虎符网络安全赛道CTF MISC 奇怪的组织

原创

enj0ym4 于 2020-04-22 08:23:50 发布 275 收藏 1

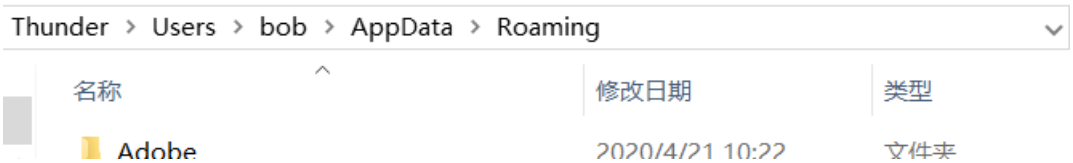
分类专栏： 2020虎符网络安全赛道CTF 文章标签： 其他

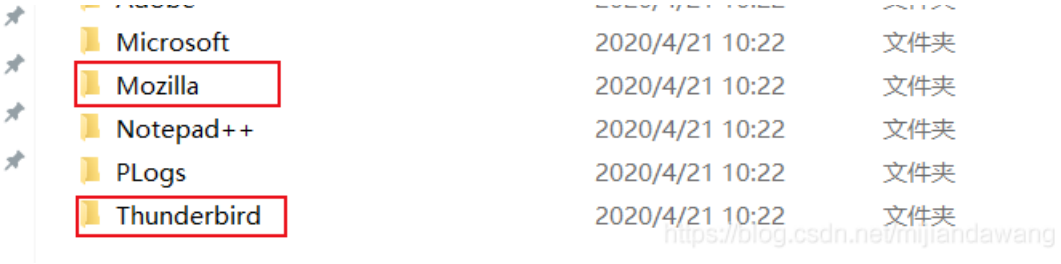
本文链接：https://blog.csdn.net/mijiandawang/article/details/105673322

