虎符CTF--MISC--奇怪的组织

原创

说白道黑 于 2020-04-21 12:09:45 发布 1673 收藏 1
分类专栏： CTF

本文链接：https://blog.csdn.net/a965527596/article/details/105644062

奇怪的组织

1.拿到文件发现是c盘文件，然后发现用phpstudy建了一个dede的站，发现了3个博客和一段密文，但是没有解密的信息。

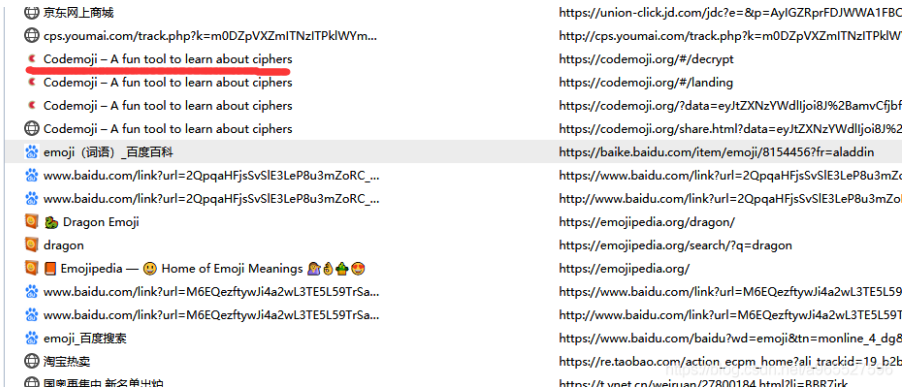
最后的波纹

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+z9Q5Yznug4MiYfkWZNHWTOt1nIUllLgNXSKQxIiF8zmWz2cdmmPxm QkeQ/uF3INEXBZlhruUFJg==
这是我最后的博文了
我不做内鬼了jojo
U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTOt1nIUllLgNXSKQxIiF8zmWz2cdmmPxm
QkeQ/uF3INEXBZlhruUFJg==
(责任编辑：admin)

先试试了base64，结果不对，然后猜测是AES加密，解密需要key，继续从文件中找。

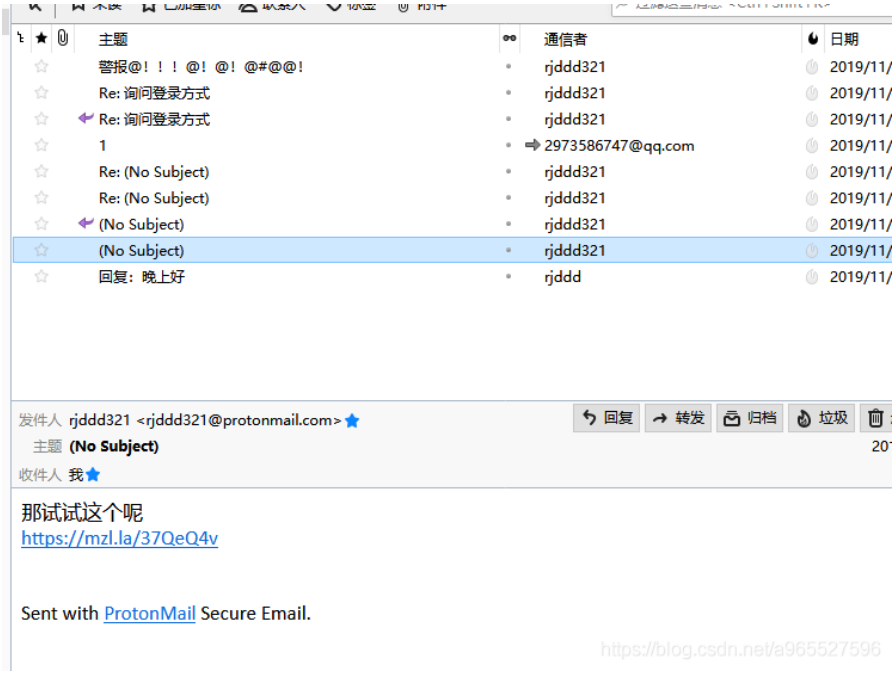
2.官方提示看浏览行为和聊天信息，于是利用places.sqlite文件还原火狐的历史记录，发现bob先是建了dede的站，然后访问了一个emoji的解密网站。

