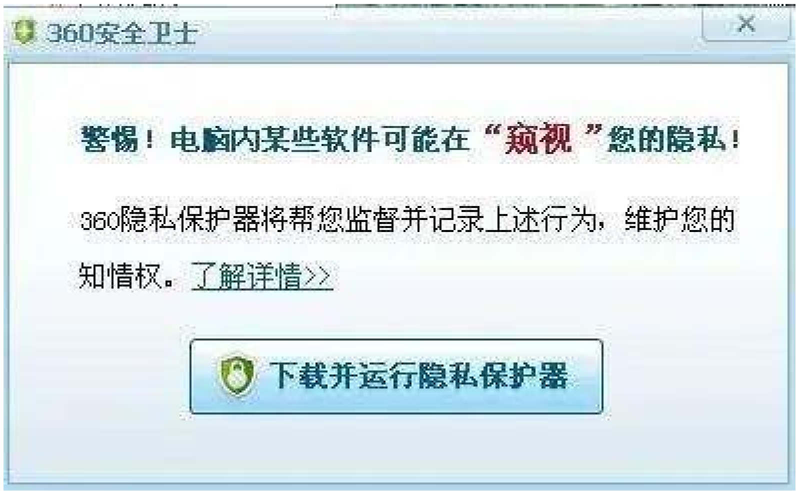
关于QQ偷偷读取用户历史浏览记录的澄清！附吾爱拦截神器！

小小莫理 莫理

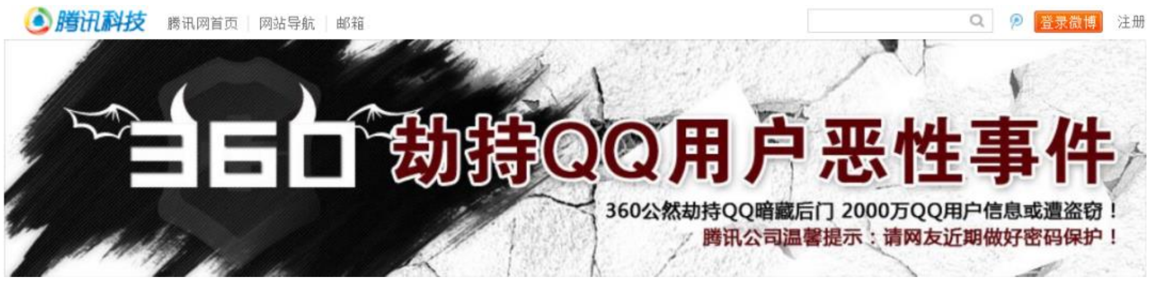
关注莫理！每天获取稀奇古怪的好东西

当年的3Q 大战



警惕！电脑内某些软件可能在“窥视 ”您的隐私！

360隐私保护器将帮您监督并记录上述行为，维护您的知情权。了解详情>>



360劫持QQ用户恶性事件

360公然劫持QQ暗藏后门 2000万QQ用户信息或遭盗窃！

腾讯公司温馨提示：请网友近期做好密码保护！

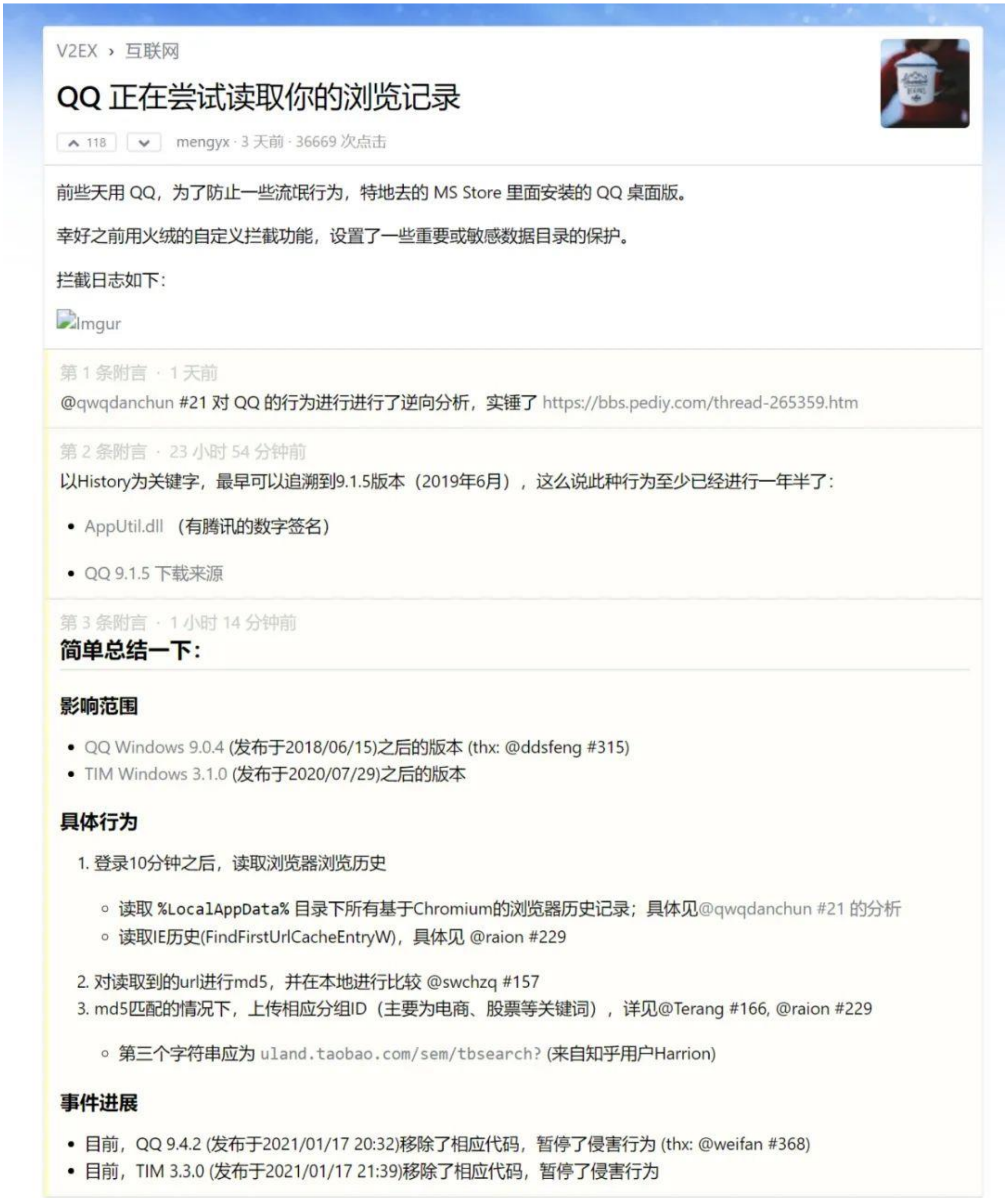
*https://tech.qq.com/zt2010/360defameqq

正文

今天看到群里发了一篇v2ex上的帖子：

https://www.v2ex.com/t/745030

但是一位小伙伴说说复现了整个过程，而且是QQ登录10分钟后才会去访问。



V2EX › 互联网

QQ 正在尝试读取你的浏览记录

118 mengyx · 3 天前 · 36669 次点击

前些天用 QQ，为了防止一些流氓行为，特地去的 MS Store 里面安装的 QQ 桌面版。

幸好之前用火绒的自定义拦截功能，设置了一些重要或敏感数据目录的保护。

拦截日志如下：

Imgur

第 1 条附言 · 1 天前

@qwqdanchun #21 对 QQ 的行为进行进行了逆向分析，实锤了 https://bbs.pediy.com/thread-265359.htm

第 2 条附言 · 23 小时 54 分钟前