题目如下

下载附件解压，根据提示找到User下的bob用户，查看AppData下的Roaming

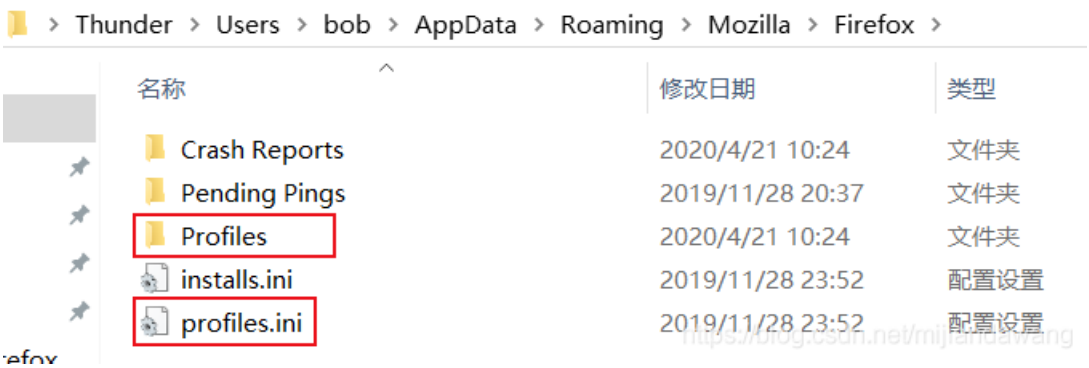
发现一个浏览器的文件和一个聊天软件的文件



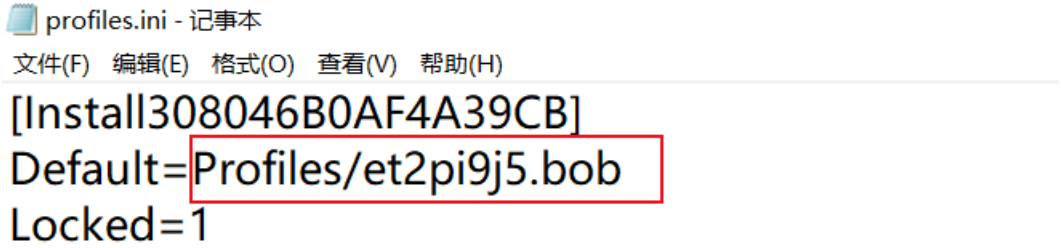


然后自己下载安装Firefox和Thunderbird，然后先启动一下这两个软件，接着就在自己的电脑找到如下文件

把下载的附件中的Firefox的如下文件覆盖到自己电脑的对应位置

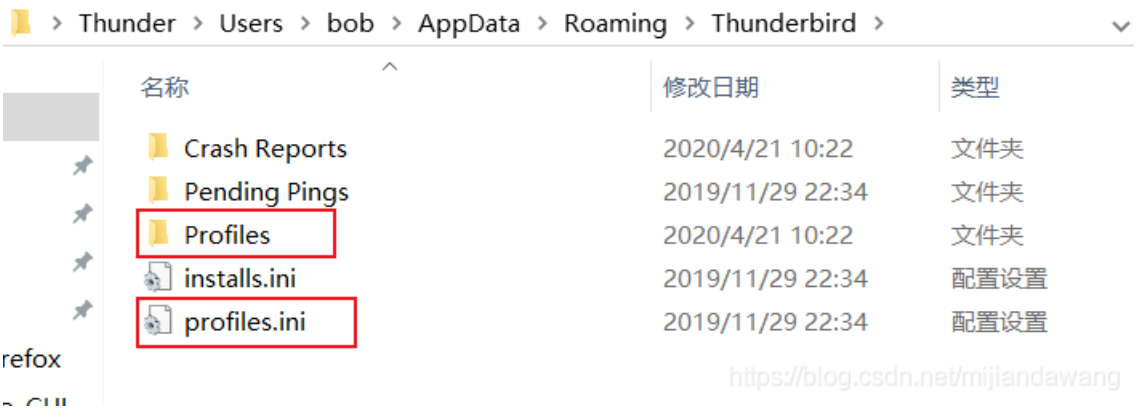


接着修改配置文件profiles.ini指定复制过来的文件



```
[Profile2]
Name=default-release-1
IsRelative=1
Path=Profiles/hn0lxrho.default-release

[Profile1]
Name=bob
IsRelative=1
Path=Profiles/et2pi9j5.bob

[Profile0]
Name=default-release
IsRelative=1
Path=Profiles/hn0lxrho.default-release
Default=1

[General]
StartWithLastProfile=1
Version=2

[InstallF60400B719B2D51E]
Default=Profiles/hn0lxrho.default-release
Locked=1
```


Thunderbird也一样



[Install8216C80C92C4E828]
Default=Profiles/7ev2i8k4.default-release
Locked=1

[Profile2]
Name=default-release-1
IsRelative=1
Path=Profiles/7ev2i8k4.default-release

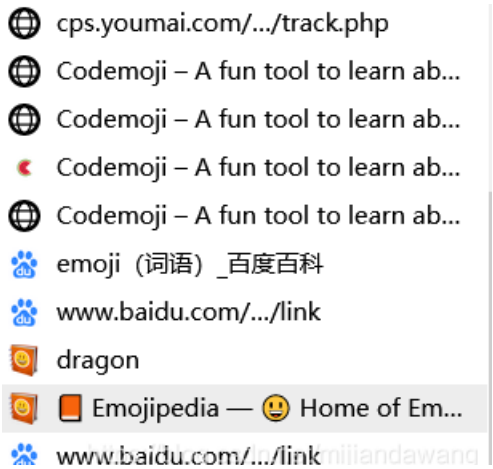
[Profile1]
Name=default
IsRelative=1
Path=Profiles/03hrkuvh.default
Default=1

[Profile0]
Name=default-release
IsRelative=1
Path=Profiles/7ev2i8k4.default-release

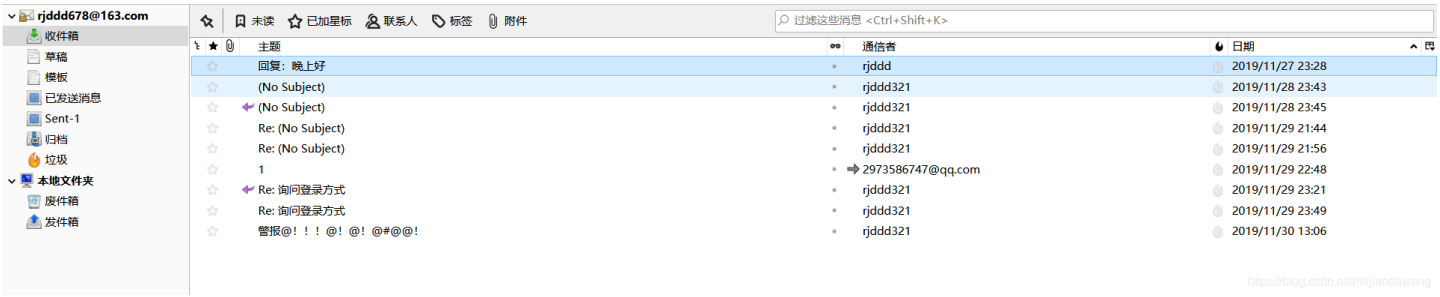
[General]
StartWithLastProfile=1
Version=2

