2012

第一届
全国网络与信息安全防护峰会

对话·交流·合作

CONVERSATION · COMMUNICATION · COOPERATION

基于行为的恶意软件自动化分析与检测

------火眼系统

姚辉
金山网络

目录

系统概要

系统概要

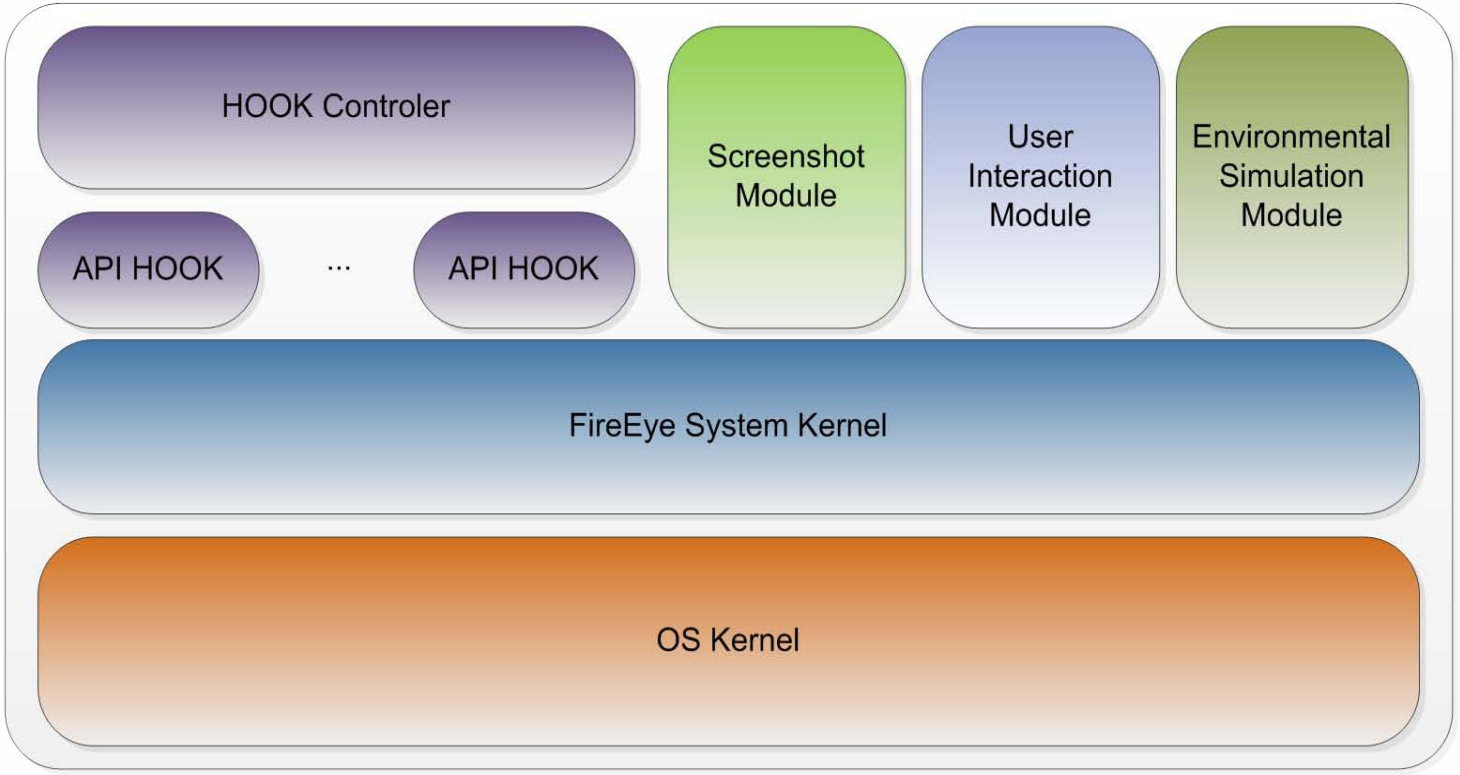
- 火眼系统是一套基于恶意软件行为的自动化分析与检测系统，由外围控制调度系统和虚拟机系统组成。
- 系统参数：
  - 单虚拟机日吞吐量1000，一台服务器可同时跑多个虚拟机
  - 火眼系统有24组服务器，日吞吐量20W
  - 支持文件类型包括：EXE、DLL、BAT、JS、VBS、HTML、APK等

框架与流程

火眼框架

- 框架特点：
  - 耦合低，各功能模块可分别单独开发调试
  - 分布式，易扩展，能简单的把空闲机器加入进来跑样本
  - 双层监控设计，系统本身具备发现监控异常情况
  - 更新和发布简单快速