以History为关键字，最早可以追溯到9.1.5版本（2019年6月），这么说此种行为至少已经进行一年半了：

- AppUtil.dll （有腾讯的数字签名）
- QQ 9.1.5 下载来源

第 3 条附言 · 1 小时 14 分钟前

简单总结一下：

影响范围

- QQ Windows 9.0.4 (发布于2018/06/15)之后的版本 (thx: @ddsfeng #315)
- TIM Windows 3.1.0 (发布于2020/07/29)之后的版本

具体行为

1. 登录10分钟之后，读取浏览器浏览历史
   - 读取 %LocalAppData% 目录下所有基于Chromium的浏览器历史记录；具体见@qwqdanchun #21 的分析
   - 读取IE历史(FindFirstUrlCacheEntryW)，具体见 @raion #229
2. 对读取到的url进行md5，并在本地进行比较 @swchzq #157
3. md5匹配的情况下，上传相应分组ID（主要为电商、股票等关键词），详见@Terang #166, @raion #229
   - 第三个字符串应为 uland.taobao.com/sem/tbsearch? (来自知乎用户Harrion)

事件进展

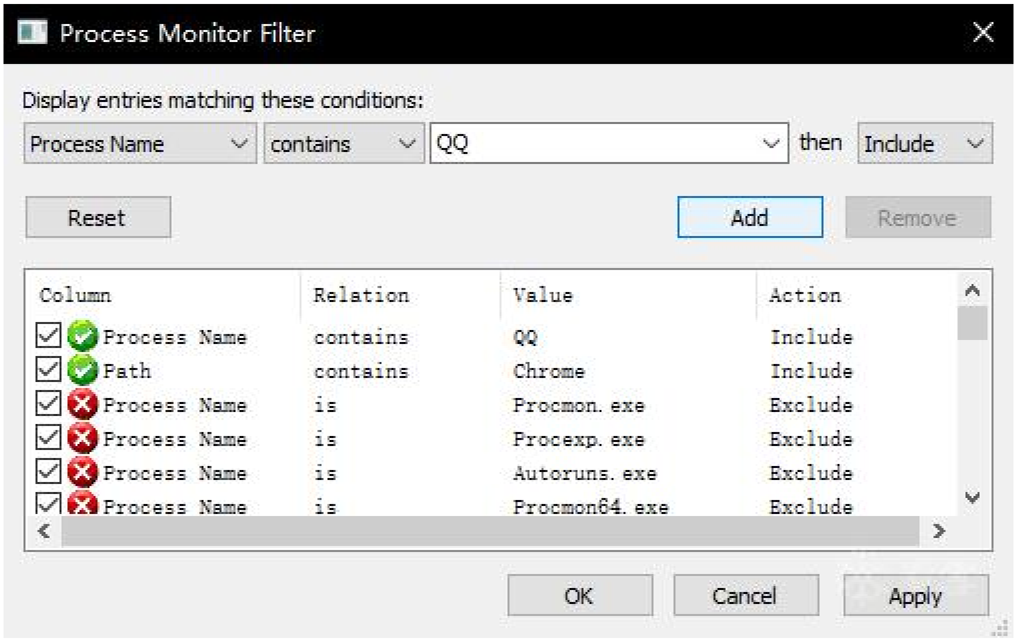
- 目前，QQ 9.4.2 (发布于2021/01/17 20:32)移除了相应代码，暂停了侵害行为 (thx: @weifan #368)
- 目前，TIM 3.3.0 (发布于2021/01/17 21:39)移除了相应代码，暂停了侵害行为