[InstallDAEA17354F10BE6B]
Default=Profiles/7ev2i8k4.default-release
Locked=1

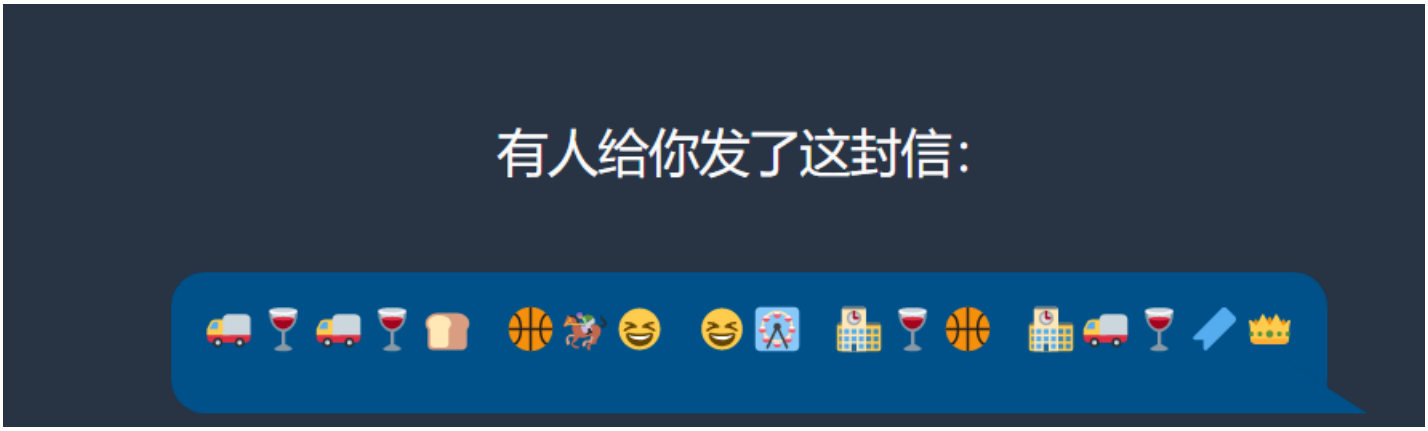
完成上述操作后，再次打开Firefox，查看浏览记录



打开Thunderbird，发现邮件，按时间排序下



然后点了下那个网站

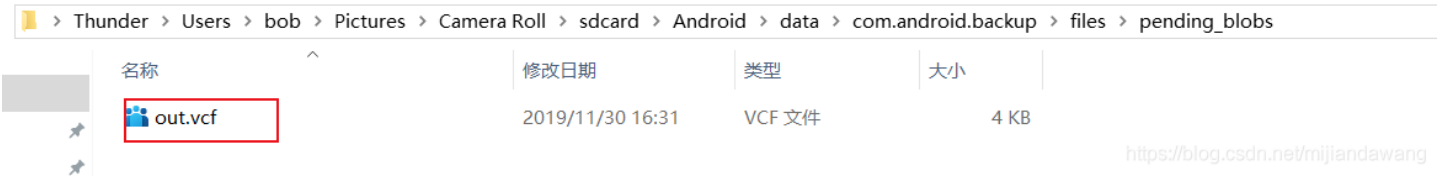


破译

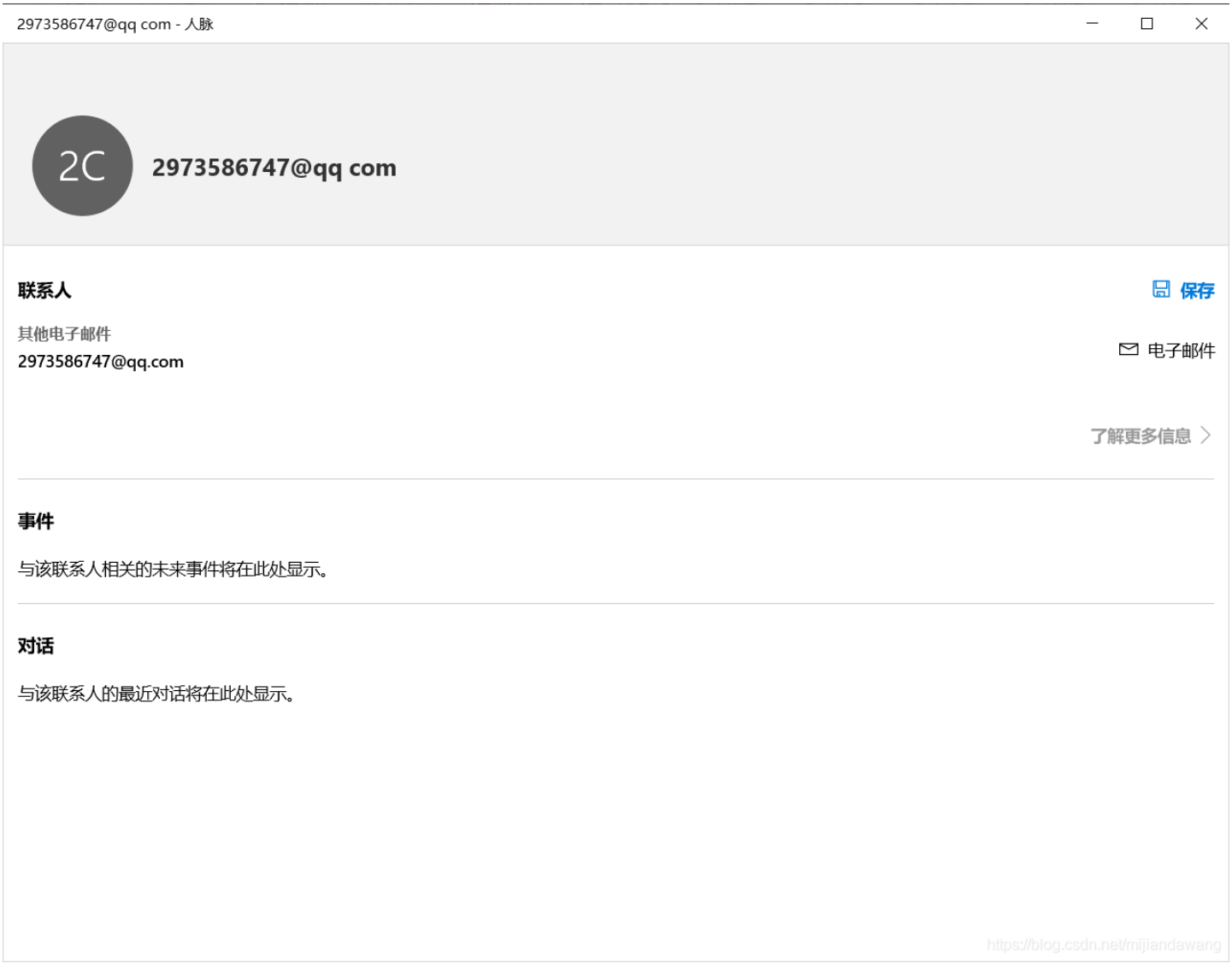
https://blog.csdn.net/mijiandawang

点击破译，似乎需要密码，想起浏览记录在浏览□这个符号，密码正是该符号
然后逐步还原信息

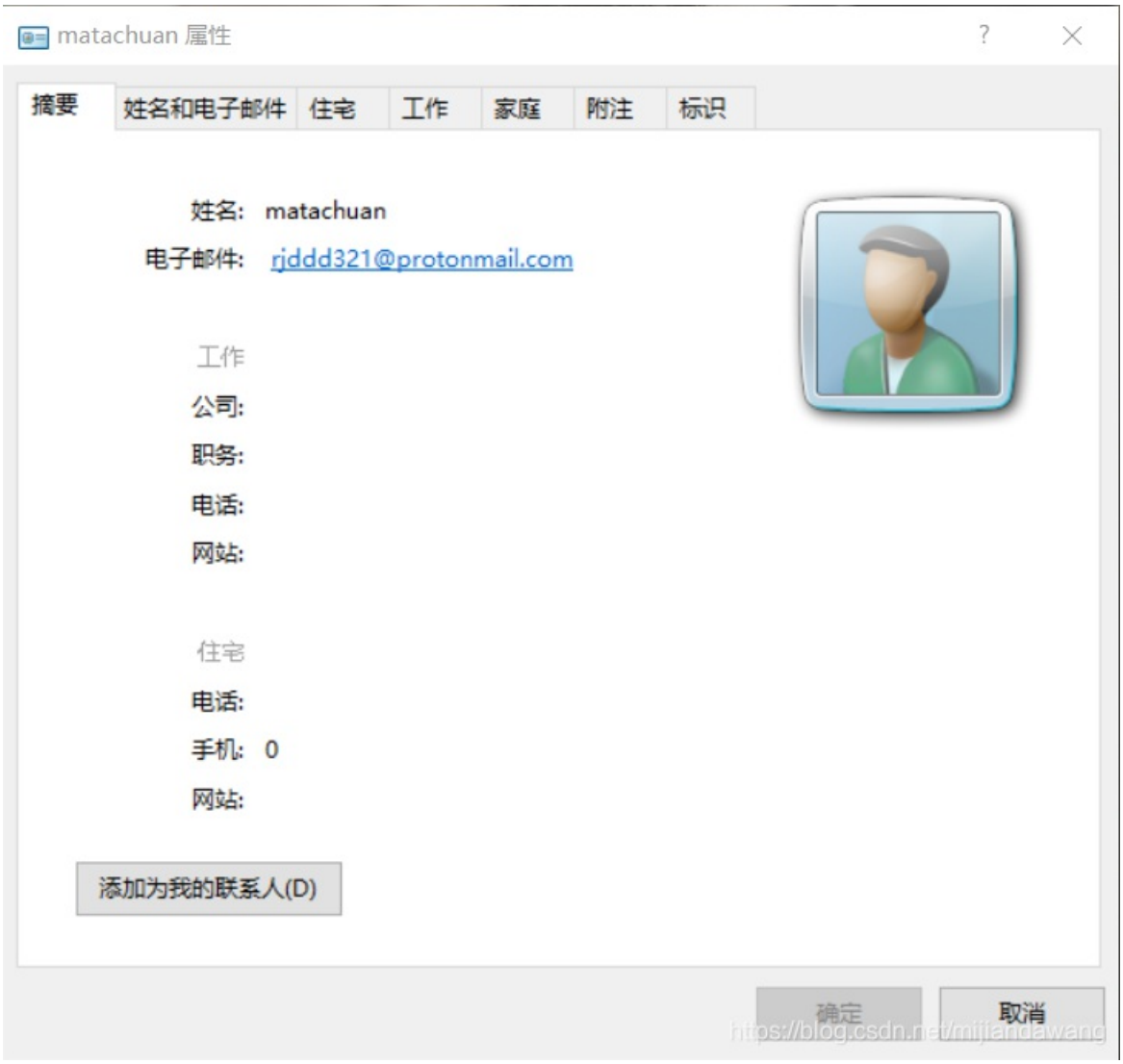
