块开发。

联想(北京)有限公司　2020/03-2020/06

高级攻防架构师

职责业绩：工作内容包含但不限于：

1. 设计基于Windows内核架构的立体攻防架构。
2. 设计和带领团队开发攻防模块，保护联想PC软件文件、进程和功能不受竞争对手攻击。
3. 研究竞争对手攻击行为，制定保护和反制措施。
4. 协助产品和项目经理按时完成项目开发任务，并给予团队开发成员技术指导和设计支持。

北京搜狗科技发展有限公司　2015/01-2020/03

高级开发工程师

当前薪资：1000元 × 14薪
汇报对象：部门负责人
下属人数：3

职责业绩：主要是带领兄弟们做各种分析，
以及研究对抗方案，更新方案优化代码，持续对抗等。
1.主页攻防（主页反劫持，长期保持反劫持成功率70% 以上）
2.推广攻防（推广安装，日装成功几十万级）
3.数据监测（每日分析处理若干个数据源，每个均为十亿级的数据）
4.竞品对抗（PC对抗开发，千万级DAU）
5.客户端开发（PC客户端开发，亿级DAU）
6.友商合作（主要是QM）
7.客户端防护（浏览器自保）

项目经验

设备互联三期项目（SmartConnect） 2023/09-至今

软件开发

项目描述: 基于联想早期开发的设备互联项目，新增功能。
实现手机、平板、PC 三端互联。

项目职责: PC端新功能的支持与设计，网络文件系统的功能的支持与定制，
虚拟目录层级结构的设计与开发，本地虚拟文件系统的支持与整合，
疑难问题的解决，BUG的解决，BSOD的解决。
编码规范的定制。

项目业绩: 在2023年9月份，四周的时间里，验证了四套不同机制的远程文件系统客户端方案，包括微软的 projfs、网盘文件系统、ftp、nfs，开发出原型并作对比。最后选择使用 nfs 作为我们的网络文件系统的支持。
在六周时间内，独立整合并修改了Windows端nfs文件系统的支持，并且对所使用模组内的异常点做针对性的修复，包括 R3 的异常和 R0 的 BSOD。
在10周时间内，独立完成了底层功能的改进，新机制的增加，如：网络文件系统虚拟目录层级，本地虚拟目录展示，文件访问缓存，等等。
以及后续的预装问题分析及BUG解决。最后保证产品于今年上半年正常发布。
PC产品在微软 AppStore 中可以下载，叫做【超级互联】，目录内 VaultPlugin 目录内，除 VaultPlugin.exe 外的其他模块均为我开发或集成。

OpenKylin Defend Sig 2022/07-至今

owner

项目描述: 其实就是个开源项目，基于Linux 内核的。
本人有幸参与到其中，作为防护系统的 Owner 及规划者，还是很不错的。
https://gitee.com/openkylin/community/tree/master/sig/defend
后续的计划是，在个人版OpenKylin上，实现类似于Windows Defender 相关的功能
目前sig 组人员还不多，还在扩充阶段，且后续的开发工作必然要求专业性非常高
本人也在和开源社区想办法讨论后续如何完成我们开发计划的方案

项目职责: Owner
开发、项目规划、推进

个人项目——Windows平台驱动程序快速开发库 2018/01-至今

全

项目描述: 个人独立项目，旨在归纳总结个人曾开发的，一些小的驱动相关的功能，封装成LIB（或直接提供代码，主要是因为使用C++开发，有些类实现直接写到了.h文件里），供未来自己可能会使用的情况下使用它。
内部包含并整合了一些常规功能（memory、buffer、file、socket、callback等），非常规功能（驱动内存加载，驱动级Shellcode生成、执行，R0调用R3函数等），以及部分网上开源的项目库（如BBDriver等），还有一些开源的第三方支持库（如cJson、tinyxml、zlib、lua引擎、asmgen、asmjit等），还有一些对抗功能（自保、ARK、透传、劫持、欺骗等）。以C++的形式，封装成类，供使用者直接调用。

项目职责: 整体框架设计，接口设计，设计模式选择，开发，代码优化，重构。
直到现在，个人有什么好点子，想到哪些有趣的功能，仍然会向内部集成。

项目业绩: 此驱动可作为一个后门驱动驻留系统。
此驱动可直接作为一个EPP相关产品的驱动模块。
关键工作全部在驱动内部完成，高危工作反向调用应用层相关代码来执行。
代码于2020年出售过2套。

WiFi 模块传输速度优化分析 2023/06-2023/08

逆向开发

项目描述: 分析单网卡，在连接两个不同设备时，如何实现不同的速度。
这个问题其实是个机制问题，网卡的机制问题，一般来说由硬件厂商来解决。
我们这边和我们合作的硬件网卡厂商是 Realtek ，解决问题需要很久，所以这里领导决定我们自己尝试解决。