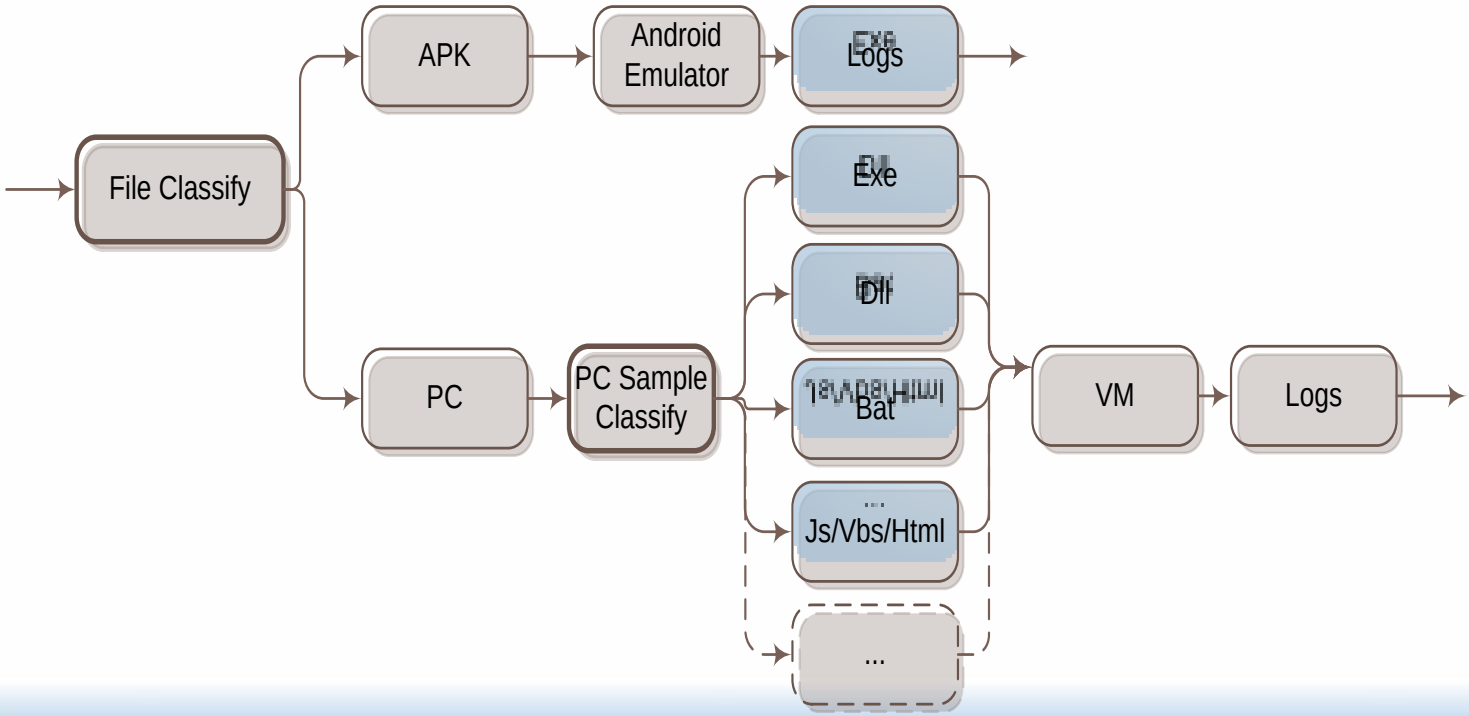
火眼框架


HOOK Controler
API HOOK
...
API HOOK
Screenshot Module
User Interaction Module
Environmental Simulation Module
FireEye System Kernel
OS Kernel

火眼流程

火眼流程

- 样本分流：
  - PC样本（EXE/DLL/BAT/JS/VBS/HTML）
  - Android样本（APK）



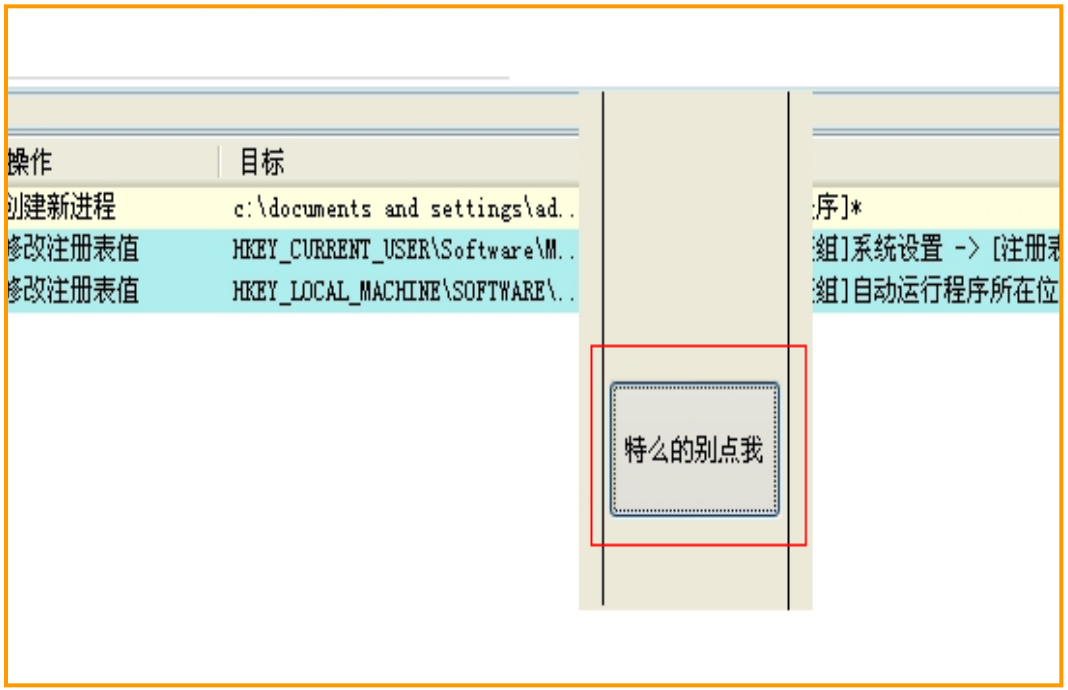
两个核心指标：
样本行为完整性和吞吐量

行为完整性-环境模拟

- 模拟内容包括：
  - 文件
  - 注册表
  - 窗口
  - 进程

行为完整性-模拟点击

- 按钮模拟点击
- 简单内容输入
- 难点：
  - 自绘按钮
  - 特定文字按钮
  - 特定输入



行为完整性-虚拟机对抗

- 硬件信息检测
  - 检测CPU型号、IDE型号等
  - 对策：
    - Patch，混淆（底层驱动），修改注册表等
- 执行环境检测 – 系统环境的探测
  - 系统CD-Key
  - 计算机名称
  - 特定的文件（文件夹）
  - 注册表键值
  - 对策：
    - 拦截/屏蔽
    - 混淆（返回假的结果）

