Who is Mr Wu?

intrusiontruth.wordpress.com/2017/05/02/who-is-mr-wu

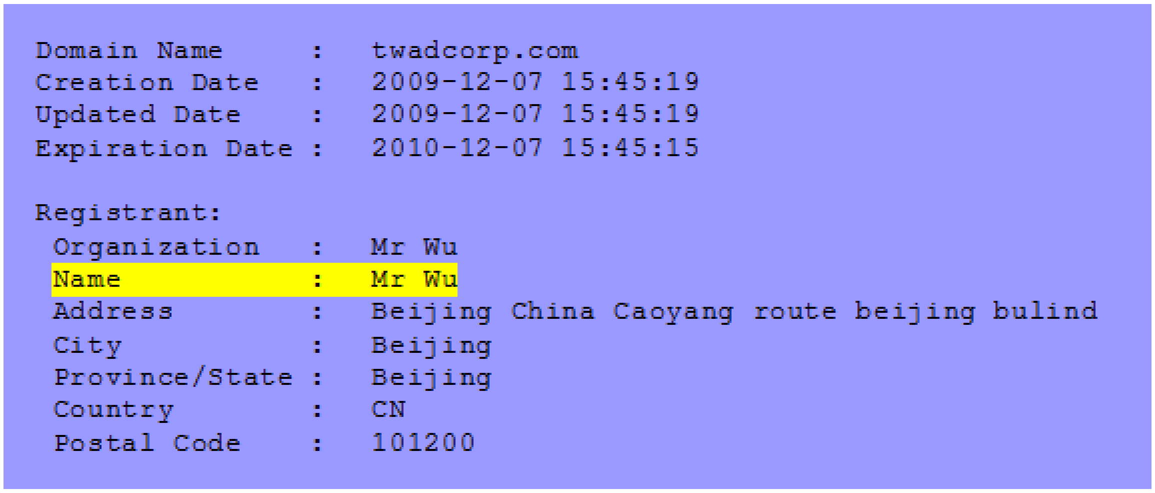
intrusiontruth

May 2, 2017

In our last post we introduced you to APT3 and promised to identify the individuals behind the intrusion. Today we will follow the trail left by APT3's infrastructure procurers and will identify our first APT3 operator, Mr Wu.

Mr Wu

The trail starts in 2010, when FireEye researchers analysing the Pirpi backdoor used by APT3 identified a sample that communicated with the domain twadcorp[.]com. WHOIS information from late 2009 for this domain gives a registrant name: "Mr Wu".



