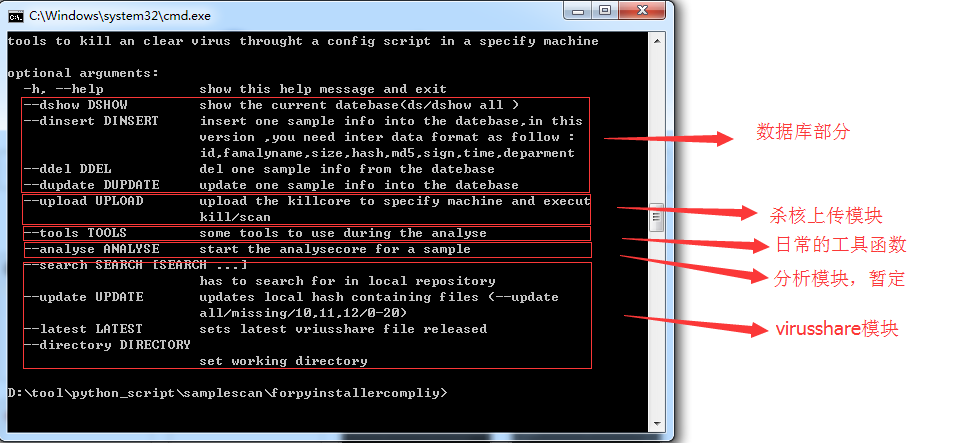
## 前言

前段时间说要写的一个专杀框架敌敌畏，后改为强撸敌敌畏，以彰显样本查杀时的气势，现在第一版已经完成了，如下图所示，使用的时候强烈建议控制台使用放大模式，这样就可以看见我花了半天才画好了logo 。



## 总的功能介绍

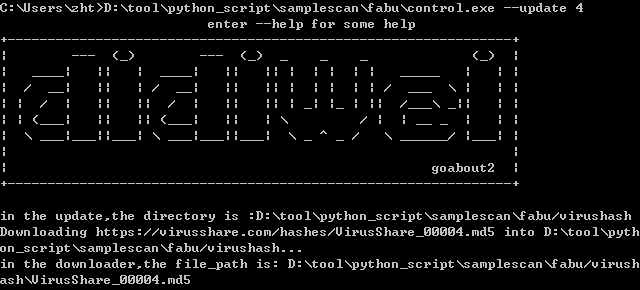


该框架目前基本分为四个部分

第一部分是一个数据库，该数据库中保存了我分析的样本的信息，主要是一个管理的用途，实现比较简单，就是通过sqlite3实现的一个轻量的数据库。



第二部分是virusshare，这个是github上的一个项目，我把它移植过来，其支持对virusshare上公开的样本的md5，hash数据库查询，以判断一个文件是否为恶意样本，这个模块使用前需要通过--update all命令下载md5，和hash文件。之后就可以通过—search命令实现查询。如下图所示



通过hash判断是否是恶意样本。

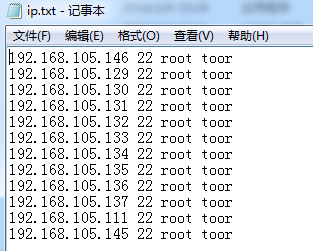


这两部分主要是为了一些后续的功能做铺垫（C:\Users\zht\AppData\Local\Temp\AV5W2LR]H5YAQXT}1N2LPDY.gif），这些数据在将来会很有用,后续还会将一些开源的特征数据加入进来，陆续工作会在第二版完成。

第三部分是tools模块，里面包含了一些我日常脚本分析会用到的python函数，目前没有提供参数控制台的参数调用，因为函数比较多，通过参数调用的话会分繁杂，后期会持续往里面写，某一块多了就可以整理成一个单独的功能模块。