吞吐量-虚拟机性能

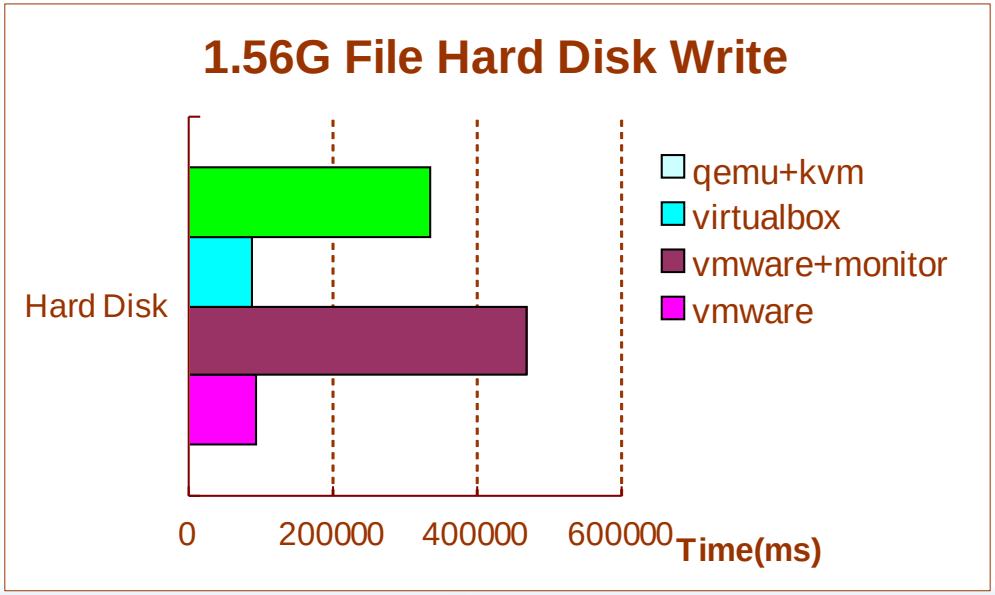
- 采用了以下四种配置来进行对比：
  - VMware
  - VMware + Monitor(我们自己开发的接管某些CPU指令的模块，解决指令级对抗）
  - VirtualBox
  - qemu+kvm
- 虚拟机cpu统一采用硬件虚拟化, 内存统一为512M

吞吐量-虚拟机性能

- 虚拟硬盘性能测试

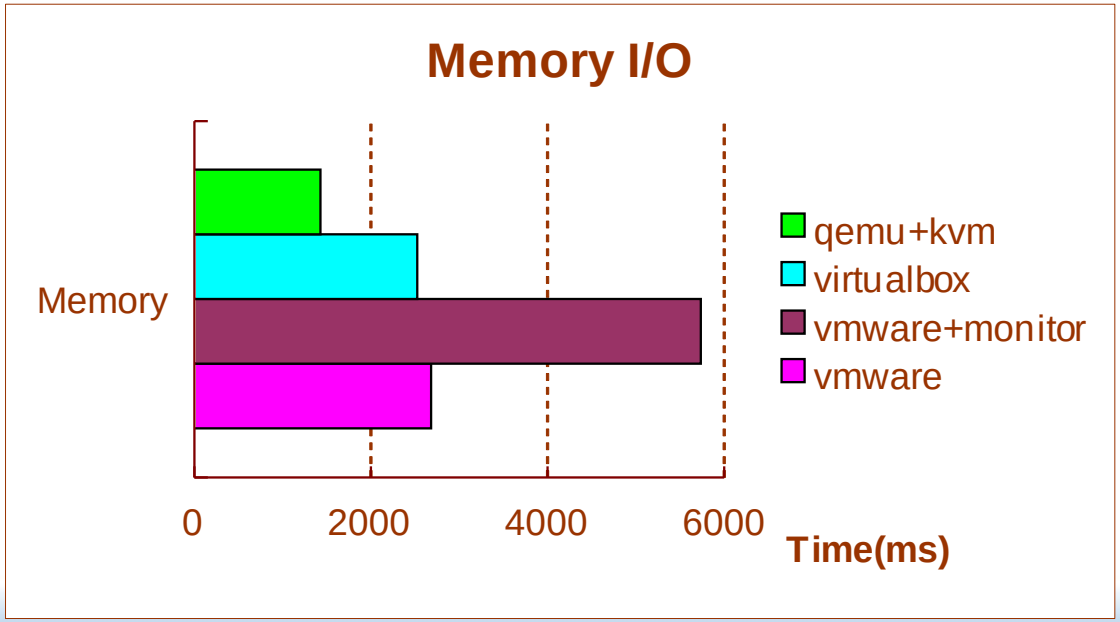
  方法：1.56G的文件写入

  结论：VirtualBox和VMWare性能更好



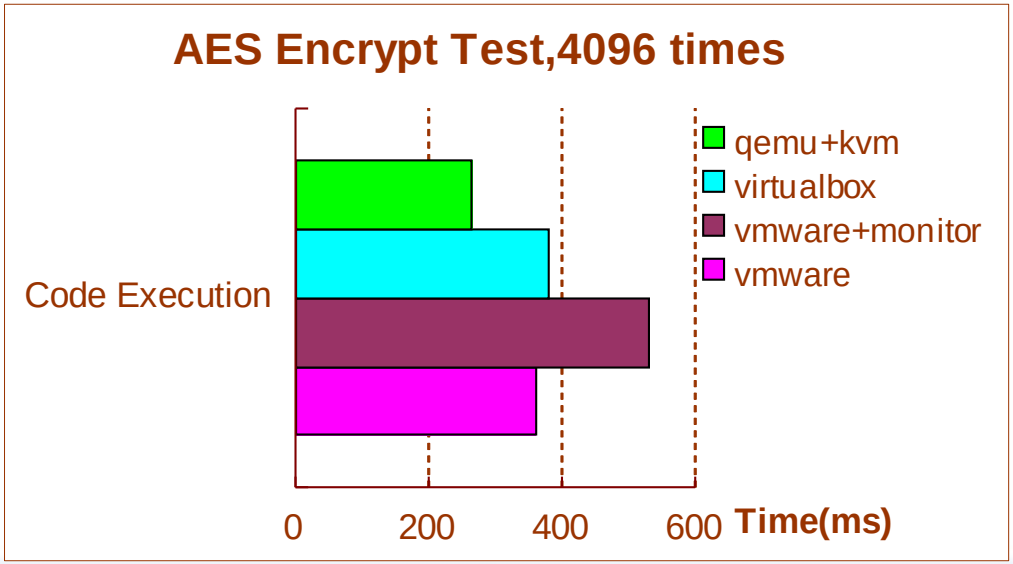
吞吐量-虚拟机性能

- 内存效率测试
  - 方法：AES加密100M数据所用的时间
  - 结论：Qemu+Kvm效率最高，VirtualBox和VMware次之



吞吐量-虚拟机性能

- 代码执行效率
  - 方法：AES循环加密测试，4096次循环加密1KB数据，
  - 结论：Qemu+Kvm最快，VMWare次之



吞吐量-虚拟机性能

- 火眼系统的选择：VMWare
- 这样选择的理由：
  - 稳定性最好；
  - 使用最广泛，技术上更成熟；
  - 通过内存盘的方式可以大大提升虚拟机性能

火眼应用

火眼应用

- 辅助分析
  - 专业病毒分析员或安全爱好者可以借助火眼在1-2分钟内了解一个未知样本的行为
- 自动鉴定
  - 丰富的火眼行为可以制定出非常精准的自动鉴定规则