项目职责: 逆向三套不同的网卡驱动，分析802.11协议的流程，
以及网卡驱动内，如何设置一些特定的参数，这三套驱动均为 realtek 的驱动，无符号。
逆向的同时，开发驱动，做双机联调，一边分析系统驱动，一边劫持系统驱动，做验证。

项目业绩: 三星期时间摸清楚了三款驱动针对我们要处理的位置的执行区别。
并且给出反馈，需求本身做不到。受硬件限制做不到。
后续realtek 厂商反馈结论与个人结论一致。

WinPC，BLE扫描时间窗缩短 2023/04-2023/05

逆向开发工程师

项目描述: 这个活实际上是个逆向分析的活。我们通过低功耗蓝牙设备做近场周边设备发现。
由于硬件设备会周期性地扫描周边其他设备。
这个周期是两个WORD参数，在Android上有Jni层的接口，但是Windows上没有。
这里就是需要通过逆向分析等操作来研究寻找Windows上的这两个参数如何设置。

项目职责: 独立搜寻资料，寻找方案。独立逆向分析2~3个模块，寻找相关内容。开发辅助工具、脚本来实现相关的分析过程，如：https://github.com/276793422/IDAPython_WDFFunctionRepair。开发Demo，验证想法，确认功能。

项目业绩: 将BLE扫描的平均时间，缩短80%。
（即基于BLE的周边设备发现时间降低80%。）

设备互联一期项目（Freestyle） 2022/11-2023/04

研发

项目描述: 联想设备互联，让不同的设备连接到一起，包括PC、手机、平板等。

项目职责: 1：从底层功能开始构建联想的设备互联架构（国内版由我们团队负责，海外版由其他团队负责）
2：设计并带领团队开发、搭建跨端（端云）、跨平台（Windows/Android）的设备互联整体架构。
3：针对现有解决方案做流程梳理优化，并且提出新的更好的解决方案。
4：针对不同的硬件特性，做可能的定制化支持，发挥硬件的最大性能。
5：带领兄弟一起做功能分析，功能拆解，工期计划，以及最后确定工期和开发任务。
6：和兄弟们一起做开发。

项目业绩: 项目上，一期目标基本达成。
由于一些其他原因，导致我们团队同时也要为外部团队提供支持，从架构上解决了一套代码同时支持我们的框架以及海外版框架的需求。

设备互联底层工作（LDPP） 2022/07-2022/10
开发

项目描述: 开发我们自己的设备互联底层框架——LDPP。
功能是通过蓝牙做周边设备发现，然后通过WiFi做指定设备的自动化配对连接。
而我们只做如上两个功能。

项目职责: 做蓝牙通信协议定制，及WiFi连接后的双端验证功能定制。
和 Android 侧同事对接。
开发PC侧功能，并解决疑难问题。

项目业绩: 三个月时间的加班加点，每月工时近380小时。
独立完成了第一版PC部分的LDPP功能。

威胁溯源相关研发 2021/05-2022/06
研发

项目描述: 我们做杀毒软件需要随时跟踪恶意软件的行为。
但是恶意软件经常使用一些常规、非常规的方法做行为关系链的截断
针对现在市面上常用的行为关系链做断链溯源相关研究。
基于研究成果，做方案的研发，并且落地。

项目职责: 分析常用的行为关系链相关的系统执行流程。
Windows 系统自身就提供了若干种不同的远程行为执行方式。
需要针对系统提供的一些机制做原理性的分析，并且找到相关的处理方式。
针对基于分析结果，做理论验证，给出针对性的解决方案。
针对提出的解决方案上报上级领导，做可行性分析研判。
针对研判结果，将方案开发出来，并且落地。
上线，持续关注结果。

金山毒霸内核驱动开发、维护 2020/06-2022/06
开发

项目描述: 根据不同维度的数据收集点，需要对系统的不同维度数据做一个实时的观察、收集，
根据收集的数据后续做清洗，然后分辨恶意软件，
由于我们早期没有相关需求，所以内核里相关的数据收集点并不全面，

针对此种问题，需要添加数据收集点，获取对应而软件行为数据。

项目职责: 根据不同的需求，针对金山毒霸驱动模块做数据监视点的修改。
设计：由于早期驱动框架无法改动，库封装并不完善，
向框架内新增代码又比较困难，需要重复使用的一些常用的函数还要手动重新实现，
所以在有此驱动改动需求后，本人重新构思了一套库的引用方式，
重新对改动相关的各个点做处理，使新的代码，均使用我新的库，
且观察点部分，代码整理，让后续加入观察点更方便。
开发：代码编写。以及自测用模拟测试框架的开发。