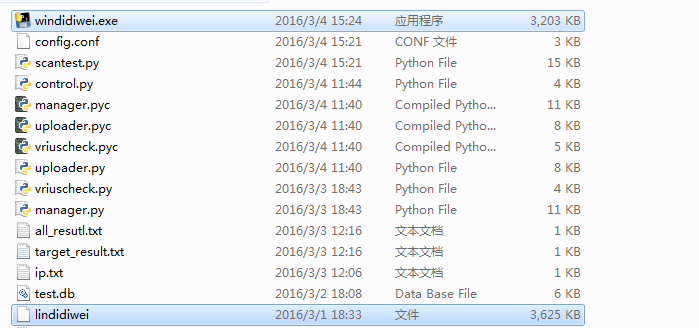
第四部分是上传模块，该模块通过提供的ip.txt配置文件，可批量上杀核文件，以实现对目标机器的的专杀，并记录查杀结果，由于通用性的原因此处使用的是ssh协议上传。

ip.txt文件需要按ip port username password的格式



## 杀核

在文件夹下的windidiwei.exe和lindidiwei分别对应window和linux下的样本查杀核心，实际上杀核是一份代码，通过pyinstaller实现的跨平台，以保证在没有python环境的机器下杀核依然可以运行，目前支持windows，和linux两个版本，mac也是支持的，但是杀核里还没实现，linux中基本覆盖大多数版本，当然前提是x86架构的，除此之外的各种稀奇古怪的cpu架构目前不予考虑。



杀核为了实现通用性，实际上是通过读取配置文件来实现对一个样本查杀，对应一个样本，将查杀的手段编写成一个相应的配置文件，杀核会自动根据配置文件去查杀。

配置文件描述如下：



### 通用选项

[linxu/windows]

标注该样本的运行环境。

[option]

该选项标注杀核需要进行的操作，支持scan/kill。

scan用于扫描目标机器中是否存在样本，选择scan时，下面需要提供filescan的选项，以及该样本的特征sign选项。

filescan 为需要扫描的目录，以分号；分割。

sigin为该样本的特征码，需要逆向提取。

kill用于对目标机器中的样本进行查杀，对于windows和linux中的样本此处的配置有较大的差别，杀核的运行逻辑是顺序执行配置文件，因此通过调换配置文件中选项的前后关系，在查杀中的逻辑也是不同的，如以下配置中，杀核先解析processes操作，再解析filedel操作，

processes = notepad.exe

filedel = D:\test\sample

通过配置文件顺序的调整，可以实现很多高难度的查杀工作。

### linux中kill支持的选项

sign，用于填写查杀样本的.

filepath，用于填写所有样本可能存在的目录，以分号；分割，杀核会根据提供的目录找出所有这些目录下的样本文件，及对应的进程（如果有）。

command 用于填写针对此次查杀中可能用到的一些额外命令，以分号；分割，以增加查杀的灵活性，但是很少用。

Filedel，用于填写针对此次查杀中所有通用的需要删除的文件，以分号；分割，此处结尾也要求以；结尾。

Initddscan，用于填写针对此次查杀中需要扫描的init启动文件，由于有些样本第一次运行之后并不会删除，用户激活时的目录是随机，因此无法通过二进制分析的手段获取到这种随机产生的目录，但是往往该目录下的这个样本都有对应的启动项（如果没有，其实是否删除该遗留下来的样本也不会有太大的问题），该选项就是通过遍历启动文件，查找此类有可能遗漏的样本，该选项也支持模糊查，一些特殊的样本生成的启动文件包含一些特征，只要在查找对象的名称的后面跟上特征\*\*d即可。

### Windows中kill支持的选项

filepath，同于linux。

fommand，同于linux。

filedel，同于linux，注意以分号；结尾。

sign，同于linux。

Register 用于填写针对此次查杀中需要删除的注册表键，用分号；分割，有些样本中注册表键名称为默认，即无名称，此时需要将键名用moren代替。

如以下注册表要删除HKEY\_CURRENT\_USER\Software\Microsoft\mspaint下的默认键，

可以这样写

register = HKEY\_CURRENT\_USER\Software\Microsoft\mspaint\moren



processes用于填写针对此次查杀中需要杀掉的进程名，用分号；分割，linux中没有该选项，因为杀核智能的进行了进程识别，但是在windows中这块的实现比较麻烦，考虑会在第二版实现，好在windows中的样本通常都是固定的名称，更有大部分都是通过注入的形式寄生在系统的特殊进程中，不会像linux那样一次出现大量的随机的进程。

devicelink用于填写针对此次查杀中需要卸载的驱动文件的文件描述符，一些样本由于驱动保护，但是往往驱动本身没有保护，通过该配置项和接下来的iocontrolcode，可以对样本的保护驱动进行卸载。

iocontrolcode用于填写针对此次查杀中需要卸载的驱动中的卸载函数。通过devicelink和iocontrolcode可以卸载掉一些较弱的驱动保护，如证券幽灵。当然这里的两个参数都需逆向获得，在对应驱动中没有导出驱动卸载函数时，该方式就没有用了。