火眼应用

- 解决杀毒软件的信任危机
  - 欺骗类病毒导致用户不信任杀毒软件报毒结果。
- 两个数据
  - 色播病毒，杀软提示病毒后有近50%的用户选择关闭杀软，运行病毒。
  - 外挂类病毒，杀软提示病毒后有近30%的用户选择关闭杀软，运行病毒。

我们的尝试


新毒霸
FIRE 火眼
腾讯QQ接收的文件是蠕虫病毒，已删除
下载文件： b99ca8aca159bcfc890b55cb0e68d97c
打开磁盘时自动运行
在磁盘根目录下添加AutoRun.inf文件，蠕虫病毒以此实现自动传播，扩大感染范围。双击盘符 D 会执行文件 re...
找回被删除的文件
我知道了

我们的尝试

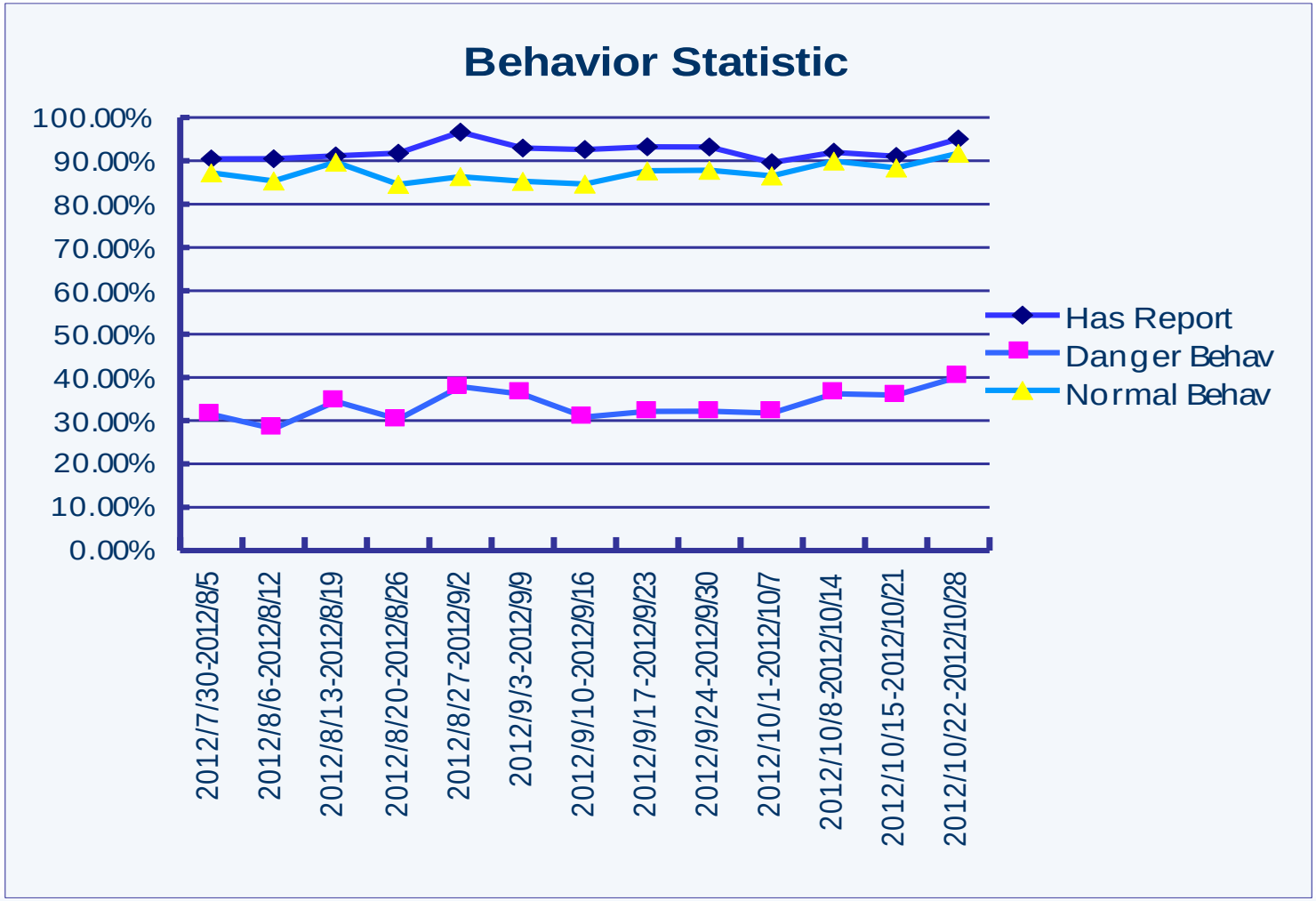

新毒霸
FIRE 火眼
谷歌浏览器下载的文件是蠕虫病毒，已删除
下载文件： b99ca8aca159bcfc89...5cb0e68d97c (1).zip
病毒名称： Heur.F_Eye.11
FIRE 火眼 经火眼分析，上述文件存在以下行为！
找回被删除的文件
我知道了

