

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[2020虎符网络安全赛道CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

题目如下

奇怪的组织

分值: 455 未解答

最近盯上了一个奇怪的组织, 我们的研究人员从一名组织成员的电脑里拿到了一些东西, 不知道这个神秘的组织在策划着什么?

附件下载 提取码: (yzsa)

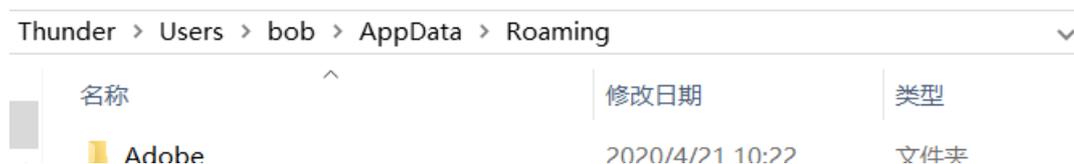
备用快传 密码: (ChunQiuGame)

注意用户的浏览行为, 注意用户的聊天内容。

Flag:

提交

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



Microsoft	2020/4/21 10:22	文件夹
Mozilla	2020/4/21 10:22	文件夹
Notepad++	2020/4/21 10:22	文件夹
PLogs	2020/4/21 10:22	文件夹
Thunderbird	2020/4/21 10:22	文件夹

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

> 此电脑 > 本地磁盘 (C:) > 用户 > 78591 > AppData > Roaming

名称	修改日期	类型
360zip	2020/4/19 9:20	文件夹
Adobe	2020/3/11 20:54	文件夹
Audacity	2020/4/19 9:32	文件夹
BurpSuite	2020/3/12 19:04	文件夹
Macromedia	2020/4/19 9:04	文件夹
Microsoft	2020/3/17 18:24	文件夹
Mozilla	2020/3/12 18:59	文件夹
Notepad++	2020/4/16 15:02	文件夹
scandirplus.ScandirPlus	2020/3/16 18:41	文件夹
Sun	2020/3/12 18:23	文件夹
SweetScape	2020/4/15 16:58	文件夹
Tencent	2020/4/19 9:10	文件夹
Thunderbird	2020/4/21 10:28	文件夹
Wireshark	2020/4/18 12:02	文件夹
jd-gui.cfg	2020/4/18 11:27	CFG 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

> Thunder > Users > bob > AppData > Roaming > Mozilla > Firefox >

名称	修改日期	类型
Crash Reports	2020/4/21 10:24	文件夹
Pending Pings	2019/11/28 20:37	文件夹
Profiles	2020/4/21 10:24	文件夹
installs.ini	2019/11/28 23:52	配置设置
profiles.ini	2019/11/28 23:52	配置设置

接着修改配置文件profiles.ini指定复制过来的文件

```
profiles.ini - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
[Install308046B0AF4A39CB]
Default=Profiles/et2pi9j5.bob
Locked=1
```

[Profile2]
Name=default-release-1
IsRelative=1
Path=Profiles/hn0lrxho.default-release

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

[Profile0]
Name=default-release
IsRelative=1
Path=Profiles/hn0lrxho.default-release
Default=1

[General]
StartWithLastProfile=1
Version=2

[InstallF60400B719B2D51E]
Default=Profiles/hn0lrxho.default-release
Locked=1

<https://blog.csdn.net/mijjandawang>

Thunderbird也一样

Thunderbird > Users > bob > AppData > Roaming > Thunderbird >

名称	修改日期	类型
Crash Reports	2020/4/21 10:22	文件夹
Pending Pings	2019/11/29 22:34	文件夹
Profiles	2020/4/21 10:22	文件夹
installs.ini	2019/11/29 22:34	配置设置
profiles.ini	2019/11/29 22:34	配置设置

refox

<https://blog.csdn.net/mijjandawang>

profiles.ini - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

file:///C:/Users/bob/AppData/Roaming/Thunderbird/Profiles/hn0lrxho.default-release