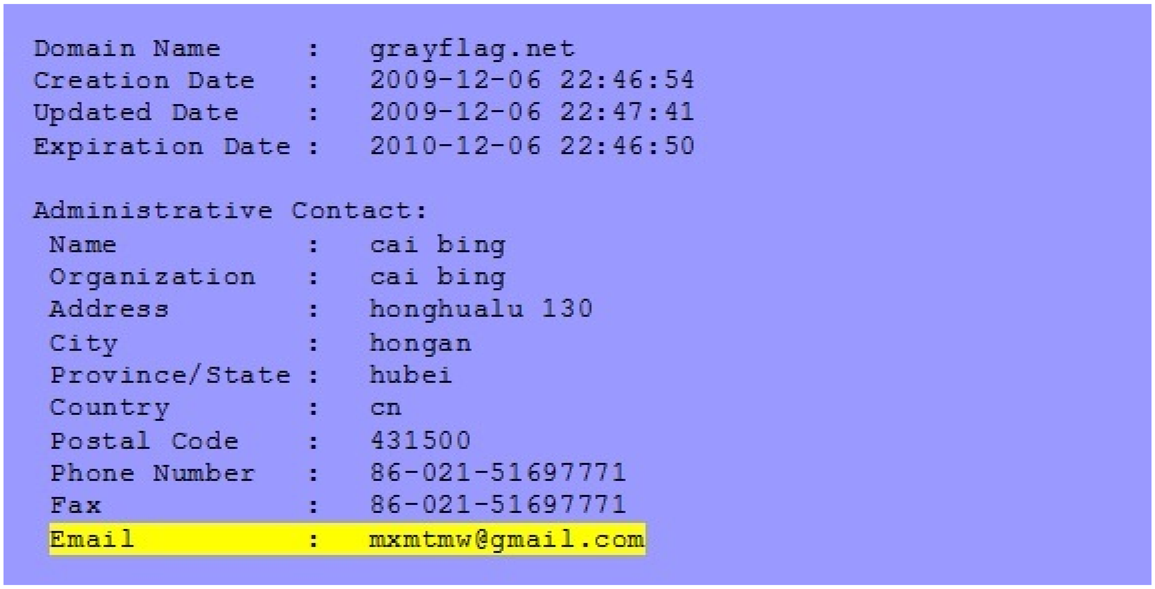
```
Domain Name     :   twadcorp.com
Creation Date   :   2009-12-07 15:45:19
Updated Date    :   2009-12-07 15:45:19
Expiration Date :   2010-12-07 15:45:15

Registrant:
 Organization   :   Mr Wu
 Name           :   Mr Wu
 Address        :   Beijing China Caoyang route beijing bulind
 City           :   Beijing
 Province/State :   Beijing
 Country        :   CN
 Postal Code    :   101200
```

Historic WHOIS data showing "Mr Wu" as registrant of twadcorp[.]com

Mr Wu is not a particularly unique name – in fact "Wu" is the 9th most common surname in China. But if we follow the trail ever further back in time we can also identify Mr Wu's given name.

From APT3 to mxmtmw

To continue the investigation, we need to examine a second Pirpi sample, this time one that communicates with the domain grayflag[.]net. WHOIS information for the domain from 2009 gives the email address mxmtmw[at]gmail.com.



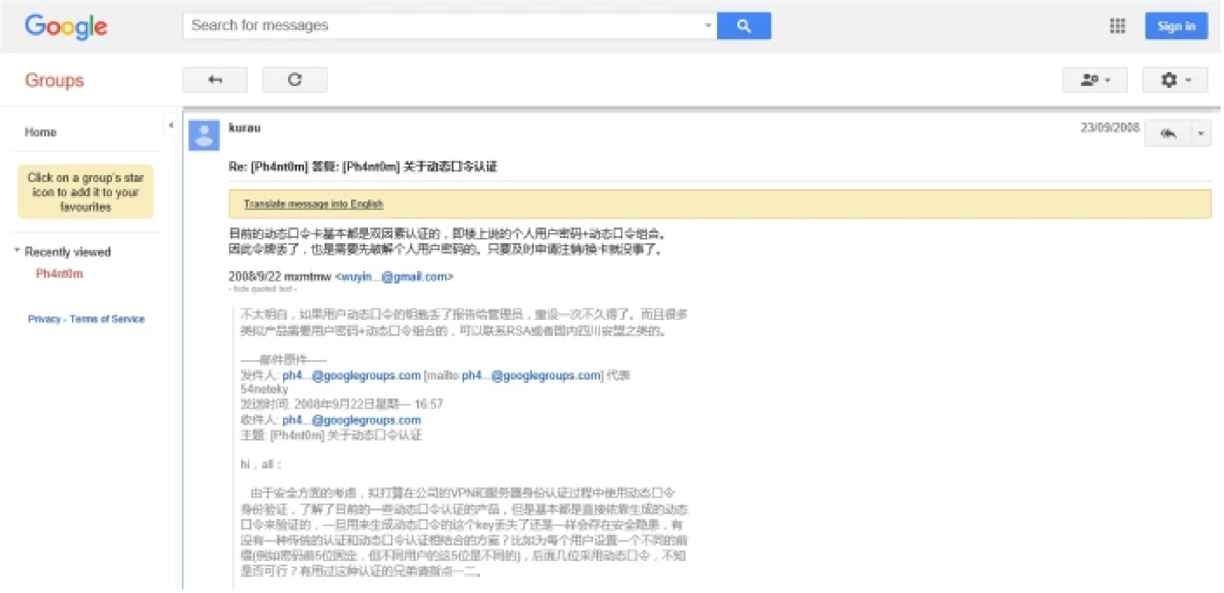
```
Domain Name      :   grayflag.net
Creation Date    :   2009-12-06 22:46:54
Updated Date     :   2009-12-06 22:47:41
Expiration Date :   2010-12-06 22:46:50

Administrative Contact:
 Name             :   cai bing
 Organization     :   cai bing
 Address          :   honghualu 130
 City             :   hongan
 Province/State :   hubei
 Country          :   cn
 Postal Code      :   431500
 Phone Number     :   86-021-51697771
 Fax              :   86-021-51697771
 Email            :   mxmtmw@gmail.com
```