cps.youmai.com/track.php?k=Ddm0DZpVXZmITNzITPklWY...	https://cps.youmai.com/track.php?k=Ddm0DZpVXZmITNzITPklV
百度一下，你就知道	https://www.baidu.com/index.php?tn=monline_3_dg
spacesniffer_1_3_0_2.zip	https://download.fosshub.com/Protected/expiretime=15749959
Download SpaceSniffer latest release	https://www.fosshub.com/SpaceSniffer.html
SpaceSniffer extras downloads	http://www.uderzo.it/main_products/space_sniffer/download_ex
SpaceSniffer download	http://www.uderzo.it/main_products/space_sniffer/download.htr
SpaceSniffer, find lost disk space the easy way.	http://www.uderzo.it/main_products/space_sniffer/
SpaceSniffer – 直观查看文件/文件夹占用磁盘空间的大小 - Wi...	https://www.windows10.pro/spacesniffer-download/
phpStudy_64.7z	http://public.xp.cn/upgrades/phpStudy_64.7z
phpStudy - 让天下没有难配的服务器环境!	https://m.xp.cn/
www.baidu.com/link?url=OIEgjCirDWPu4BDX2HKPJOllXW...	https://www.baidu.com/link?url=OIEgjCirDWPu4BDX2HKPJOllXV
www.baidu.com/link?url=OIEgjCirDWPu4BDX2HKPJOllXW...	http://www.baidu.com/link?url=OIEgjCirDWPu4BDX2HKPJOllXW
phpstudy_百度搜索	https://www.baidu.com/baidu?wd=phpstudy&tn=monline_3_dg
Inbox | rjddd321@protonmail.com | ProtonMail	https://mail.protonmail.com/inbox
Login | ProtonMail	https://mail.protonmail.com/login
Secure email: ProtonMail is free encrypted email.	https://protonmail.com/
www.baidu.com/link?url=oDrY_xLVCZFcIrpdDjEwAHsv9Yny...	https://www.baidu.com/link?url=oDrY_xLVCZFcIrpdDjEwAHsv9Y
protonmail_百度搜索	https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&t
www.baidu.com/link?url=E-ZGhaDooJTiSn6cFua2hm4RQO...	https://www.baidu.com/link?url=E-ZGhaDooJTiSn6cFua2hm4RQ
新浪_百度搜索	https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&t
火狐_百度搜索	https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&t
www.mozilla.org/zh-CN/privacy/firefox/	https://www.mozilla.org/zh-CN/privacy/firefox/



3.根据文件的名字发送thunderbird邮件发送软件，根据thunderbird数据迁移，还原thunderbird的记录发现了邮件记录。

https://support.mozilla.org/zh-CN/kb/将%20Thunderbird%20的数据迁移到另一台计算机



聊天都是加密的，发现了刚才浏览器里面的解密网站，解密需要选一个表情，根据浏览记录的龙，所以用龙的表情来解密。

邮件记录为：

rjddd：无内鬼来点题目

rjddd321：那试试这个呢（haha, now we can chat!）

rjddd321：哦对了，密码你知道的，还是那个

rjddd：当然

rjddd：but this key is too weak!

rjddd321：yeah, maybe... let me think ...

rjddd321：haha, this way is safe!Remember my real name!

https://mzl.la/2svfAf5

然后就换了加密方式，把密文前几个goole搜一下发现是这个网站的加密https://aghorler.github.io/emoji-aes/，需要ket才能解密，

而且提示记住我的真实姓名，于是再从文件中找相关的信息。

4.再看看文件里面的内容，还发现了装有TeamViewer但是没有任何数据，最后在图片里面发现了sdcard文件，是手机的系统文件，先在里面发现了几张钉钉打开的截图，名字是大黑，拿去解密结果不对，大黑应该rjddd的真实姓名，rjddd321和他是朋友，于是想到去恢复手机通讯录，goole搜索得知手机通讯录的文件后缀为vcf，然后在everything中搜素vcf发现了Contacts.vcf，利用vcf编辑器恢复，发现了rjddd312的姓名为matachuan，拿去解密成功解密。

rjddd321：这个还能加密中文呢，无敌了

rjddd：那你把后台账户发我吧

rjddd321：admin admin

rjddd：好的，我一会上去看一看，对了，组织的暗号已经换了，“GxD1r”

rjddd321：帮你传了点东西，以后你写博客应该用的到

GxD1r为博客中AES密文的密码然后解密

flag{3e5923d2-c31c-49cd-bfa3-e366a1a59c4d}

GxD1r

密码是可选项，也就是可以不填。

解密 加密

U2FsdGVkX1+z9Q5Yznug4MiYfkWZNHWTOt1nIUllLgNXSKQxIiF8zmWz2cdmmPxm QkeQ/uF3INEXBZIhruUFJg==