游戏安全的攻防艺术

joeywzhu@tencent.com

2019.02

TenProtect Conficential, Copyright @Tencent, 2019

个人简介

- 2013至今， 腾讯游戏业务安全部技术专家
- 2005-2012， 趋势科技架构师

- 2005-2008，开发和设计 PE病毒沙箱
- 2008-2012, 开发和设计脚本漏洞分析引擎
- 2013 to now, 开发和设计游戏安全通用方案

- 2011.8 Defcon讲演 “Chinese phishing at **Defcon19**”, Las Vegas

TenProtect Conficential, Copyright @Tencent, 2019

1. 外挂是什么

TenProtect Conficential, Copyright @Tencent, 2019

多少秒扫雷能够完成

TenProtect Conficential, Copyright @Tencent, 2019

CrossFire透视外挂

TenProtect Conficential, Copyright @Tencent, 2019

CrossFire 手游透视外挂

注: 为了适应手游屏幕特点，手游上的外挂增加了射线

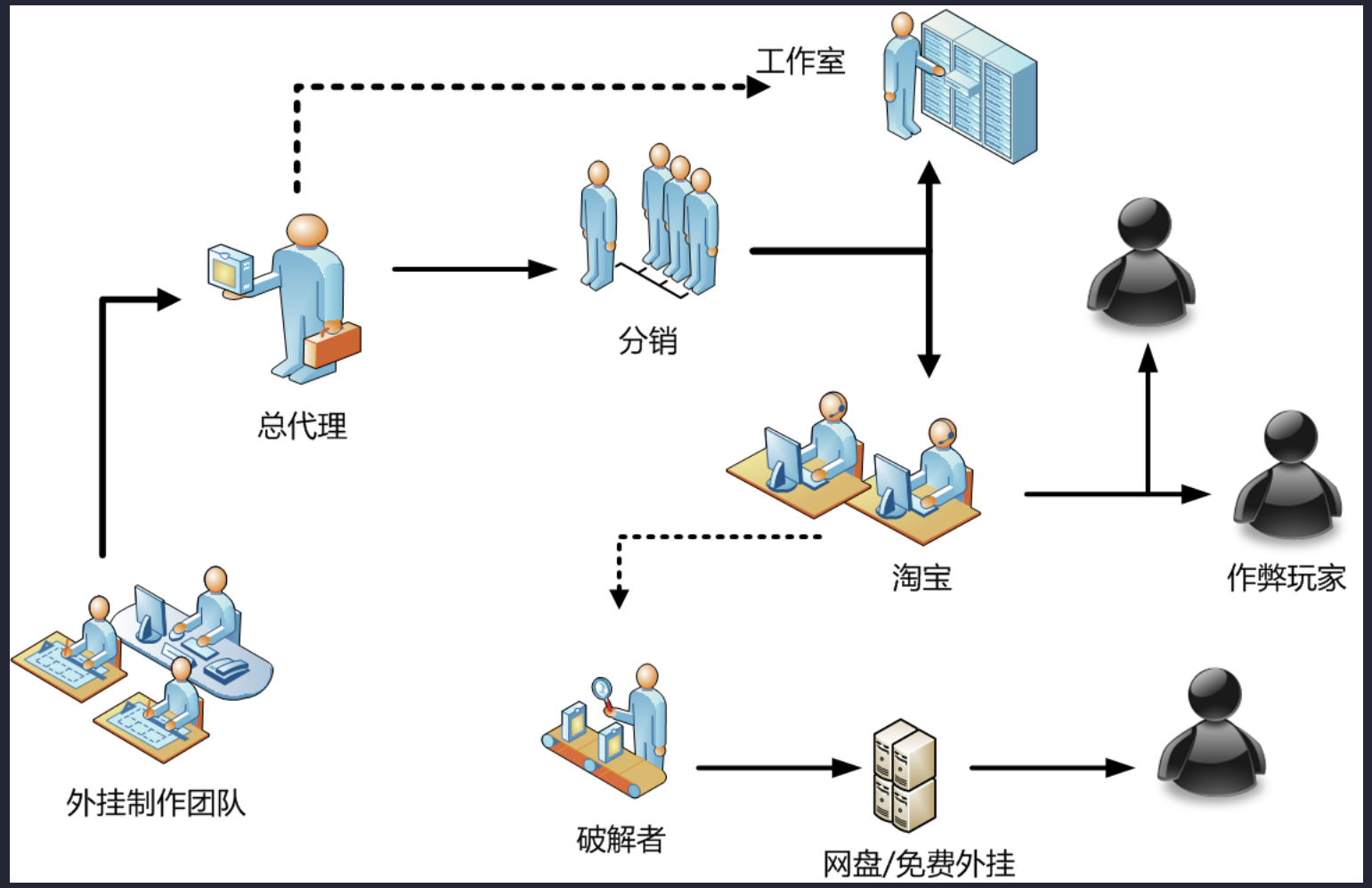
TenProtect Conficential, Copyright @Tencent, 2019

