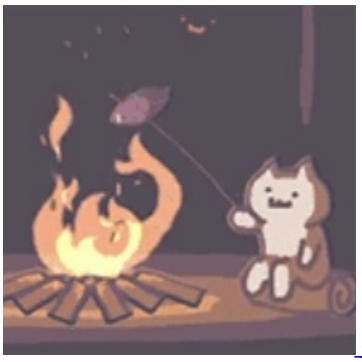
[BUUCTF]大流量分析 writeup

原创

shu天 于 2021-09-05 00:08:30 发布 205 收藏

分类专栏： ctf 文章标签： tcp/ip http windows ctf misc



重要的话写前面，不要靠近这个题，会变得不幸

没什么逻辑，感觉是大流量 恶心人的…也可能是我没看懂哦

[BUUCTF]大流量分析

> 某黑客对A公司发动了攻击，以下是一段时间内我们获取到的流量包
> 1.黑客的攻击ip是多少？
> 2.黑客使用了哪个邮箱给员工发送了钓鱼邮件?
> 3.那黑客预留的后门的文件名是什么？

统计出现频率比较高的IP，这里不知道D和H的区别所以两个都看看

172.16.61.200

183.129.152.140 黑客IP

172.16.103.1

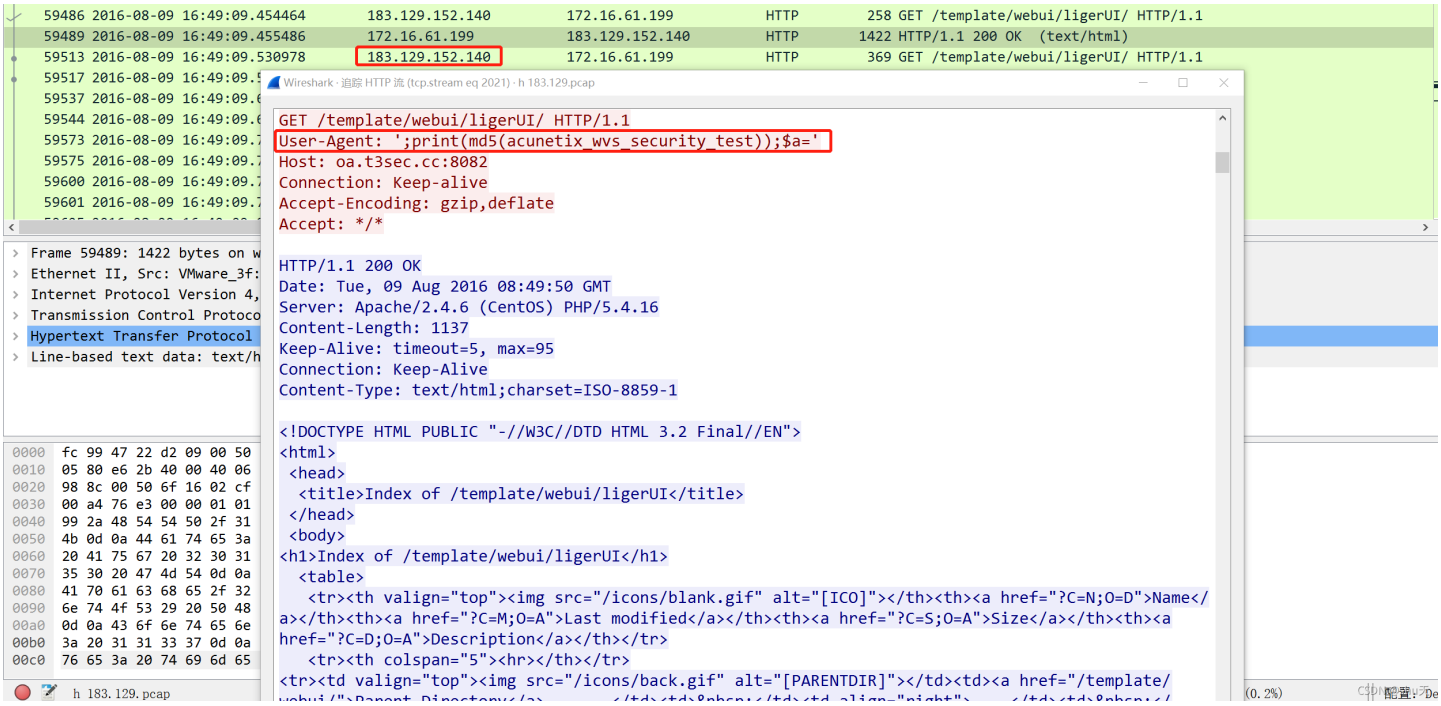
172.16.61.199

1.攻击IP

分别过滤几个IP：`http && ip.addr == 183.129.152.140`

在H流量包中可以看到183.129.152.140对172.16.61.199发起**目录穿透**恶意请求，并且在header添加恶意代码

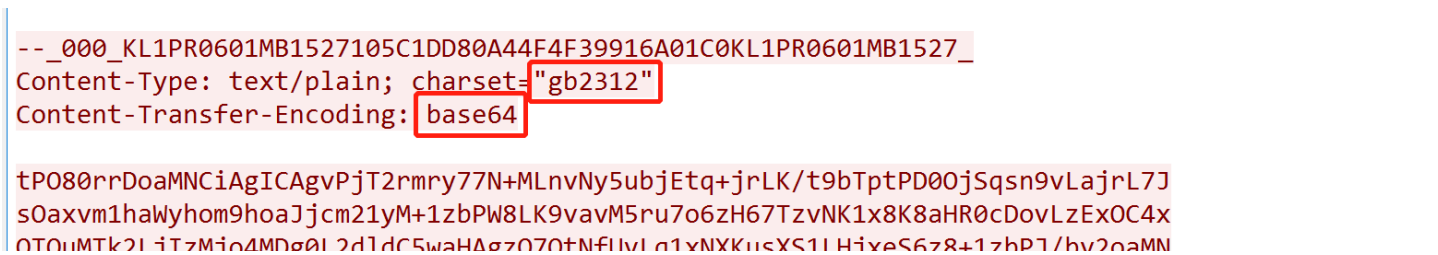
黑客IP183.129.152.140



2.邮箱钓鱼

在第一个流量包中查找SMTP协议，追踪TCP流，可以确定发送邮箱是`MAIL FROM:<xsser@live.cn>`

最后面有邮件内容



```
CiAgICDQu9C7tPO80qOhDQoNCg==

--_000_KL1PR0601MB1527105C1DD80A44F4F39916A01C0KL1PR0601MB1527_
Content-Type: text/html; charset="gb2312"
Content-Transfer-Encoding: quoted-printable

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dgb2312">