但是还有两封主题为：Re: 询问登录方式 的邮件没能同意的方法破解，然后根据聊天内容，我们需要找到real name，或许real name是解密那两封邮件的密钥，接着在如下目录发现一个vCalendar 文件



但是直接打开，有可能是下面这种情况，需要用windows联系人的方式打开

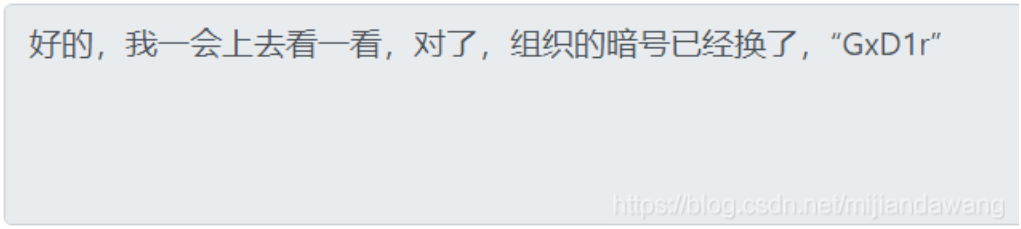


就很奇怪，没看到什么姓名，然后点取消，发现由弹一个联系人出来，一直取消一直弹，一直弹一直取消，然后发现如下一个联系人，和Thunderbird一样的电子邮件。



然后使用这个网站：

https://aghorler.github.io/emoji-aes/进行剩下的emoji解密，其中有一段是下面这样的，发现一个暗号，并且根据聊天内容可知有一个后台网站



然后就找phpstudy_pro

逐个打开后，发现一段密文：
U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTOt1nlUllLgNXSKQxliF8zmWz2cdmmPxmQkeQ/uF3INEXBZlhruUFJg==

最后的波纹

时间:2019-11-30 12:56来源:未知 作者:admin 点击: 次
这是我最后的博文了 我不做内鬼了jojo U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTOt1nlUllLgNXSKQxliF8zmWz2cdmmPxm QkeQ/uF3INEXBZlhruUFJg==
这是我最后的博文了
我不做内鬼了jojo
U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTOt1nlUllLgNXSKQxliF8zmWz2cdmmPxm
QkeQ/uF3INEXBZlhruUFJg==
(责任编辑：admin)

密钥为暗号GxD1r拿去AES解密即可得到flag