外挂的发展史

- 单机游戏， CheatEngine/FPE
- 网络游戏
  - 脱机挂 (WPE/WireShark)
  - 加速/倍攻 (数值异常)
  - 透视/自瞄 (Hook, 驱动)
  - 炸房/强登
- 打金工作室/代充/代练
- 手游模拟器

TenProtect Conficential, Copyright @Tencent, 2019

目前中国的外挂行业运作模式



TenProtect Conficential, Copyright @Tencent, 2019

中国网游作弊用户分布

- 越热门的游戏作弊越多
- 一些作弊软件卖的很贵
- 绝大作弊者都是新进玩家
- 60% 作弊发生在网吧
- 由于PUBG的影响，fps作弊现在非常流行

TenProtect Conficential, Copyright @Tencent, 2019

FPS游戏作弊的爆发

- **PUBG**
  - 在2108年，超过**2700**款外挂被监控到
  - 高峰期每天超过100款外挂进行更新
- **FPS**
  - 2018年大约有60款以上的FPS生存游戏
  - 所有的游戏都发现有外挂的存在
- **APEX**
  - 自02-05发布以来，72小时超过1000万玩家
  - 已经发现超过60外挂在售卖

TenProtect Conficential, Copyright @Tencent, 2019

月入宝马不是梦

TenProtect Conficential, Copyright @Tencent, 2019

2. 外挂技术原理的讨论

TenProtect Conficential, Copyright @Tencent, 2019

安全领域的大讨论

- 软件漏洞
  - 游戏bug，复制金币
  - 客户端逻辑没有服务器验证
  - 盗版问题
- 网络安全
  - 报文篡改
  - DDOS攻击
- 服务器、数据安全
  - 服务器入侵
  - SQL注入/回档

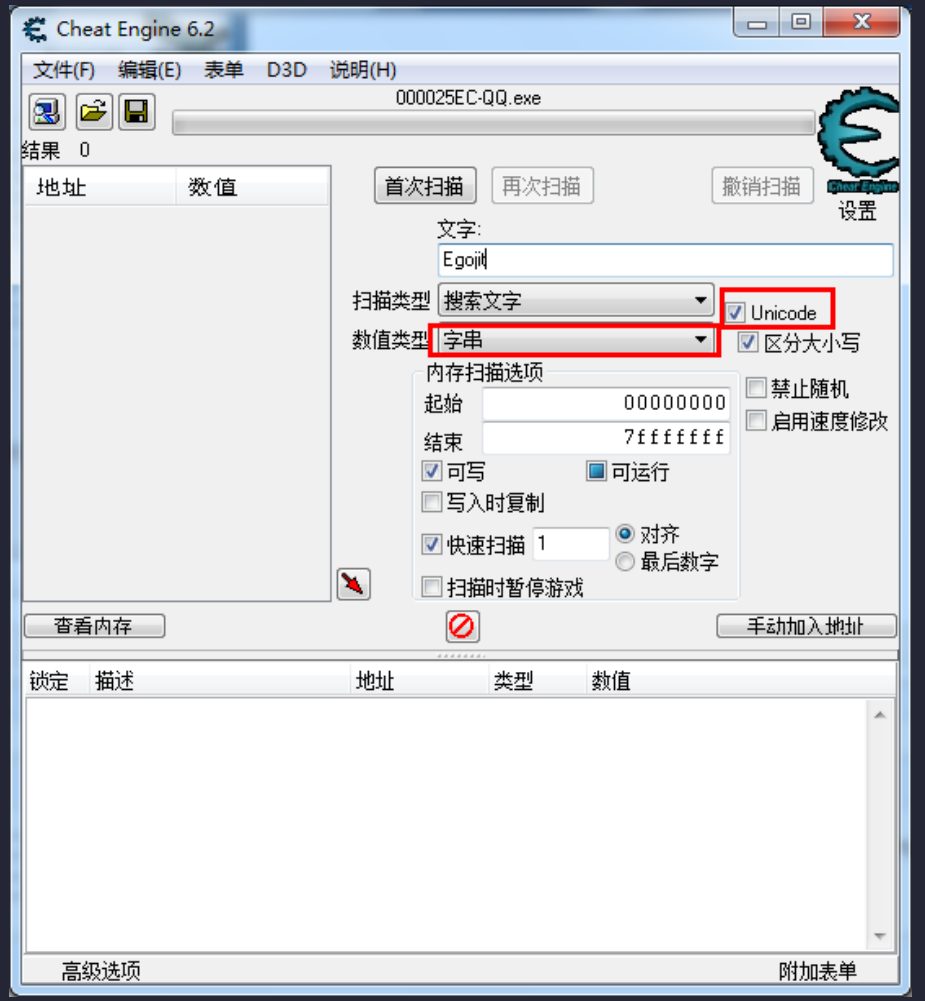
TenProtect Conficential, Copyright @Tencent, 2019