<style type=3D"text/css" style=3D"display:none;"><!-- P {margin-top:0;margi=
n-bottom:0;} --></style>
</head>
<body dir=3D"ltr">
<div id=3D"divtagdefaultwrapper" style=3D"font-size:12pt;color:#000000;back=
ground-color[14 bytes missing in capture file].family:Calibri,Arial,Helvetica,sans-serif;">
<p><span id=3D"ms-rterangepaste-start"></span></p>
<div>=B4=F3=BC=D2=BA=C3=A1=A3<br>
     =BC=F8=D3=DA=B9=AB=CB=BE=CD=F8=C2=E7=BC=DC=B9=B9=
=B8=C4=B6=AF=A3=AC=B2=BF=B7=D6=D3=A6=D3=C3=D0=E8=D2=AA=C9=FD=BC=B6=A3=AC=BE=
=C9=B0=E6=B1=BEmail=A1=A2oa=A1=A2crm=B5=C8=CF=B5=CD=B3=D6=F0=B2=BD=BD=AB=CC=
=E6=BB=BB=A3=AC=C7=EB=B4=F3=BC=D2=B5=C7=C2=BChttp://118.194.196.232:8084/ge=
t.php =CC=EE=D0=B4=D7=D4=BC=BA=B5=C4=D5=CA=BA=C5=D2=D4=B1=E3=C5=E4=BA=CF=CF=
```


tPO80rrDoaMNCiAgICAgvPjT2rmry77N+MLnvNy5ubjEtq+jrLK/t9bTptPD0OjSqsn9vLajrL7J
sOaxvm1haWyhom9hoaJjcm21yM+1zbPW8LK9vavM5ru7o6zH67TzvNK1x8K8aHR0cDovLzExOC4x
OTQuMTk2LjIzMjo4MDg0L2dldC5waHAgzO7QtNfUvLq1xNXKusXS1LHjxeS6z8+1zbPJ/by2oaMN
CiAgICDQu9C7tPO80qOhDQoNCg==