我们的尝试

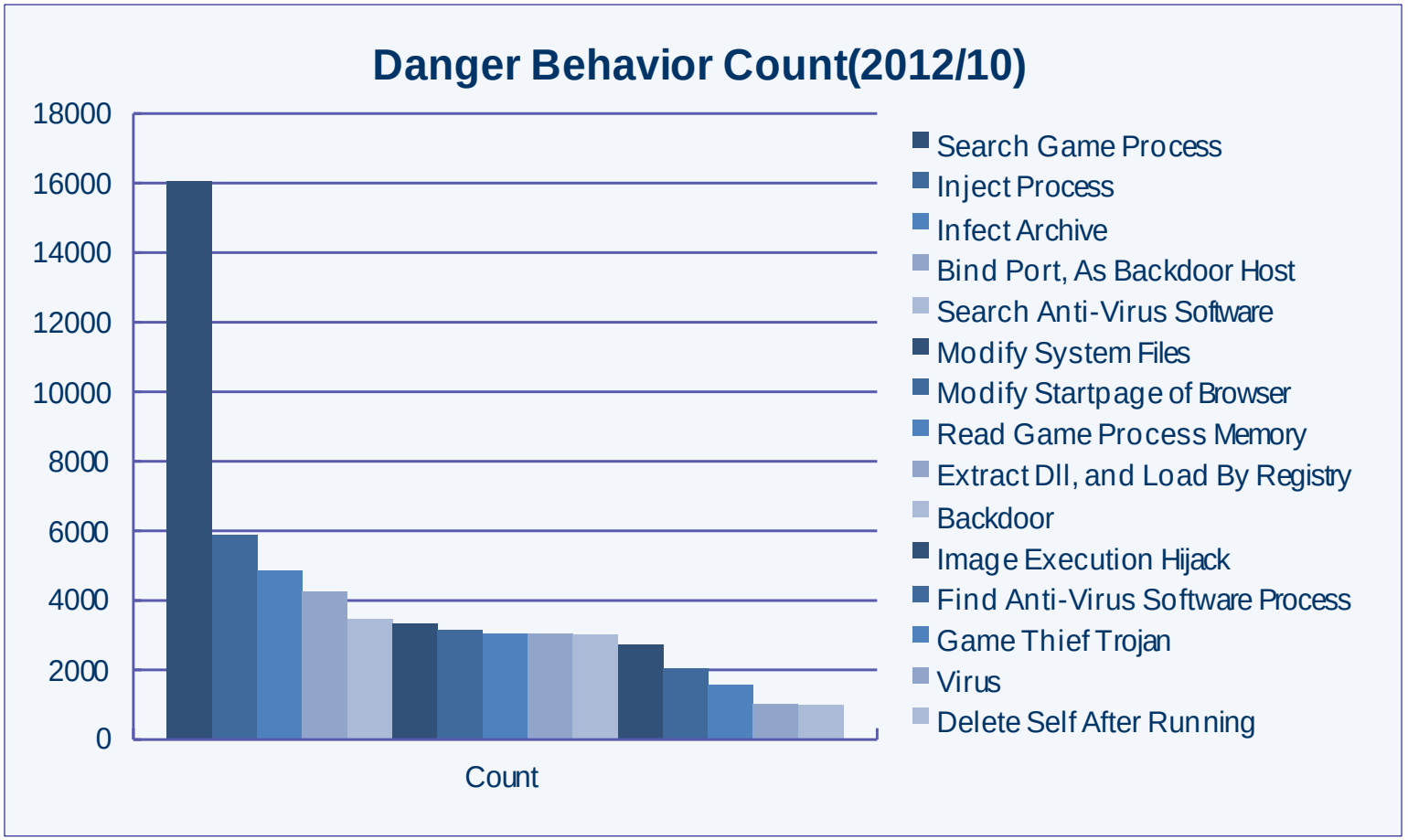

新毒霸
FIRE 火眼
腾讯QQ接收的文件是蠕虫病毒，已删除
下载文件： b99ca8aca159bcfc890b55cb0e68d97c
破坏系统安全模式
删除注册表中“安全模式”相关的项，使系统无法进入安全模式。
找回被删除的文件
我知道了