暗黑3漏洞 - 金币复制

TenProtect Conficential, Copyright @Tencent, 2019

内存修改型

- 游戏对象属性
  - 血量，攻击力，怪物等等
- 修改或调用游戏逻辑
  - 碰撞检测，自动瞄准
- 游戏资源文件
  - 手游/弱联网
  - 本地效果



TenProtect Conficential, Copyright @Tencent, 2019

LOL 改模型

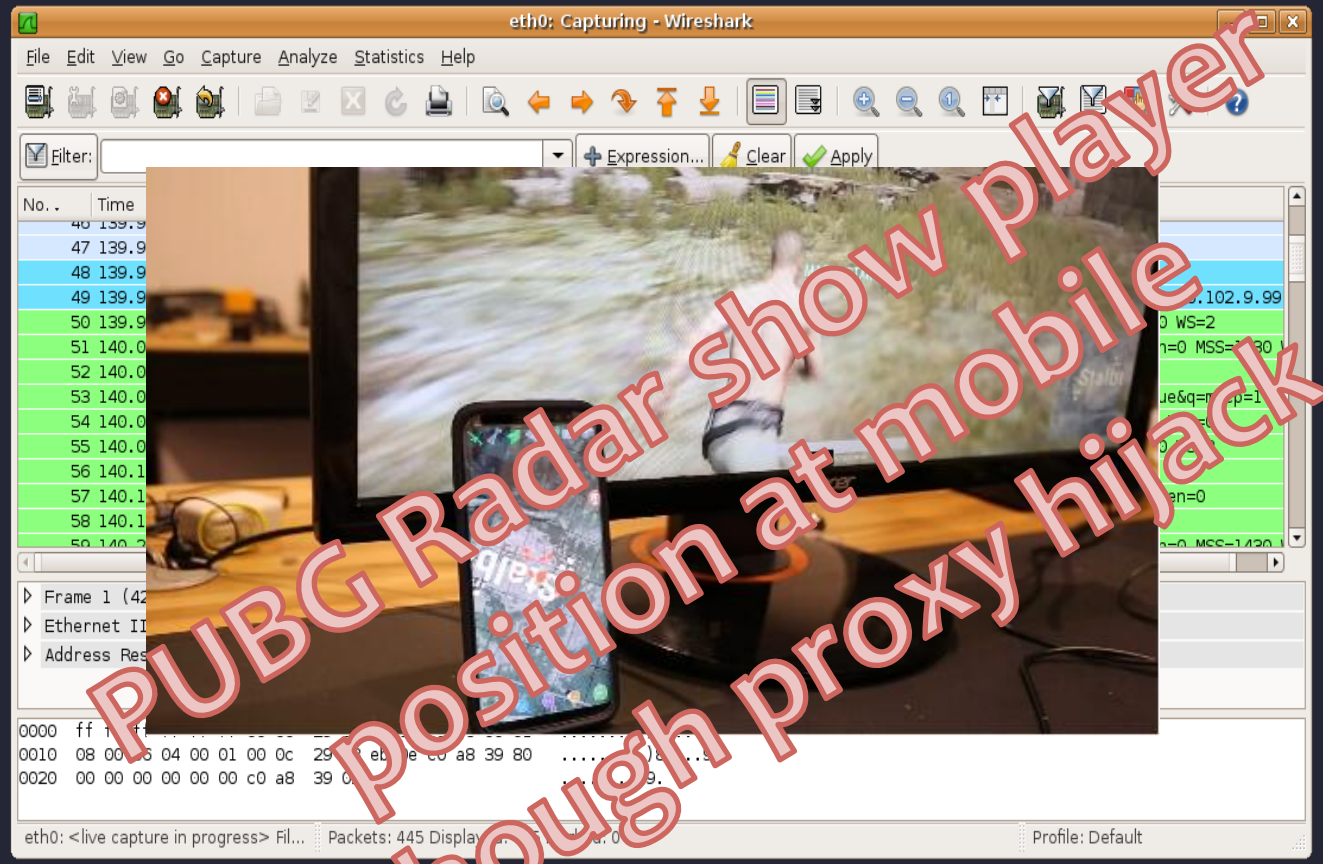
TenProtect Conficential, Copyright @Tencent, 2019