贴中说QQ会读取Chrome的历史记录，被火绒自定义规则拦截了，本来我是不信的。

但是一位小伙伴说说复现了整个过程，而且是QQ登录10分钟后才会去访问。

这我就想去验证下了，开虚拟机装QQ、Chrome。

然后打开Process Monitor开始等。规则简单的过滤下。



Process Monitor Filter

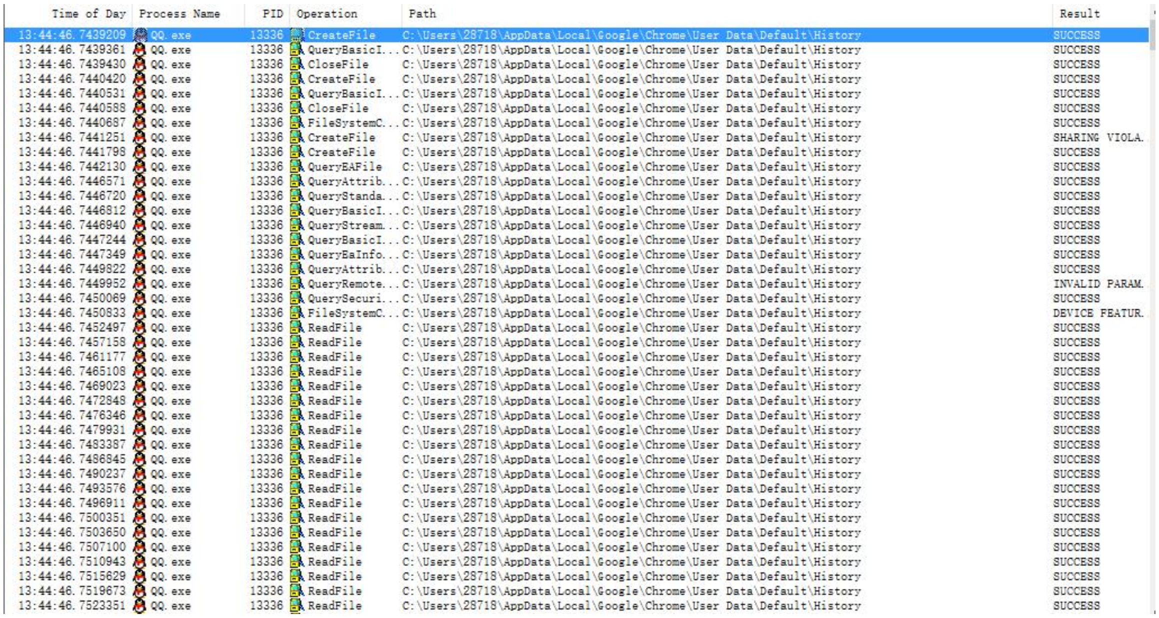
Display entries matching these conditions:

Process Name | contains | QQ | then | Include

Column	Relation	Value	Action
☑ ✓ Process Name	contains	QQ	Include
☑ ✓ Path	contains	Chrome	Include
☑ ☒ Process Name	is	Procmon.exe	Exclude
☑ ☒ Process Name	is	Procexp.exe	Exclude
☑ ☒ Process Name	is	Autoruns.exe	Exclude
☑ ☒ Process Name	is	Procmon64.exe	Exclude

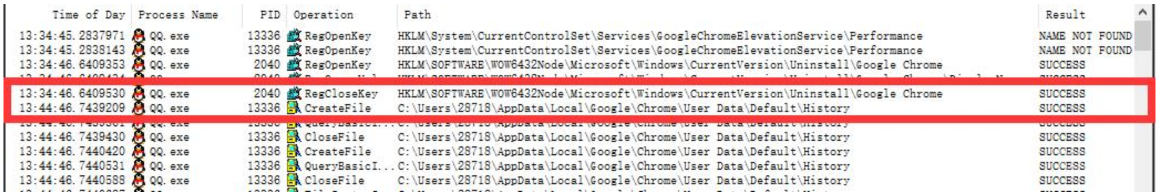
果然看到了读取下面目录的操作。

AppData\Local\Google\Chrome\UserData\Default\History



```
     Time of Day  Process Name     PID  Operation       Path                                                        Result
13:44:46.7439209  QQ.exe         13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7439361  QQ.exe         13336  QueryBasicI...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7439430  QQ.exe         13336  CloseFile       C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7440420  QQ.exe         13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7440531  QQ.exe         13336  QueryBasicI...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7440588  QQ.exe         13336  CloseFile       C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7440687  QQ.exe         13336  FileSystemC...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7441251  QQ.exe         13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SHARING VIOLA.
13:44:46.7441798  QQ.exe         13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7442130  QQ.exe         13336  QueryEAFile     C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7446571  QQ.exe         13336  QueryAttrib...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7446720  QQ.exe         13336  QueryStanda...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7446812  QQ.exe         13336  QueryBasicI...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7446940  QQ.exe         13336  QueryStream...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7447244  QQ.exe         13336  QueryBasicI...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7447349  QQ.exe         13336  QueryEaInfo...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7449822  QQ.exe         13336  QueryAttrib...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7449952  QQ.exe         13336  QueryRemote...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  INVALID PARAM.
13:44:46.7450069  QQ.exe         13336  QuerySecuri...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7450833  QQ.exe         13336  FileSystemC...  C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  DEVICE FEATUR.
13:44:46.7452497  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7457158  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7461177  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7465108  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7469023  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7472848  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7476346  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7479931  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7483387  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7486845  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7490237  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7493576  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7496911  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7500351  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7503650  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7507100  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7510943  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7515629  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7519673  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
13:44:46.7523351  QQ.exe         13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History  SUCCESS
```