[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

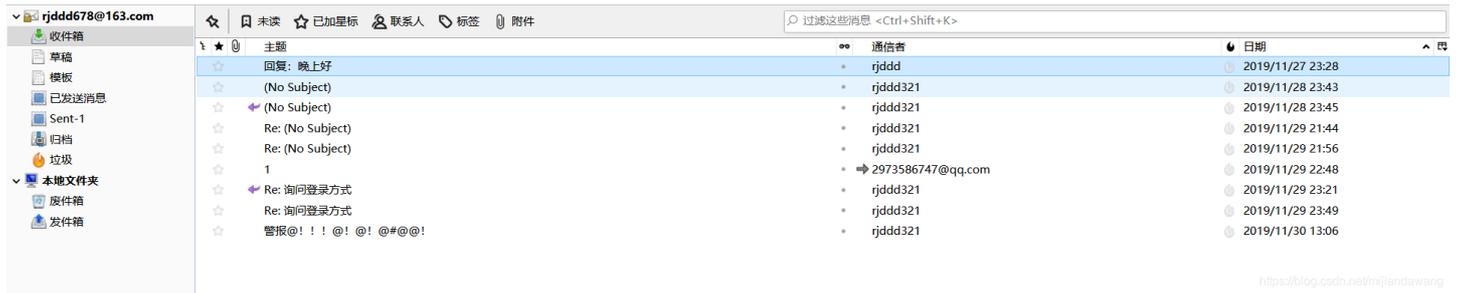
Locked=1

<https://blog.csdn.net/mijiandawang>

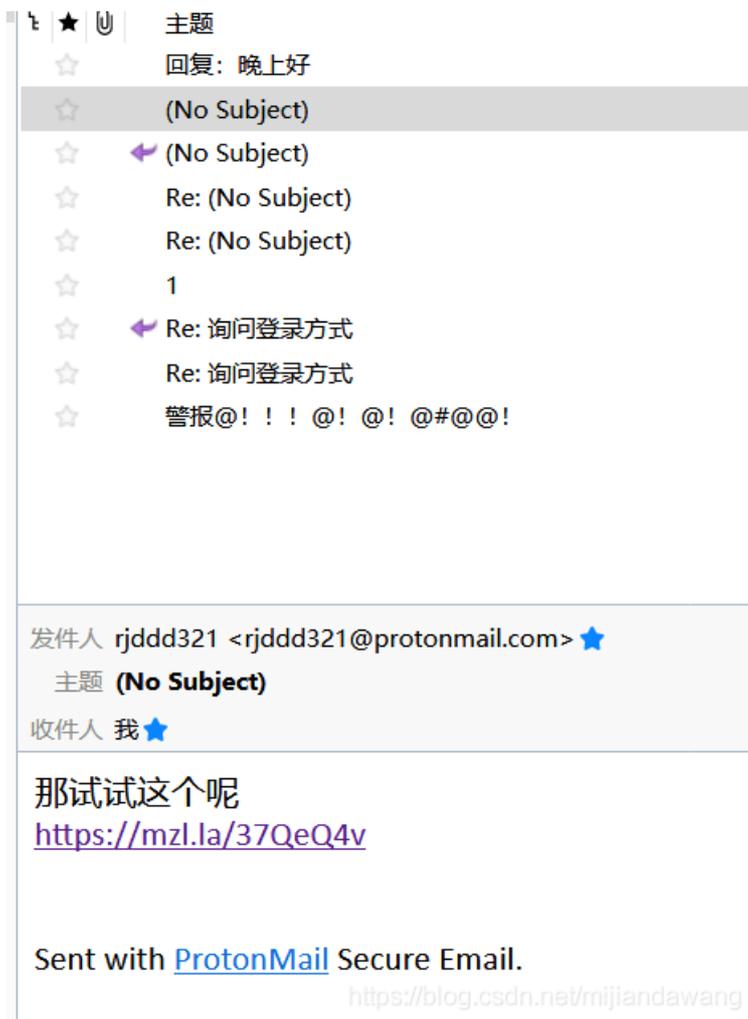
完成上述操作后，再次打开Firefox，查看浏览记录

-  cps.youmai.com/.../track.php
-  Codemoji – A fun tool to learn ab...
-  Codemoji – A fun tool to learn ab...
-  Codemoji – A fun tool to learn ab...
-  Codemoji – A fun tool to learn ab...
-  emoji (词语) _百度百科
-  www.baidu.com/.../link
-  dragon
-  Emojipedia — 😊 Home of Em...
-  www.baidu.com/.../link mijiandawang

打开Thunderbird，发现邮件，按时间排序下



然后点了下那个网站



有人给你发了这封信：

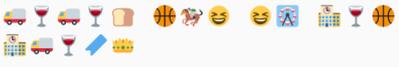


破译

<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

加扰信息



表情符号来解读信息



你的信息

哈哈，现在我们可以聊天了！

9~10成熟！

创建新消息

<https://blog.csdn.net/mijiandawang>

加扰信息



表情符号来解读信息



你的信息

是啊也许...。让我想想...