火眼数据分享

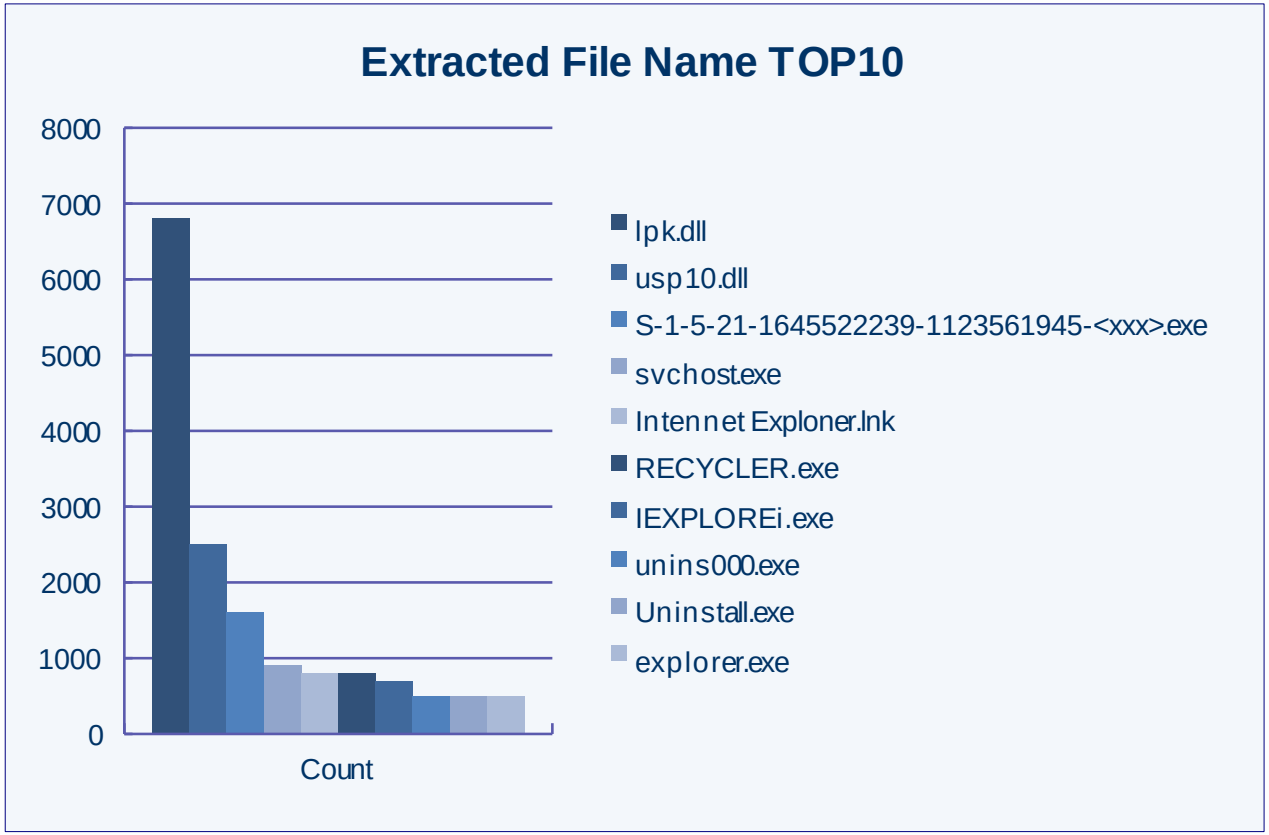
火眼数据分享


Behavior Statistic
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
2012/7/30-2012/8/5
2012/8/6-2012/8/12
2012/8/13-2012/8/19
2012/8/20-2012/8/26
2012/8/27-2012/9/2
2012/9/3-2012/9/9
2012/9/10-2012/9/16
2012/9/17-2012/9/23
2012/9/24-2012/9/30
2012/10/1-2012/10/7
2012/10/8-2012/10/14
2012/10/15-2012/10/21
2012/10/22-2012/10/28
Has Report
Danger Behav
Normal Behav

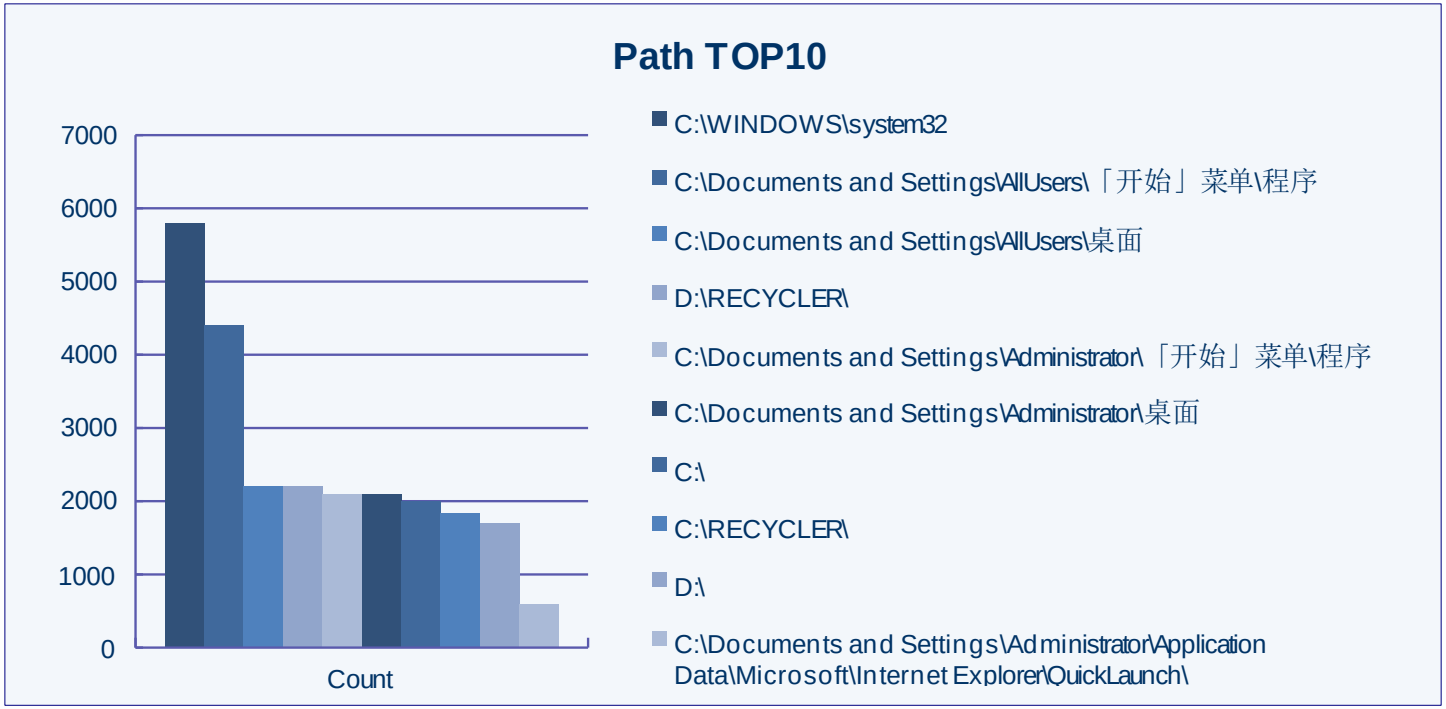
火眼数据分享


Danger Behavior Count(2012/10)
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
Count
Search Game Process
Inject Process
Infect Archive
Bind Port, As Backdoor Host
Search Anti-Virus Software
Modify System Files
Modify Startpage of Browser
Read Game Process Memory
Extract Dll, and Load By Registry
Backdoor
Image Execution Hijack
Find Anti-Virus Software Process
Game Thief Trojan
Virus
Delete Self After Running