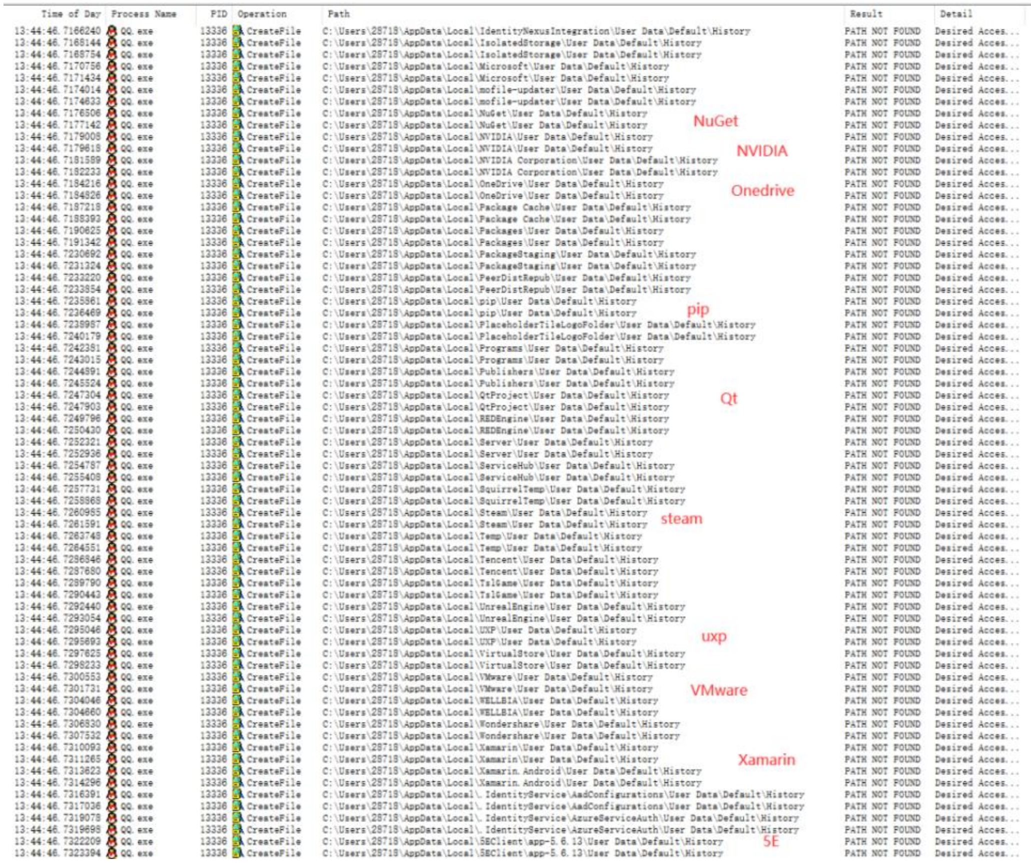
而且时间也是恰到好处的十分钟。



```
Time of Day       Process Name  PID    Operation        Path                                                                          Result
13:34:45.2837971  QQ.exe        13336  RegOpenKey       HKLM\System\CurrentControlSet\Services\GoogleChromeElevationService\Performance  NAME NOT FOUND
13:34:45.2838143  QQ.exe        13336  RegOpenKey       HKLM\System\CurrentControlSet\Services\GoogleChromeElevationService\Performance  NAME NOT FOUND
13:34:46.6409353  QQ.exe        2040   RegOpenKey       HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome  SUCCESS
13:34:46.6409530  QQ.exe        2040   RegCloseKey      HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome  SUCCESS
13:44:46.7439209  QQ.exe        13336  CreateFile       C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History          SUCCESS
13:44:46.7439430  QQ.exe        13336  CloseFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History          SUCCESS
13:44:46.7440420  QQ.exe        13336  CreateFile       C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History          SUCCESS
13:44:46.7440531  QQ.exe        13336  QueryBasicI...   C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History          SUCCESS
13:44:46.7440588  QQ.exe        13336  CloseFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History          SUCCESS
```