Historic WHOIS showing mxmtmw[at]gmail.com as a contact for grayflag[.]net

To confirm that we're still on the trail of a Cyber actor, the e-mail address also appeared in an online advert in Chinese for Trojan development.

Advert in Chinese offering development of customised Trojans

Luckily for us, the string "mxmtmw" is fairly unique online and has also appeared elsewhere, including in a group called Ph4nt0m in 2008, a year before the Mr Wu registration entry for twadcorp[.]com above. In one of those posts the mxmtmw string was used as the username of a poster, part of whose email address is visible in the archives as wuyin…[at]gmail.com.


Google
Search for messages
Sign in
Groups
Home
Click on a group's star icon to add it to your favourites
Recently viewed
Ph4nt0m
Privacy - Terms of Service
Translate message into English

kurau 23/09/2008

Re: [Ph4nt0m] 答复: [Ph4nt0m] 关于动态口令认证

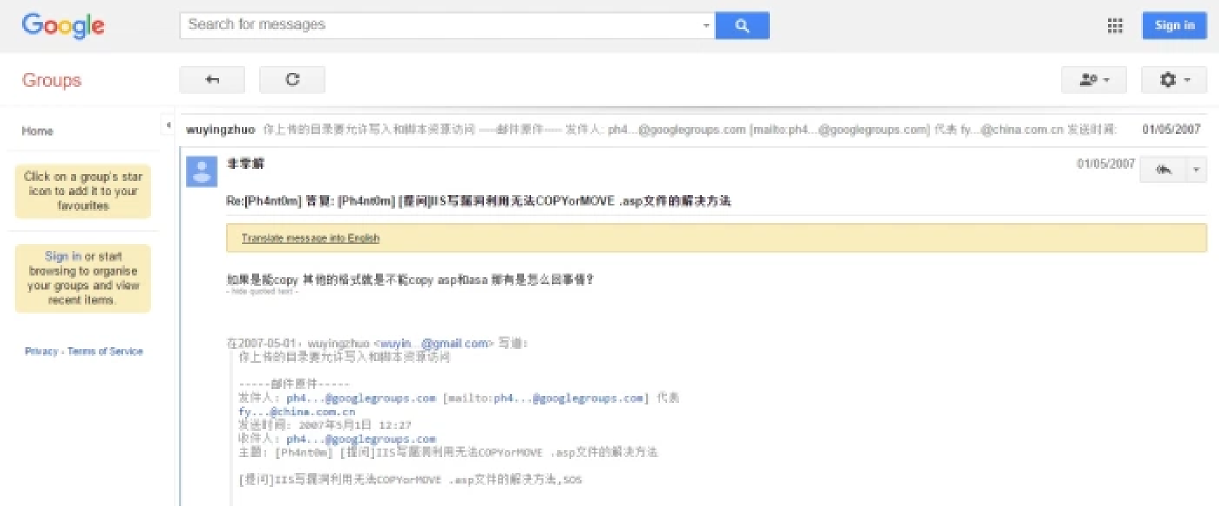
目前的动态口令卡基本都是双因素认证的，即楼上说的个人用户密码+动态口令组合。
因此令牌丢了，也是需要先破解个人用户密码的。只要及时申请注销/换卡就没事了。