堡垒之夜/人物透视

TenProtect Conficential, Copyright @Tencent, 2019

脱机挂/协议模拟

- 端游
  - UnReal Engine(开源)
  - 外挂工作室
- 页游
  - Fiddle
- 手游
  - 离线



TenProtect Conficential, Copyright @Tencent, 2019

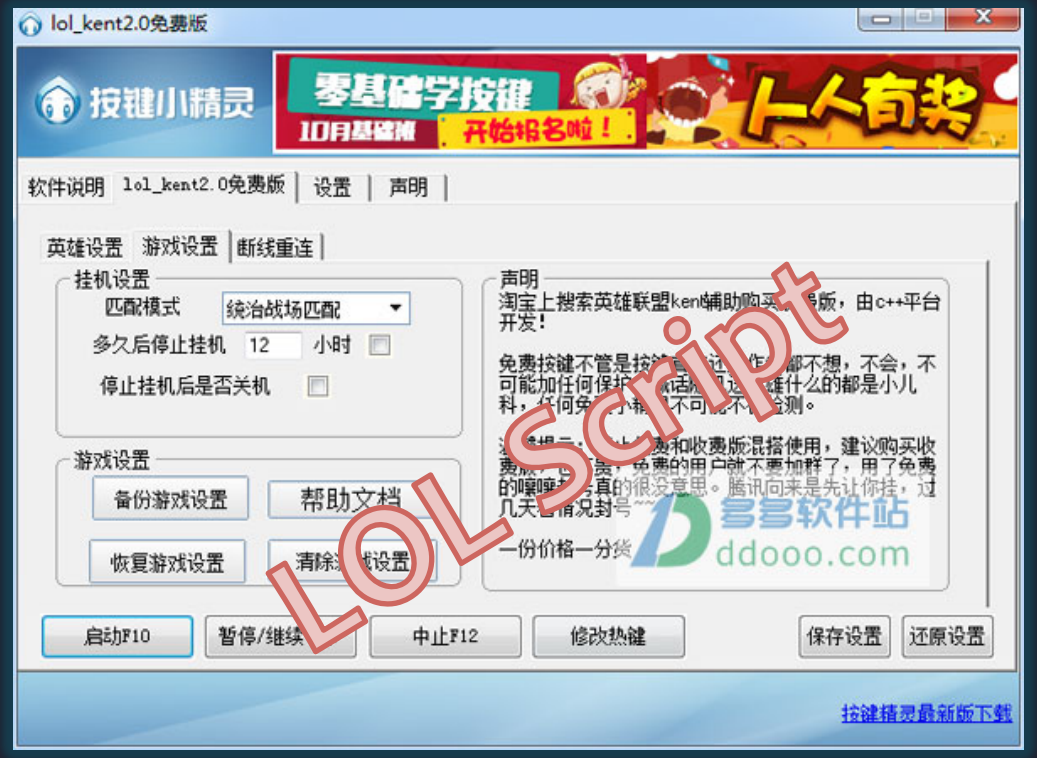
针对腾讯游戏的DDOS

- **LOL:**
  - 当对局要输时DDOS导致服务端崩溃
- **QQCart:**
  - 海量数据包导致安全包解析失败
- 灰色产业:
  - 中小厂商相互攻击

TenProtect Conficential, Copyright @Tencent, 2019

模拟按键

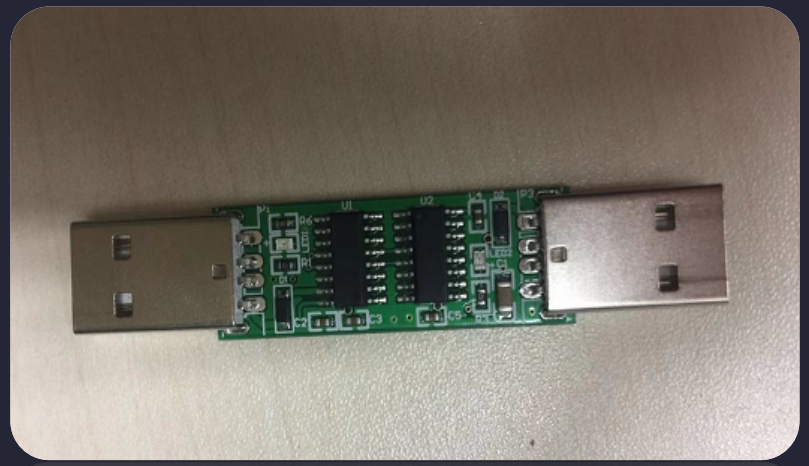
- 技术点
  - SendMessage/SendInput/KdbClass
  - 图像识别
  - 简单的状态机/深度学习AI
- 用途
  - 自动瞄准/自动开枪
  - 挂机脚本