这是实锤了QQ和Chrome过不去啊，这我可不信！

把规则去掉，重新翻了一下才发现果然是冤枉QQ了啊。



```
Time of Day       Process Name  PID    Operation   Path                                                                                   Result          Detail
13:44:46.7166240  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\IdentityNexusIntegration\User Data\Default\History         PATH NOT FOUND  Desired Acces...
13:44:46.7168144  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\IsolatedStorage\User Data\Default\History                  PATH NOT FOUND  Desired Acces...
13:44:46.7168754  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\IsolatedStorage\User Data\Default\History                  PATH NOT FOUND  Desired Acces...
13:44:46.7170756  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Microsoft\User Data\Default\History                        PATH NOT FOUND  Desired Acces...
13:44:46.7171434  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Microsoft\User Data\Default\History                        PATH NOT FOUND  Desired Acces...
13:44:46.7174014  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\mofile-updater\User Data\Default\History                   PATH NOT FOUND  Desired Acces...
13:44:46.7174633  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\mofile-updater\User Data\Default\History                   PATH NOT FOUND  Desired Acces...
13:44:46.7176506  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\NuGet\User Data\Default\History                            PATH NOT FOUND  Desired Acces...
13:44:46.7177142  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\NuGet\User Data\Default\History                            PATH NOT FOUND  Desired Acces...
13:44:46.7179008  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\NVIDIA\User Data\Default\History                           PATH NOT FOUND  Desired Acces...
13:44:46.7179618  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\NVIDIA\User Data\Default\History                           PATH NOT FOUND  Desired Acces...
13:44:46.7181589  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\NVIDIA Corporation\User Data\Default\History               PATH NOT FOUND  Desired Acces...
13:44:46.7182233  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\NVIDIA Corporation\User Data\Default\History               PATH NOT FOUND  Desired Acces...
13:44:46.7184216  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\OneDrive\User Data\Default\History                         PATH NOT FOUND  Desired Acces...
13:44:46.7184526  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\OneDrive\User Data\Default\History                         PATH NOT FOUND  Desired Acces...
13:44:46.7187218  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Package Cache\User Data\Default\History                    PATH NOT FOUND  Desired Acces...
13:44:46.7188393  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Package Cache\User Data\Default\History                    PATH NOT FOUND  Desired Acces...
13:44:46.7190625  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Packages\User Data\Default\History                         PATH NOT FOUND  Desired Acces...
13:44:46.7191342  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Packages\User Data\Default\History                         PATH NOT FOUND  Desired Acces...
13:44:46.7230692  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\PackageStaging\User Data\Default\History                   PATH NOT FOUND  Desired Acces...
13:44:46.7231324  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\PackageStaging\User Data\Default\History                   PATH NOT FOUND  Desired Acces...
13:44:46.7233220  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\PeerDistRepub\User Data\Default\History                    PATH NOT FOUND  Desired Acces...
13:44:46.7233854  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\PeerDistRepub\User Data\Default\History                    PATH NOT FOUND  Desired Acces...
13:44:46.7235861  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\pip\User Data\Default\History                              PATH NOT FOUND  Desired Acces...
13:44:46.7236469  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\pip\User Data\Default\History                              PATH NOT FOUND  Desired Acces...
13:44:46.7238987  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\PlaceholderTileLogoFolder\User Data\Default\History        PATH NOT FOUND  Desired Acces...
13:44:46.7240179  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\PlaceholderTileLogoFolder\User Data\Default\History        PATH NOT FOUND  Desired Acces...
13:44:46.7242381  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Programs\User Data\Default\History                         PATH NOT FOUND  Desired Acces...
13:44:46.7243015  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Programs\User Data\Default\History                         PATH NOT FOUND  Desired Acces...
13:44:46.7244891  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Publishers\User Data\Default\History                       PATH NOT FOUND  Desired Acces...
13:44:46.7245524  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Publishers\User Data\Default\History                       PATH NOT FOUND  Desired Acces...
13:44:46.7247304  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\QtProject\User Data\Default\History                        PATH NOT FOUND  Desired Acces...
13:44:46.7247903  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\QtProject\User Data\Default\History                        PATH NOT FOUND  Desired Acces...
13:44:46.7249796  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\REDEngine\User Data\Default\History                        PATH NOT FOUND  Desired Acces...
