一、概述

在系统被入侵后，要想了解下系统被入侵的过程，最好的途径大概就是通过查看日志，对日志进行分析，来还原整个过程的来龙去脉。每次对几百兆的日志进行查看时确实头疼，尤其是对关键字进行搜索时还会出现编辑器卡顿的情况。所以就想着能不能利用脚本去完成一些常规的排查过程，来辅助完成日志分析工作，先简单说下日志分析的思路，此处只是对于web日志进行分析。

二、功能简述

1. 根据关键字进行搜索
2. 目的：尝试通过在日志中搜索后门名称、时间等关键字，更快找到有用信息。
3. 使用方法：运行rizhi\_find.py,该模块最多支持两个关键字搜索，关键字之间以逗号隔开，

当最后一个关键字为1时，表示对关键字1和关键字2同时进行搜索；

当最后一个关键字为2时，表示搜索满足关键字1或关键字2的日志；

当最后一个关键字为空时，表示只是对关键字1进行搜索；

1. 结果保存：搜索出的结果均会保存在当前目录下的find\_result.txt文档中。

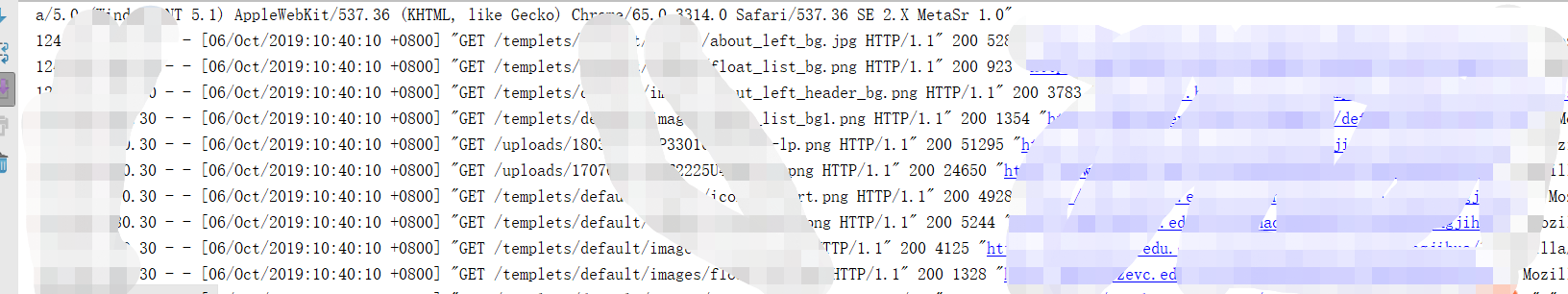
如搜索test.php，输入格式test.php,, 输出如下：



搜索10月6号访问test.php的日志，输入格式test.php, 06/Oct/,1 输出如下：

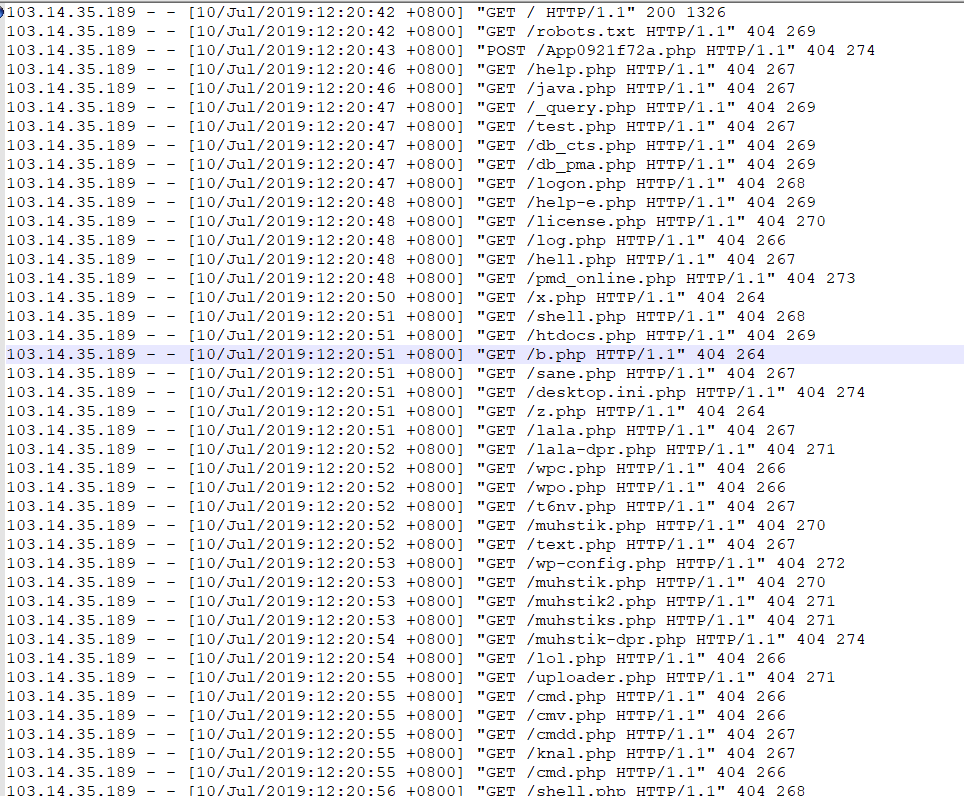


搜索10月6号或访问test.php的日志，输入格式test.php, 06/Oct/,2 输出如下：