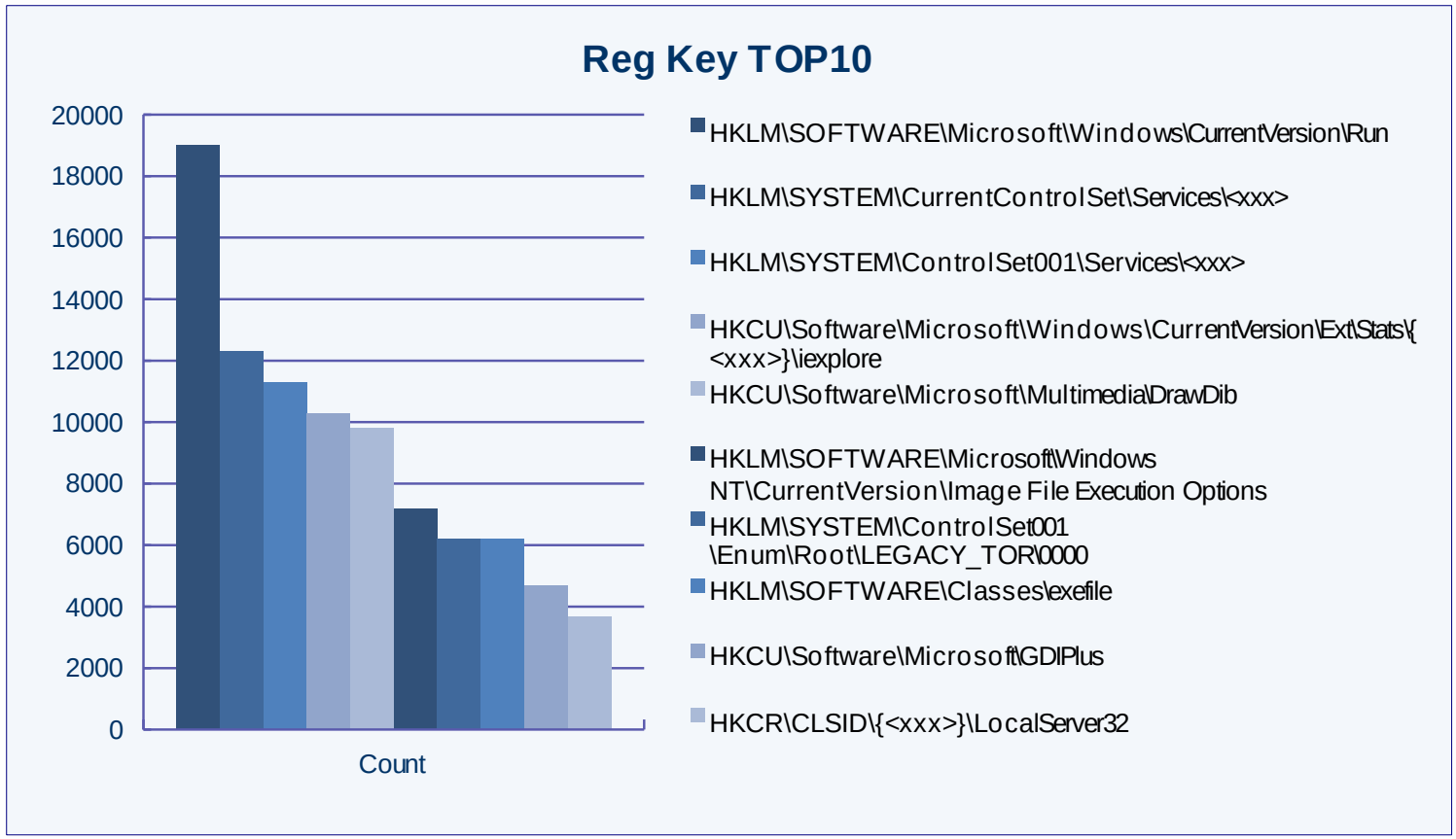
火眼数据分享


Extracted File Name TOP10
8000
7000
6000
5000
4000
3000
2000
1000
0
Count
lpk.dll
usp10.dll
S-1-5-21-1645522239-1123561945-<xxx>.exe
svchost.exe
Intennet Exploner.lnk
RECYCLER.exe
IEXPLOREi.exe
unins000.exe
Uninstall.exe
explorer.exe

火眼数据分享

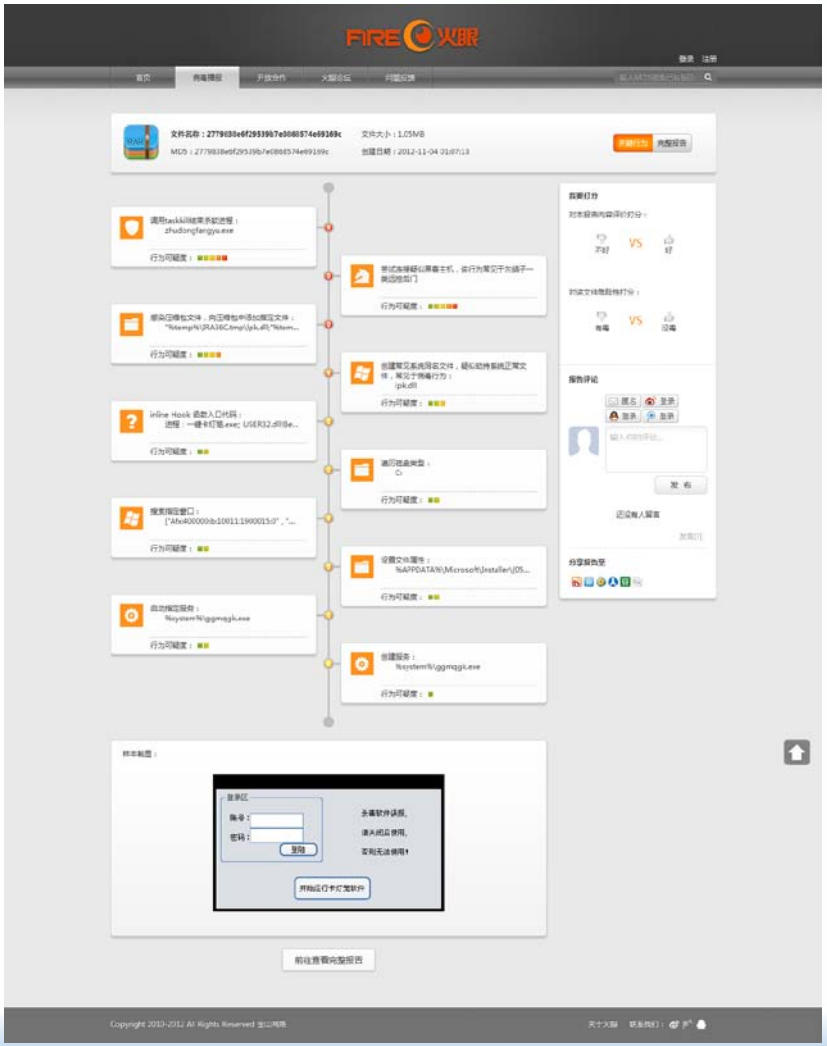

Path TOP10
7000
6000
5000
4000
3000
2000
1000
0
Count
C:\WINDOWS\system32
C:\Documents and Settings\AllUsers\「开始」菜单\程序
C:\Documents and Settings\AllUsers\桌面
D:\RECYCLER\
C:\Documents and Settings\Administrator\「开始」菜单\程序
C:\Documents and Settings\Administrator\桌面
C:\
C:\RECYCLER\
D:\
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\QuickLaunch\