13:44:46.7250430  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\REDEngine\User Data\Default\History                        PATH NOT FOUND  Desired Acces...
13:44:46.7252321  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Server\User Data\Default\History                           PATH NOT FOUND  Desired Acces...
13:44:46.7252936  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Server\User Data\Default\History                           PATH NOT FOUND  Desired Acces...
13:44:46.7254787  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\ServiceHub\User Data\Default\History                       PATH NOT FOUND  Desired Acces...
13:44:46.7255408  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\ServiceHub\User Data\Default\History                       PATH NOT FOUND  Desired Acces...
13:44:46.7257731  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\SquirrelTemp\User Data\Default\History                     PATH NOT FOUND  Desired Acces...
13:44:46.7258868  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\SquirrelTemp\User Data\Default\History                     PATH NOT FOUND  Desired Acces...
13:44:46.7260965  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Steam\User Data\Default\History                            PATH NOT FOUND  Desired Acces...
13:44:46.7261591  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Steam\User Data\Default\History                            PATH NOT FOUND  Desired Acces...
13:44:46.7263748  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Temp\User Data\Default\History                             PATH NOT FOUND  Desired Acces...
13:44:46.7264551  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Temp\User Data\Default\History                             PATH NOT FOUND  Desired Acces...
13:44:46.7286846  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Tencent\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7287680  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Tencent\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7289790  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\TslGame\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7290443  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\TslGame\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7292440  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\UnrealEngine\User Data\Default\History                     PATH NOT FOUND  Desired Acces...
13:44:46.7293054  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\UnrealEngine\User Data\Default\History                     PATH NOT FOUND  Desired Acces...
13:44:46.7295046  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\UXP\User Data\Default\History                              PATH NOT FOUND  Desired Acces...
13:44:46.7295693  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\UXP\User Data\Default\History                              PATH NOT FOUND  Desired Acces...
13:44:46.7297625  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\VirtualStore\User Data\Default\History                     PATH NOT FOUND  Desired Acces...
13:44:46.7298233  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\VirtualStore\User Data\Default\History                     PATH NOT FOUND  Desired Acces...
13:44:46.7300553  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\VMware\User Data\Default\History                           PATH NOT FOUND  Desired Acces...
13:44:46.7301731  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\VMware\User Data\Default\History                           PATH NOT FOUND  Desired Acces...
13:44:46.7304046  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\WELLBIA\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7304660  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\WELLBIA\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7306830  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Wondershare\User Data\Default\History                      PATH NOT FOUND  Desired Acces...
13:44:46.7307532  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Wondershare\User Data\Default\History                      PATH NOT FOUND  Desired Acces...
13:44:46.7310093  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Xamarin\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7311265  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Xamarin\User Data\Default\History                          PATH NOT FOUND  Desired Acces...
13:44:46.7313623  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Xamarin.Android\User Data\Default\History                  PATH NOT FOUND  Desired Acces...
13:44:46.7314296  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\Xamarin.Android\User Data\Default\History                  PATH NOT FOUND  Desired Acces...
13:44:46.7316391  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\.IdentityService\AadConfigurations\User Data\Default\History  PATH NOT FOUND  Desired Acces...
13:44:46.7317036  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\.IdentityService\AadConfigurations\User Data\Default\History  PATH NOT FOUND  Desired Acces...
13:44:46.7319078  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\.IdentityService\AzureServiceAuth\User Data\Default\History   PATH NOT FOUND  Desired Acces...
13:44:46.7319698  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\.IdentityService\AzureServiceAuth\User Data\Default\History   PATH NOT FOUND  Desired Acces...
13:44:46.7322209  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\5EClient\app-5.6.13\User Data\Default\History              PATH NOT FOUND  Desired Acces...
13:44:46.7323394  QQ.exe        13336  CreateFile  C:\Users\28718\AppData\Local\5EClient\app-5.6.13\User Data\Default\History              PATH NOT FOUND  Desired Acces...
```

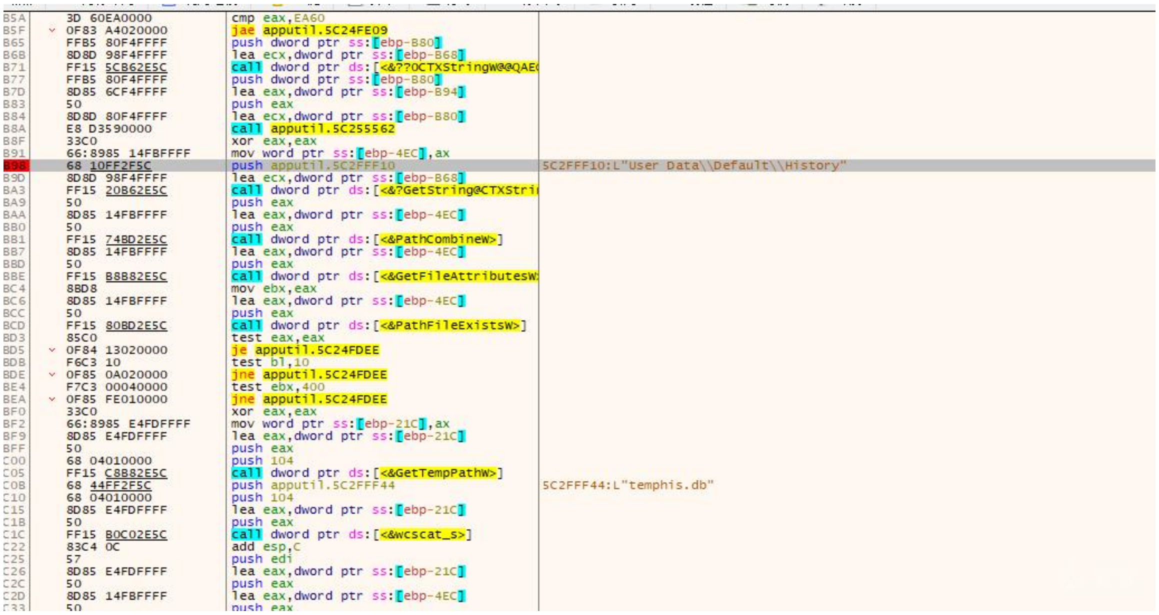
受害人之多令人震惊，仔细一看，这玩意是遍历了Appdata\Local\下的所有文件夹。