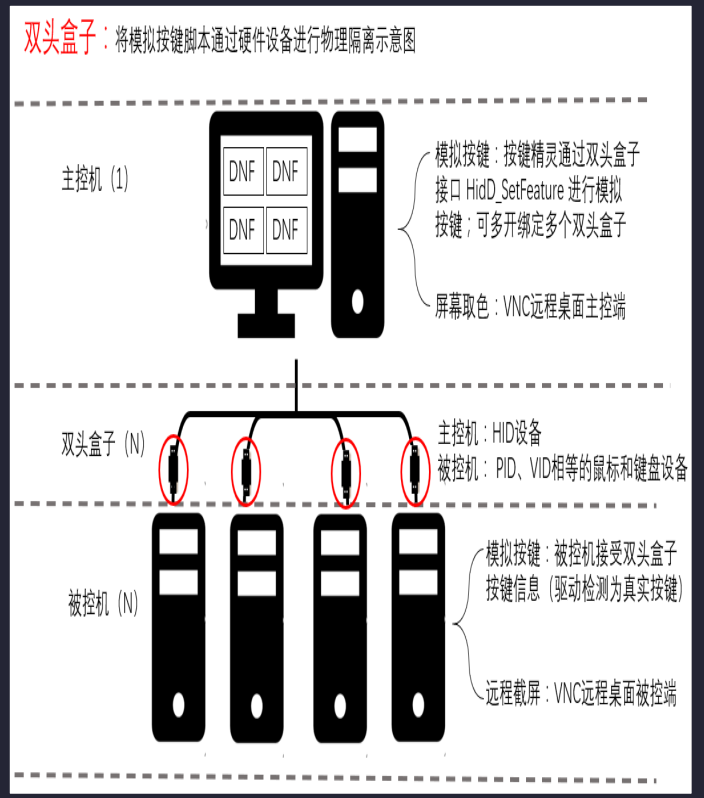


TenProtect Conficential, Copyright @Tencent, 2019

同步器硬件

dnf工作室





注: 可以在淘宝上买到

TenProtect Conficential, Copyright @Tencent, 2019

3. 游戏保护与安全对抗

TenProtect Conficential, Copyright @Tencent, 2019

游戏安全的特殊性

- 玩家
  - 要求打击
  - 侥幸心理/协助外挂
- 游戏开发运营
  - KPI考核，活跃和营收
- 工作室
  - 靠量取胜

TenProtect Conficential, Copyright @Tencent, 2019

外挂对抗之产品侧

- 举报
  - 视频举报
  - 恶意挂机
- 处罚手段
  - 封号/封禁机器
  - 踢人
  - 限制收益
  - 禁闭、禁言

TenProtect Conficential, Copyright @Tencent, 2019

外挂对抗之技术侧

- 通用检测
  - 基础保护
  - 样本
  - 举例: EAC(Easy Anti-Cheat), BattleEye (at PUBG)

- 行为检测
  - 收益
  - 伤害
  - 坐标

TenProtect Conficential, Copyright @Tencent, 2019

基础保护

- 反调试/加壳/代码混淆
  - VMP
- 完整性检测
- 驱动
  - 基于VT的保护（腾讯）

TenProtect Conficential, Copyright @Tencent, 2019

基于样本的保护

- 样本收集渠道
  - 量少
- 分析系统的容量
  - 依赖人工
- 样本自身的加密变形
  - 特征难于提取
- 外网特征运营的安全性
  - 风险不可控

TenProtect Conficential, Copyright @Tencent, 2019

基于行为的保护

- 游戏数据
  - 通关时间/人物属性
  - 坐标
- 数据挖掘
  - 修改点，样本
  - 历史战绩

TenProtect Conficential, Copyright @Tencent, 2019

LOL 工作室

- LOL坐标
- CNN
  - 160*160, ResNet
- LSTM 坐标序列

方案	训练	验证	测试
图片CNN	99.80%	99%	98%
灰度图CNN	97.80%	98%	97.60%
LSTM	96%	94%	94%

TenProtect Conficential, Copyright @Tencent, 2019

图像识别检测透视

TenProtect Conficential, Copyright @Tencent, 2019

gslab.qq.com

TenProtect Conficential, Copyright @Tencent, 2019