火眼数据分享

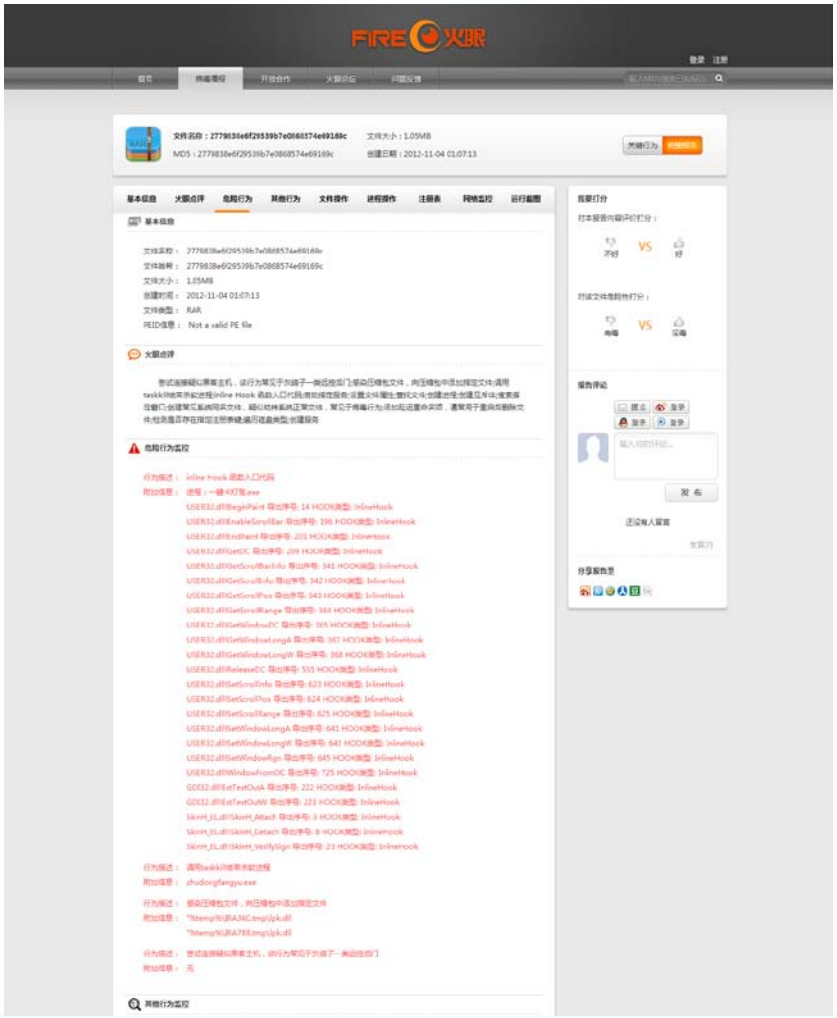

Reg Key TOP10
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
Count
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SYSTEM\CurrentControlSet\Services\<xxx>
HKLM\SYSTEM\ControlSet001\Services\<xxx>
HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{<xxx>}\iexplore
HKCU\Software\Microsoft\Multimedia\DrawDib
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TOR\0000
HKLM\SOFTWARE\Classes\exefile
HKCU\Software\Microsoft\GDIPlus
HKCR\CLSID\{<xxx>}\LocalServer32

火眼报告展示

火眼报告展示


FIRE 火眼
首页
病毒报告
开放合作
火眼论坛
问题反馈
登录 注册
文件名称：2779838e6f29539b7e0868574e69369c
MD5：2779838e6f29539b7e0868574e69369c
文件大小：1.05MB
创建日期：2012-11-04 21:07:13
关键行为
完整报告
调用task标签来创建进程：
zhudongfangyu.exe
行为可疑度：
行为可疑度：
行为可疑度：
行为可疑度：
行为可疑度：
行为可疑度：
行为可疑度：
我要打分
不好
VS
好
报告评论
发布
还没有人留言
分享报告至
样本截图：
登录区
账号：
密码：
登陆
杀毒软件误报，
退出后启用，
否则无法使用！
开始运行卡巴斯基软件
前往查看完整报告
Copyright 2010-2012 All Rights Reserved 安云网络
关于火眼
联系我们：

火眼报告展示


FIRE 火眼
基本信息
火眼点评
危险行为
其他行为
文件操作
进程操作
注册表
网络监控
运行截图
危险行为监控
其他行为监控

火眼报告展示


运行截图
夜雨挂号协议免费版
运行截图
打开一个YY
关闭全部YY
批量注册YY帐号
隐藏所有YY图标
显示所有YY图标
自定义YY路径
运行截图
12:43
贴吧更快更省流
尽享贴吧清爽体验！

火眼报告展示

- 一个典型的后门：
  - http://fireeye.ijinshan.com/analyse.html?md5=2779838e6f29539b7e0868574e69169c
  - http://fireeye.ijinshan.com/en/analyse.html?md5=2779838e6f29539b7e0868574e69169c（英文版）
- APK行为分析实例：
  - http://fireeye.ijinshan.com/analyse.html?md5=a58659ca069a10ecdfe577878718ce4c

合作

合作对象

对话·交流·合作

- 合作对象
  - 安全企业
  - 院校
  - 安全技术爱好者

合作方法

- 合作方法
  - 分析报告
  - 底层行为日志
  - SDK

- 谢谢！