然后加上User Data\Default\History去读啊。

User Data\Default\History是谷歌系浏览器（火狐等浏览器不熟，不清楚目录如何）默认的历史纪录存放位置，Chrome中枪也就很正常了。

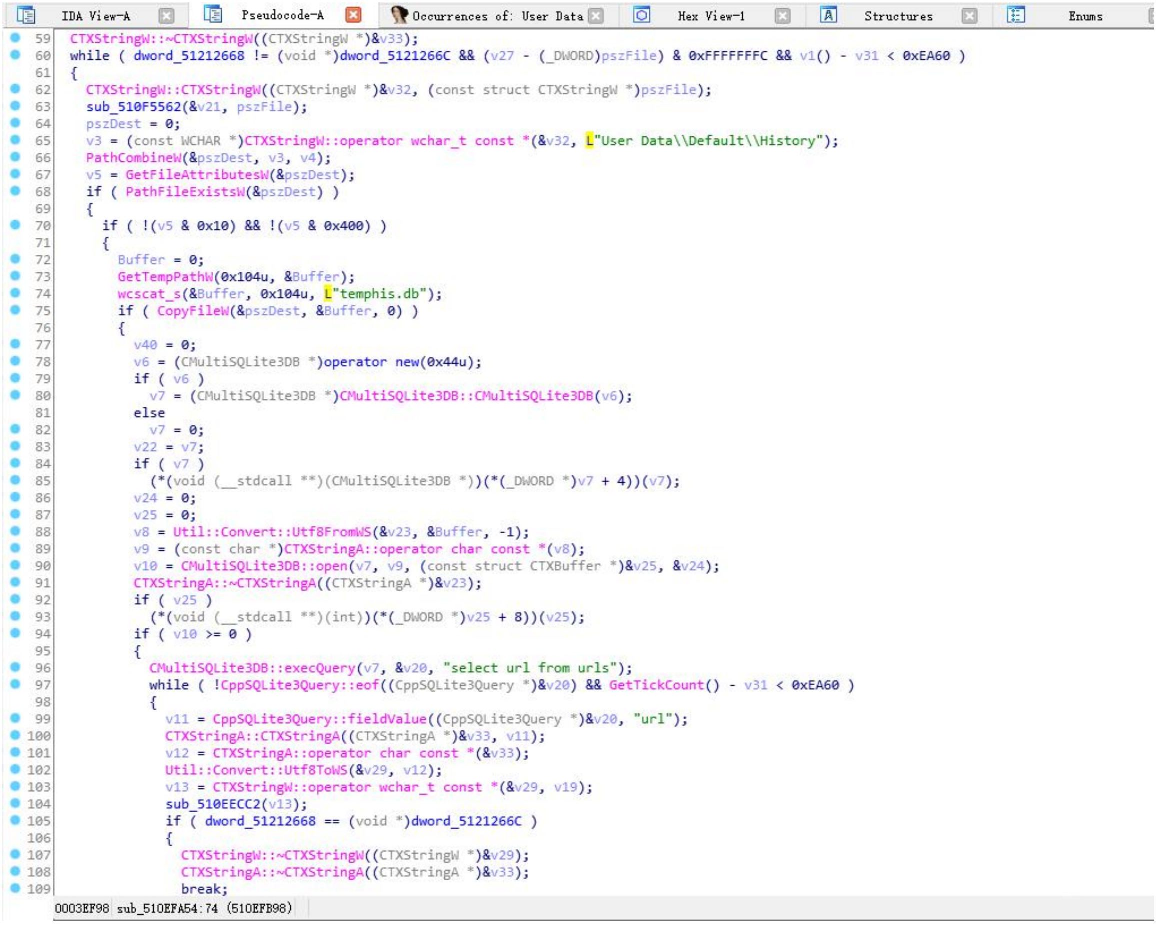
然后就该研究研究QQ为啥要这么干了，读取到的浏览器历史记录又拿来干啥了呢？

挂上x32dbg，动态调试找到位置。



```
B5A   3D 60EA0000         cmp eax,EA60
B5F   0F83 A4020000       jae apputil.5C24FE09
B65   FFB5 80F4FFFF       push dword ptr ss:[ebp-B80]
B6B   8D8D 98F4FFFF       lea ecx,dword ptr ss:[ebp-B68]
B71   FF15 5CB62E5C       call dword ptr ds:[<&??0CTXStringW@@QAE
B77   FFB5 80F4FFFF       push dword ptr ss:[ebp-B80]
B7D   8D85 6CF4FFFF       lea eax,dword ptr ss:[ebp-B94]
B83   50                  push eax
B84   8D8D 80F4FFFF       lea ecx,dword ptr ss:[ebp-B80]
B8A   E8 D3590000         call apputil.5C255562
B8F   33C0                xor eax,eax
B91   66:8985 14FBFFFF    mov word ptr ss:[ebp-4EC],ax
B98   68 10FF2F5C         push apputil.5C2FFF10          5C2FFF10:L"User Data\\Default\\History"
B9D   8D8D 98F4FFFF       lea ecx,dword ptr ss:[ebp-B68]
BA3   FF15 20B62E5C       call dword ptr ds:[<&?GetString@CTXStri
BA9   50                  push eax
BAA   8D85 14FBFFFF       lea eax,dword ptr ss:[ebp-4EC]
BB0   50                  push eax
BB1   FF15 74BD2E5C       call dword ptr ds:[<&PathCombineW>]
BB7   8D85 14FBFFFF       lea eax,dword ptr ss:[ebp-4EC]
BBD   50                  push eax
BBE   FF15 B8B82E5C       call dword ptr ds:[<&GetFileAttributesW
BC4   8BD8                mov ebx,eax
BC6   8D85 14FBFFFF       lea eax,dword ptr ss:[ebp-4EC]
BCC   50                  push eax
BCD   FF15 80BD2E5C       call dword ptr ds:[<&PathFileExistsW>]
BD3   85C0                test eax,eax
BD5   0F84 13020000       je apputil.5C24FDEE
BDB   F6C3 10             test bl,10
BDE   0F85 0A020000       jne apputil.5C24FDEE
BE4   F7C3 00040000       test ebx,400
BEA   0F85 FE010000       jne apputil.5C24FDEE
BF0   33C0                xor eax,eax
BF2   66:8985 E4FDFFFF    mov word ptr ss:[ebp-21C],ax
BF9   8D85 E4FDFFFF       lea eax,dword ptr ss:[ebp-21C]
BFF   50                  push eax
C00   68 04010000         push 104
C05   FF15 C8B82E5C       call dword ptr ds:[<&GetTempPathW>]
C0B   68 44FF2F5C         push apputil.5C2FFF44          5C2FFF44:L"temphis.db"
C10   68 04010000         push 104
C15   8D85 E4FDFFFF       lea eax,dword ptr ss:[ebp-21C]
C1B   50                  push eax
C1C   FF15 B0C02E5C       call dword ptr ds:[<&wcscat_s>]
C22   83C4 0C             add esp,C
C25   57                  push edi
C26   8D85 E4FDFFFF       lea eax,dword ptr ss:[ebp-21C]
C2C   50                  push eax
C2D   8D85 14FBFFFF       lea eax,dword ptr ss:[ebp-4EC]
C33   50                  push eax
```