编码源格式：◉文本 ○Hex 解码结果： 自动检测 中文编码： GB2312 编码 解码

大家好。
鉴于公司网络架构改动，部分应用需要升级，旧版本mail、oa、crm等系统逐步将替换，请大家登录http://118.194.196.232:8084/get.php
填写自己的帐号以便配合系统升级。
谢谢大家！

base64和quoted-printable解码一样的内容，注意是gb2312编码

Wireshark · 追踪 HTTP 流 (tcp.stream eq 7351) · ht.pcap

```
GET /admin.bak.php?a=assert&b=phpinfo() HTTP/1.1
Host: oa.t3sec.cc:8082
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: my_expand_3=2%2C1%2C; PHPSESSID=lq5vn8k9fe72pnsffjv35ljj71;
po_auth=MQkwOWZiY2U0NjU1NDEwYmMwM2JhZmExZDExZjc2ODQ3NQ%3D%3D;
loginpass=ec38fe2a8497e0a8d6d349b3533038cb
Connection: keep-alive

NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0" src="/admin.bak.php?=PHPE9568F34-D428-11d2-
A769-00AA001ACF42" alt="PHP Logo" /></a><h1 class="p">PHP Version 5.4.16</h1>
</td></tr>
</table><br />
```

```
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Linux localhost.localdomain 3.10.0-123.el7.x86_64 #1
SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 </td></tr>
<tr><td class="e">Build Date </td><td class="v">May 12 2016 13:46:18 </td></tr>
<tr><td class="e">Server API </td><td class="v">Apache 2.0 Handler </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc </td></tr>
<tr><td class="e">Loaded Configuration File </td><td class="v">/etc/php.ini </td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">/etc/php.d </td></tr>
<tr><td class="e">Additional .ini files parsed </td><td class="v">/etc/php.d/curl.ini,
/etc/php.d/fileinfo.ini,
```

分组 34858。2 客户端 分组，36 服务器 分组，2 turn(s).点击选择。 CSDN @shu天

3.黑客后门

我猜最后一个流量包会有shell，可以进一步过滤 `http.request && ip.addr == 183.129.152.140`

受不了了，这个黑客上传了好多疑似shell的东西（/data/uploadfile），看了别人的wp发现是**搜phpinfo()**，居然会有人用get传命令哦

Wireshark · 追踪 HTTP 流 (tcp.stream eq 7351) · ht.pcap

```
GET /admin.bak.php?a=assert&b=phpinfo() HTTP/1.1
Host: oa.t3sec.cc:8082
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: my_expand_3=2%2C1%2C; PHPSESSID=lq5vn8k9fe72pnsffjv35ljj71;
po_auth=MQkwOWZiY2U0NjU1NDEwYmMwM2JhZmExZDExZjc2ODQ3NQ%3D%3D;
loginpass=ec38fe2a8497e0a8d6d349b3533038cb
Connection: keep-alive

NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0" src="/admin.bak.php?=PHPE9568F34-D428-11d2-
A769-00AA001ACF42" alt="PHP Logo" /></a><h1 class="p">PHP Version 5.4.16</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Linux localhost.localdomain 3.10.0-123.el7.x86_64 #1
SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 </td></tr>
<tr><td class="e">Build Date </td><td class="v">May 12 2016 13:46:18 </td></tr>
<tr><td class="e">Server API </td><td class="v">Apache 2.0 Handler </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc </td></tr>
<tr><td class="e">Loaded Configuration File </td><td class="v">/etc/php.ini </td></tr>
<tr><td class="e">Scan this dir for additional .ini files </td><td class="v">/etc/php.d </td></tr>
<tr><td class="e">Additional .ini files parsed </td><td class="v">/etc/php.d/curl.ini,
/etc/php.d/fileinfo.ini,
```

分组 34858。2 客户端 分组，36 服务器 分组，2 turn(s).点击选择。 CSDN @shu天

后门文件 `admin.bak.php`