2008/9/22 mxmtmw <wuyin...@gmail.com>
- hide quoted text -

> 不太明白，如果用户动态口令的钥匙丢了报告给管理员，重设一次不久得了。而且很多类似产品需要用户密码+动态口令组合的，可以联系RSA或者国内四川安盟之类的。
>
> -----邮件原件-----
> 发件人: ph4...@googlegroups.com [mailto:ph4...@googlegroups.com] 代表 54netoky
> 发送时间: 2008年9月22日星期一 16:57
> 收件人: ph4...@googlegroups.com
> 主题: [Ph4nt0m] 关于动态口令认证
>
> hi，all：
>
> 由于安全方面的考虑，拟打算在公司的VPN和服务器身份认证过程中使用动态口令身份验证，了解了目前的一些动态口令认证的产品，但是基本都是直接依靠生成的动态口令来验证的，一旦用来生成动态口令的这个key丢失了还是一样会存在安全隐患，有没有一种传统的认证和动态口令认证相结合的方案？比如为每个用户设置一个不同的前缀(例如密码前5位固定，但不同用户的这5位是不同的)，后面几位采用动态口令，不知是否可行？有用过这种认证的兄弟请指点一二。

Google Group entry associating "mxmtmw" with wuyin…[at]gmail.com

Continuing our journey back in time, a search on the wuyin partial email address reveals other posts related to the same partial address. In one posting from 2007, the poster used a username more helpful to our cause: “wuyingzhuo”. Might this be the same Mr Wu?


Google
Search for messages
Sign in
Groups
Home
Click on a group's star icon to add it to your favourites
Sign in or start browsing to organise your groups and view recent items.
Privacy - Terms of Service
Translate message into English
- hide quoted text -

wuyingzhuo 你上传的目录要允许写入和脚本资源访问 -----邮件原件----- 发件人: ph4...@googlegroups.com [mailto:ph4...@googlegroups.com] 代表 fy...@china.com.cn 发送时间: 01/05/2007

李学新 01/05/2007

Re:[Ph4nt0m] 答复: [Ph4nt0m] [提问]IIS写漏洞利用无法COPYorMOVE .asp文件的解决方法

如果是能copy 其他的格式就是不能copy asp和asa 都有是怎么回事情？

在2007-05-01，wuyingzhuo <wuyin...@gmail.com> 写道:
你上传的目录要允许写入和脚本资源访问

-----邮件原件-----
发件人: ph4...@googlegroups.com [mailto:ph4...@googlegroups.com] 代表
fy...@china.com.cn
发送时间: 2007年5月1日 12:27
收件人: ph4...@googlegroups.com
主题: [Ph4nt0m] [提问]IIS写漏洞利用无法COPYorMOVE .asp文件的解决方法