目前第一版能根据配置文件完成日常的样本的查杀，当然不包括一些腻害的rootkit，说白了就是有驱动级别保护的没法处理。

### 实例

Linux平台下的

#### Xor家族

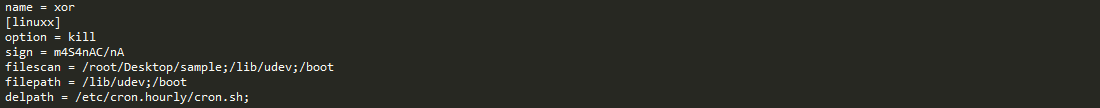
scan



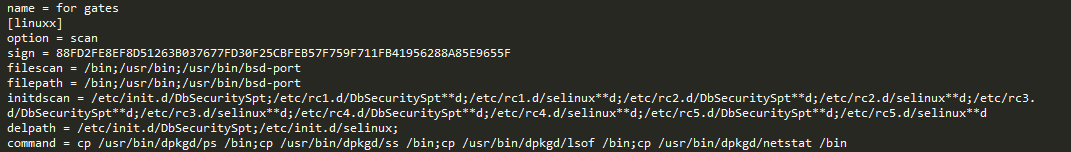


Kill





#### Gates家族



扫描



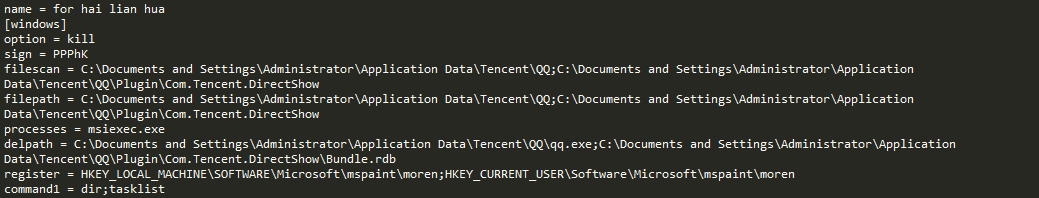


查杀

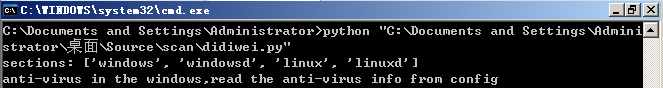


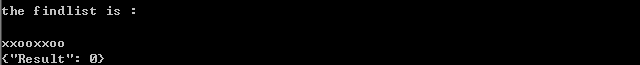
Window平台下的

#### 海莲花

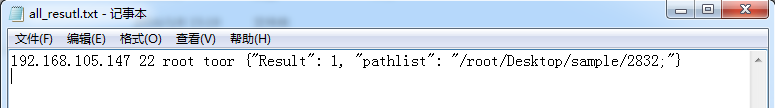


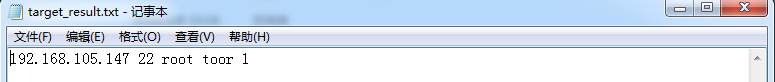
扫描并查杀





证券幽灵理论上也能够查杀，但是由于没有一个好的运行环境，所以就不放出来了。

扫描的结果会放在生成的文件all\_resutl.txe，和target\_result.txt中，其中all\_resutl.exe是所有主机的扫描信息，target\_result.txt是过滤之后感染的肉鸡。 



## 目前的一些问题。

1. 用的时候可能会有各种小问题，请及时联系我，非常感谢。
2. Windows中对远程上传的支持是在不是很友好，所以目前整个上传模块都是按ssh来写哒，windows中也是默认对方机器中有ssh才能上传，代码已经写好，但是由于我实在是找不到一台好用的有ssh的windows机器做测试，故你懂得。。。。。

## 未来的规划：

1. 先把第一版的各种小问题解决。
2. 既然是跨多平台，是不是考虑吧mac上的也实现？这个后期会考虑，但是由于mac上样本的分析经验不足，所以目前也没有很多很好的专杀思路。
3. Pyinstall能解决windows上所有的问题，但是linux上很多奇葩的型号可能会没法运行，考虑后期linux的杀核会用c重写。
4. 现有两个平台的杀核能力的提升，我们需要进军内核。
5. 以及其他更多更多amazing的功能。