金山毒霸主机防护功能开发、维护、升级、增强、分析 2020/06-2022/06

项目描述: 通过分析各种恶意软件，来获知毒霸主机防护可能存在的不足或缺陷
分析各类不足或缺陷，提出解决、增强方案
基于可行的解决、增强方案，针对金山毒霸，做功能上的增强

项目职责: 1：毒霸新功能模块的开发
2：毒霸现有模块的维护
3：毒霸现有安全功能的升级（降低误报，性能优化）
4：毒霸现有防护功能的增强（增加恶意软件的识别能力）
5：毒霸出现的一些崩溃分析（dump分析），以及一些系统的蓝屏dump分析

基于LLVM的Windows程序编译解决方案 2019/06-2020/05
全

项目描述: 由于攻防对抗需要，需要对代码做一定程度的保护，使用弱壳达不到保护的效果，但是由于效率问题又无法使用强壳，在这样一个背景下，我考虑将移动端上的代码保护解决方案移动到PC端上，即在Windows上通过LLVM来编译部分代码，最终实现对代码的保护。好处是，逻辑可控，保护强度可控。不足是，逻辑部分可能需要开发人员来编写，与使用现有解决方案相比，成本稍高。
LLVM使用版本为最新版本LLVM8.0.1（从4.0.0和6.0.0移植上来的）。

项目职责: 所有研究工作均为个人职责。研究基于Windows的LLVM编译框架，实现字符串加密、指令替换等功能。
实现基于Windows的编译阶段代码保护。研究整理业界常用PASS，移植进我们的Pass插件中。

项目业绩: 打通完整一套解决方案，并且可以实现LLVM在Windows平台上执行编译。
目前在准备向驱动方面兼容，使其可以编译驱动程序。

自动化主页反劫持对抗平台 2018/01-2020/03
设计、协调、开发

项目描述: 沟通测试人员、数据组同事，梳理完整对抗过程，整合数据资源、测试资源，
以流程化思考的方式分析每个细节，将每个需要人工参与的细节都使用自动化的方式替换掉，
最终将整个流程打造成一个闭环，用以实现对抗。
各个节点通过自研服务器的web hook 来做每一步功能的传递，实现从发布一版数据，到收回一版竞品对抗结果的完整闭环流程。

项目职责: 平台设计，完整的框架搭建，以及框架相关代码开发，包括如下：

1：不同服务器间的通信协议设计
2：不同服务器间的通信框架实现
3: 自动化数据分析服务器，分析处理客户端上报的数据

4：自动化数据编译服务器，编译相关数据的功能

5：自动化测试服务器，多平台方案同步测试分发框架，以及测试结果收集功能

6：自动提交上线功能软件，由于我们的策略部署上线平台无法支持自动部署，自动上线，所以这里我针对此做了处理

7：客户端数据处理功能

8：其他（数据分析插件框架等）

项目业绩: 流程自动，实现完整的自动化对抗闭环，部署完成后，真正的实现开发、测试人员零参与（数据无强烈波动的情况下）。
应对迅速，对手执行一次劫持行为后，我们的平台会在最短15分钟之内就检测到，最快2小时内会测试完新一批的数据，同时提交上线，最快4小时内课通过常规渠道下发至各个客户端。（早期由人参与时，手动对抗一版，至少要1~2人日）

云控平台开发维护升级（云端和PC客户端） 2016/01-2020/03

开发

项目描述: 云控平台相关。
以及云控平台相关的附属工作事宜。

项目职责: 客户端平台现有代码维护，客户端和云端平台升级方案制定，云端数据流量监视，
云端云控方案的分析，客户端代码编写，沟通友商、外包。

项目业绩: 客户端为亿级DAU的PC客户端产品。
客户端应用级的软件逻辑对抗，方案快速跟进迭代。
异常数据信息实时获取，云端以2小时为一个周期做解析。
主页反劫持，长期保持反劫持成功率70% 以上。
推广安装，日装成功几十万级。

自保护模块 2016/08-2017/03

设计、开发

项目描述: 基于Windows 驱动程序的自保护模块，通过云控下发策略，本地实现对应策略的保护，
来实现我们需要它保护的位置。（自保功能）

项目职责: 驱动部分的框架设计，驱动部分的开发，各版本迭代的开发，
云控相关的接口设计，本地对应接口的开发，应用层相关部分代码的开发。
此模块只有我一个开发，凡是能接触到代码的几乎全都是我做。

教育经历

吉林大学（第二学历）

本科 · 计算机科学与技术

2015/03-2017/09

语言能力

英语

普通话