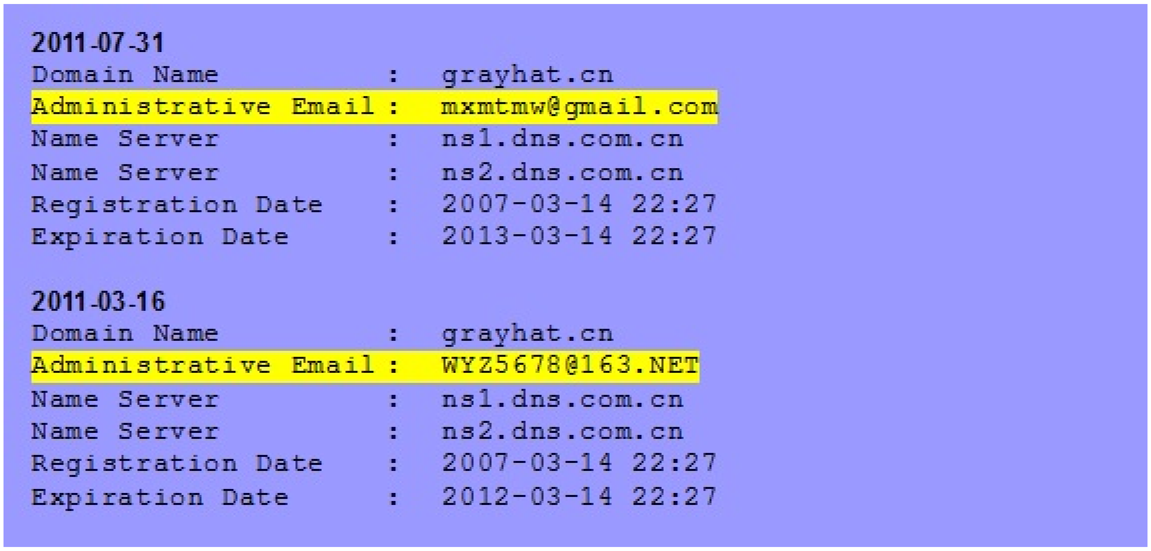
[提问]IIS写漏洞利用无法COPYorMOVE .asp文件的解决方法,SOS

Google Group entry showing poster wuyin…[at]gmail.com using username wuyingzhuo

From mxmtmw to wyz5678

Two further domain name records can be used to confirm Yingzhuo as Mr Wu’s given name.

Returning to the mxmtmw e-mail address, it also briefly appeared in registration data in mid-2011 for the domain grayhat[.]cn. Another e-mail address that was associated with the same domain (it appeared both before and after mxmtmw in the data) is wyz5678[at]163.net. “wyz” possibly stands for “wuyingzhuo”, the name we found in Google Groups.



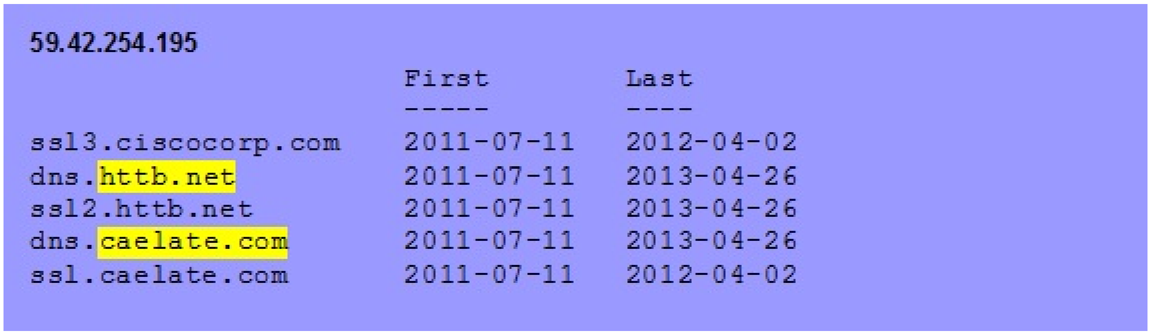
```
2011-07-31
Domain Name            :  grayhat.cn
Administrative Email :  mxmtmw@gmail.com
Name Server            :  ns1.dns.com.cn
Name Server            :  ns2.dns.com.cn
Registration Date      :  2007-03-14 22:27
Expiration Date        :  2013-03-14 22:27

2011-03-16
Domain Name            :  grayhat.cn
Administrative Email :  WYZ5678@163.NET
Name Server            :  ns1.dns.com.cn
Name Server            :  ns2.dns.com.cn
Registration Date      :  2007-03-14 22:27
Expiration Date        :  2012-03-14 22:27
```

Historic WHOIS showing relationship between mxmtmw and wyz5678

The wyz5678 e-mail address also appears in registration information for another domain-name: ciscocorp[.]com which may lead us to a possible location for APT3.