<https://blog.csdn.net/mijiandawang>

加扰信息



表情符号来解读信息



你的信息

啊哈，这条路很安全！记住我的真名！

<https://blog.csdn.net/mijiandawang>

加扰信息



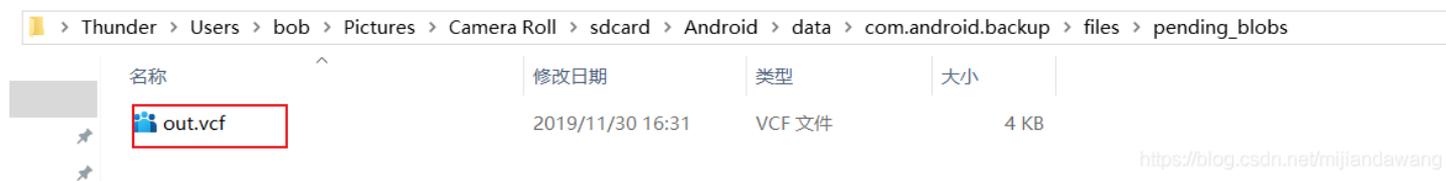
表情符号来解读信息



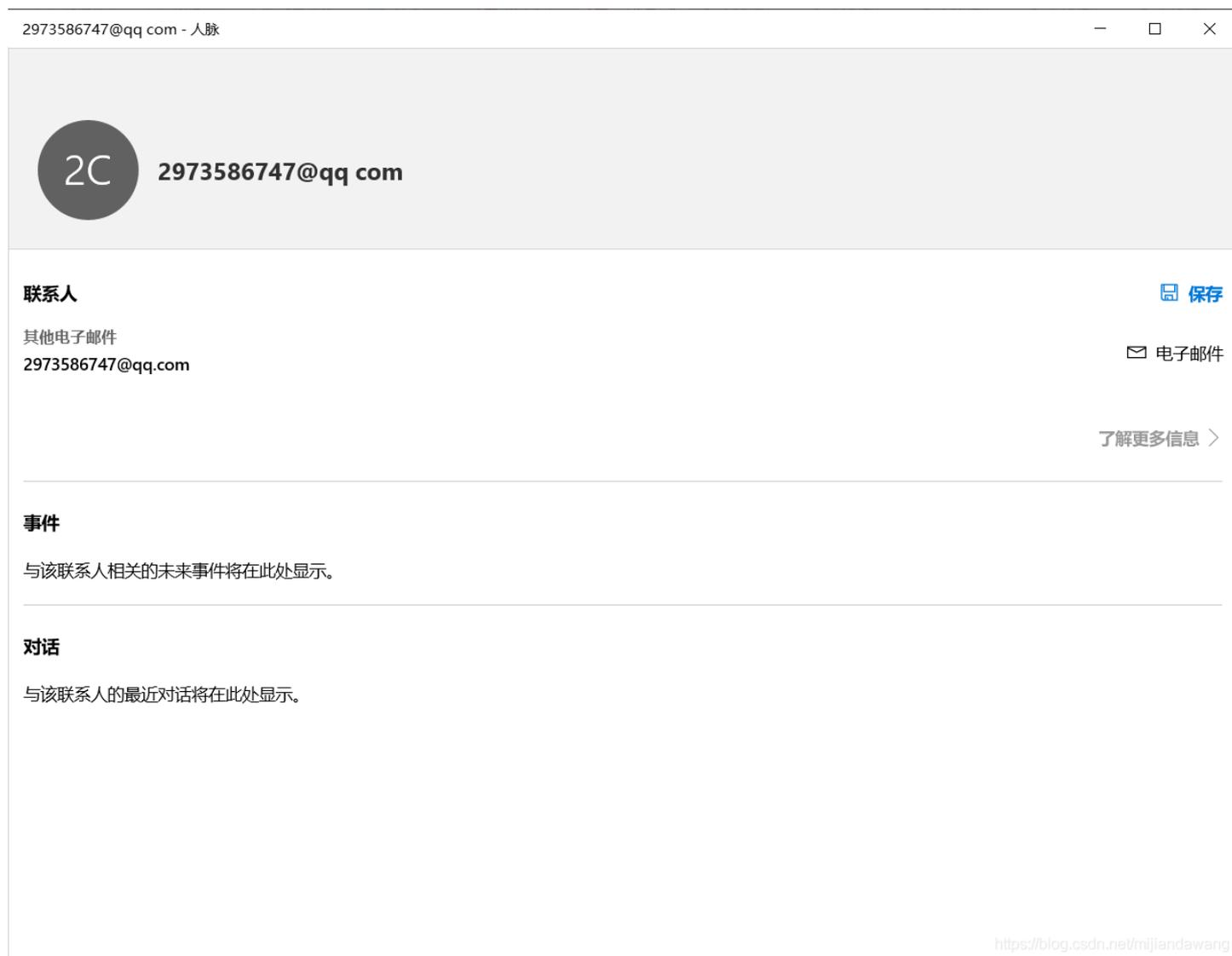
你的信息

但这把钥匙太弱了！

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

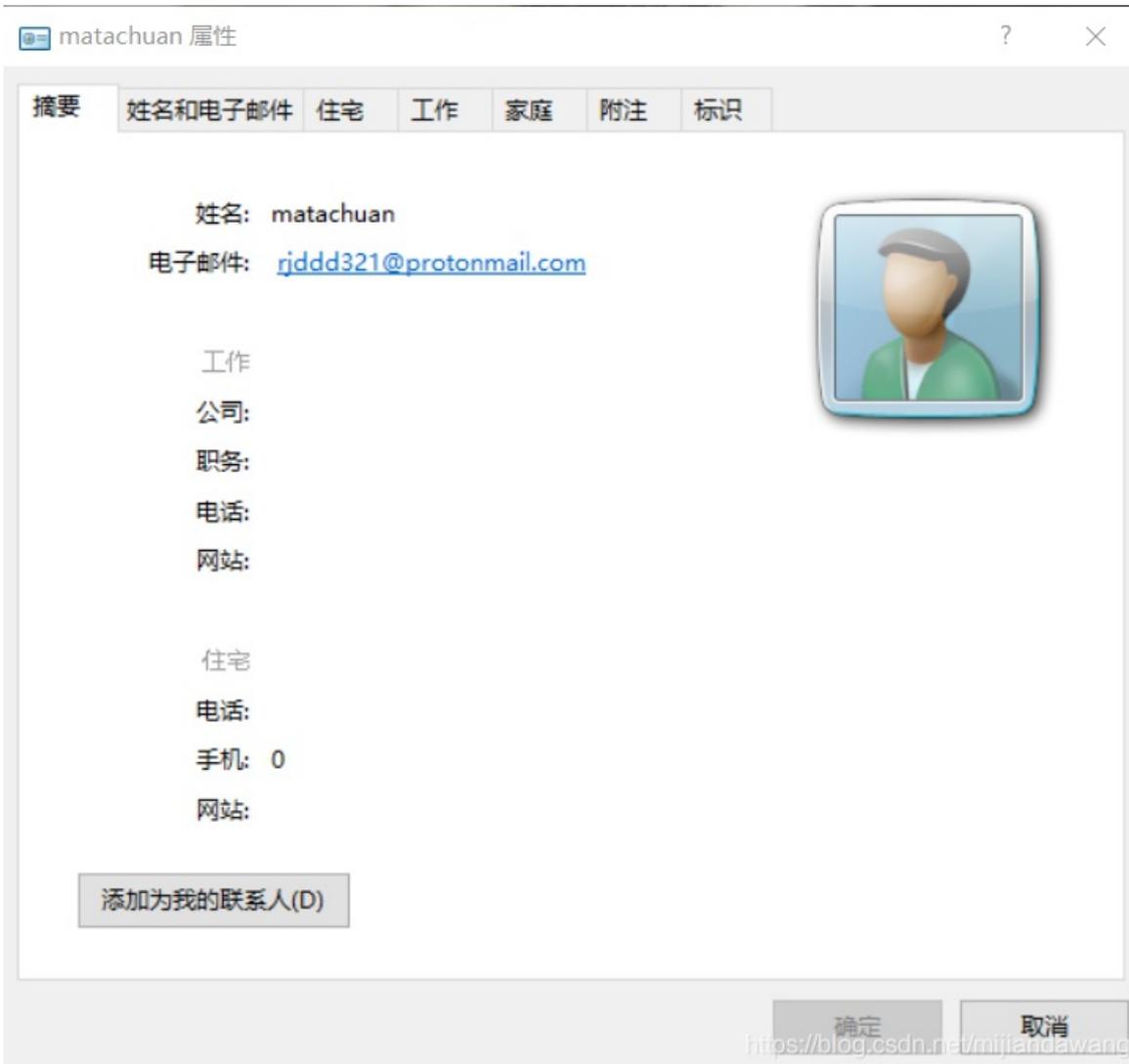


但是直接打开, 有可能是下面这种情况, 需要用windows联系人的方式打开





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

好的，我一会上去看一看，对了，组织的暗号已经换了，“GxD1r”

<https://blog.csdn.net/mijiandawang>

然后就找phpstudy_pro

Thunder > phpstudy_pro > WWW > dede > a > Blog > 2019 > 1130 搜索"1130"

名称	修改日期	类型	大小
 2.html	2019/11/30 12:56	QQBrowser HT...	19 KB
 3.html	2019/11/30 12:57	QQBrowser HT...	19 KB
 4.html	2019/11/30 12:57	QQBrowser HT...	19 KB

<https://blog.csdn.net/mijiandawang>

逐个打开后，发现一段密文：

U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTot1nIUllgNXSKQxliF8zmWz2cdmmPxmQkeQ/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+z9Q5Yznug4MiYfkWZNHWTot1nIUllgNXSKQxliF8zmWz2cdmmPxm QkeQ/uF3INEXBZlhruUFJg==

这是我最后的博文了

我不做内鬼了jojo

U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTot1nIUllgNXSKQxliF8zmWz2cdmmPxm

QkeQ/uF3INEXBZlhruUFJg==

(责任编辑: admin)

<https://blog.csdn.net/mijiandawang>

密钥为暗号GxD1r拿去AES解密即可得到flag