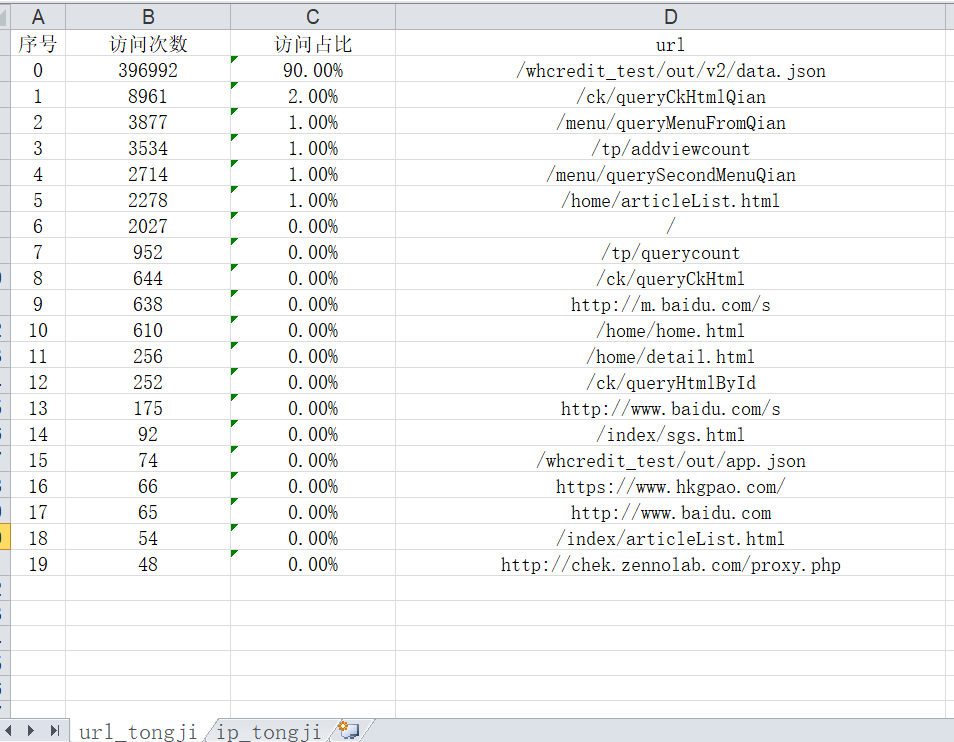


1. ip地址查询：

对搜索到结果进行ip地址提取，查看攻击者的ip还做过哪些操作，并将搜索结果保存在log.txt中



1. Ip、url分析
2. 目的：提取日志中所有的ip地址，并对ip归属地进行查询，并对出现次数做统计；根据日志分析url访问情况，记录访问路径、访问次数，并将结果保存到tongji.xsl表格中。
3. 使用方法：将需要查询的日志放到当前路径/log/目录下，运行python rizhifenxi.py。
4. 结果保存：会在result目录下生成tongji.xls。



url统计表



Ip地址统计表

三、有待改进

1、很多时候即使是筛选出来后还是更多的靠人为去分析，脚本只是辅助工具，所以存在不够通用的问题；

2、ip地址在查询中由于查询接口原因，会存在查询失败情况；

3、当日志格式为自定义情况下，需要根据定义格式在自行修改脚本中分割日志的格式；

四、最后

现成的日志分析工具，网上大牛已经分享了很多，现有的如elk、web-log-parser、360星图等，也有大牛们自己编写的一些工具。这里只是根据自己的需求重点做了搜索、异常地址访问列表提取、ip地址归属地查询、url汇总功能，还是有很多功能可以添加完善的，可根据自己的需求做修改完善处理，有好的意见也可以多多指出。