Infrastructure in Guangdong, China

DNS analysis of the ciscocorp domain shows that ssl3.ciscocorp[.]com previously resolved to IP address 59.42.254[.]195. That IP is owned by "guangdong guangxin tongxin fuwu you", which translates into English as the "Guangdong Guanxin Communications Services Company", a wireless telecommunications services company in Guangdong, China. This is possibly an ISP used by APT3 and may give some clue as to the location of the group.

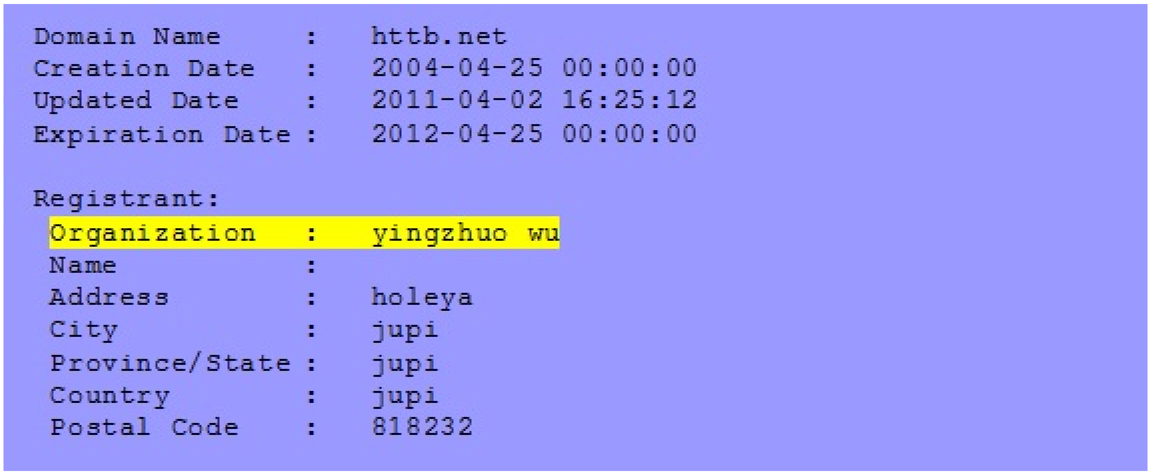


```
59.42.254.195
                          First        Last
                          -----        ----
ssl3.ciscocorp.com        2011-07-11   2012-04-02
dns.httb.net              2011-07-11   2013-04-26
ssl2.httb.net             2011-07-11   2013-04-26
dns.caelate.com           2011-07-11   2013-04-26
ssl.caelate.com           2011-07-11   2012-04-02
```

Historic DNS resolutions pointing to 59.42.254[.]195

Wu Yingzhuo

As shown above, similar sub-domains of two other domain names – httb[.]net and caelate[.]com – have also previously resolved to the same IP address. This is significant because the registered name in 2011 for both domains was "yingzhuo wu".



```
Domain Name     :   httb.net
Creation Date   :   2004-04-25 00:00:00
Updated Date    :   2011-04-02 16:25:12
Expiration Date :   2012-04-25 00:00:00

Registrant:
 Organization   :   yingzhuo wu
 Name           :
 Address        :   holeya
 City           :   jupi
 Province/State :   jupi
 Country        :   jupi
 Postal Code    :   818232
```

Historic WHOIS for httb.net showing the registrant as **yingzhuo wu**

In summary, it is possible to follow domain name registration data from APT3 tools and domains to Wu Yingzhuo. Wu Yingzhuo might live or work in Guangdong, China, and has expressed an interest online in Trojan development.

We intend to continue the trail from httb[.]net and to introduce you to a second member of APT3. Read our next post for more truth behind this intrusion.