然后去IDA里直接反编译出来，如下（位置在AppUtil.dll中.text:510EFB98 附近）

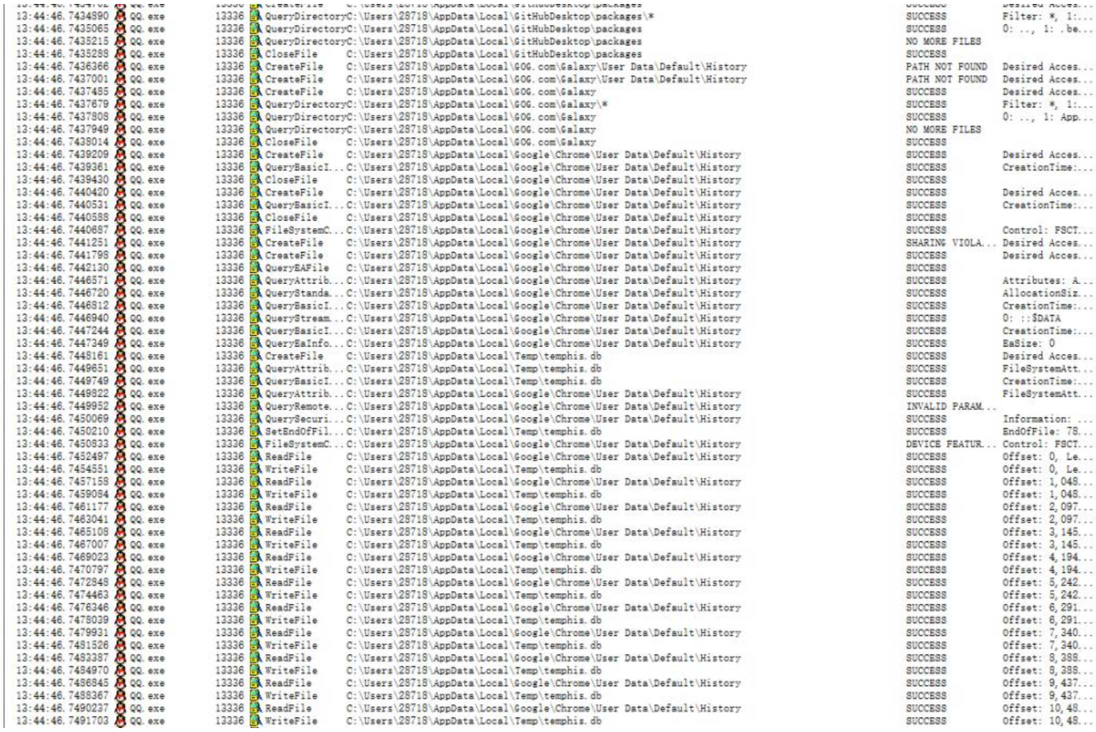

IDA View-A
Pseudocode-A
Occurrences of: User Data
Hex View-1
Structures
Enums
0003EF98 sub_510EFA54:74 (510EFB98)

```
CTXStringW::~CTXStringW((CTXStringW *)&v33);
while ( dword_51212668 != (void *)dword_5121266C && (v27 - (_DWORD)pszFile) & 0xFFFFFFFC && v1() - v31 < 0xEA60 )
{
  CTXStringW::CTXStringW((CTXStringW *)&v32, (const struct CTXStringW *)pszFile);
  sub_510F5562(&v21, pszFile);
  pszDest = 0;
  v3 = (const WCHAR *)CTXStringW::operator wchar_t const *(&v32, L"User Data\\Default\\History");
  PathCombineW(&pszDest, v3, v4);
  v5 = GetFileAttributesW(&pszDest);
  if ( PathFileExistsW(&pszDest) )
  {
    if ( !(v5 & 0x10) && !(v5 & 0x400) )
    {
      Buffer = 0;
      GetTempPathW(0x104u, &Buffer);
      wcscat_s(&Buffer, 0x104u, L"temphis.db");
      if ( CopyFileW(&pszDest, &Buffer, 0) )
      {
        v40 = 0;
        v6 = (CMultiSQLite3DB *)operator new(0x44u);
        if ( v6 )
          v7 = (CMultiSQLite3DB *)CMultiSQLite3DB::CMultiSQLite3DB(v6);
        else
          v7 = 0;
        v22 = v7;
        if ( v7 )
          (*(void (__stdcall **)(CMultiSQLite3DB *))(*(_DWORD *)v7 + 4))(v7);
        v24 = 0;
        v25 = 0;
        v8 = Util::Convert::Utf8FromWS(&v23, &Buffer, -1);
        v9 = (const char *)CTXStringA::operator char const *(v8);
        v10 = CMultiSQLite3DB::open(v7, v9, (const struct CTXBuffer *)&v25, &v24);
        CTXStringA::~CTXStringA((CTXStringA *)&v23);
        if ( v25 )
          (*(void (__stdcall **)(int))(*(_DWORD *)v25 + 8))(v25);
        if ( v10 >= 0 )
        {
          CMultiSQLite3DB::execQuery(v7, &v20, "select url from urls");
          while ( !CppSQLite3Query::eof((CppSQLite3Query *)&v20) && GetTickCount() - v31 < 0xEA60 )
          {
            v11 = CppSQLite3Query::fieldValue((CppSQLite3Query *)&v20, "url");
            CTXStringA::CTXStringA((CTXStringA *)&v33, v11);
            v12 = CTXStringA::operator char const *(&v33);
            Util::Convert::Utf8ToWS(&v29, v12);
            v13 = CTXStringW::operator wchar_t const *(&v29, v19);
            sub_510EECC2(v13);
            if ( dword_51212668 == (void *)dword_5121266C )
            {
              CTXStringW::~CTXStringW((CTXStringW *)&v29);
              CTXStringA::~CTXStringA((CTXStringA *)&v33);
              break;
```

这一段的逻辑还是很好看懂的，先读取各种User Data\Default\History文件。

读到了就复制到Temp目录下的temphis.db。

回去看下Procmom，果然没错。



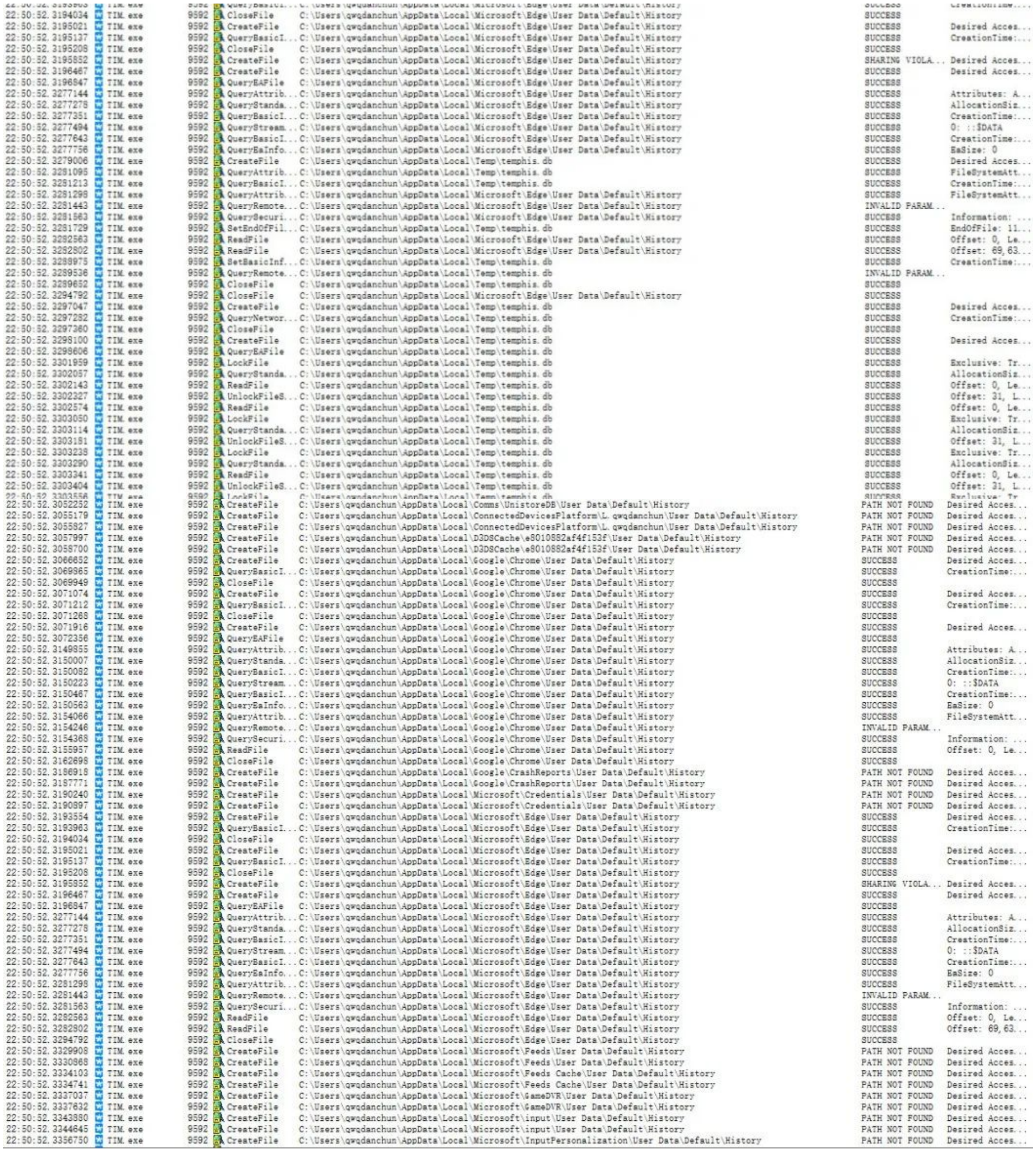
```
13:44:46.7434782  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\GitHubDesktop\packages                          SUCCESS           Desired Acces...
13:44:46.7434890  QQ.exe  13336  QueryDirectoryC:\Users\28718\AppData\Local\GitHubDesktop\packages\*                        SUCCESS           Filter: *, 1:...
13:44:46.7435065  QQ.exe  13336  QueryDirectoryC:\Users\28718\AppData\Local\GitHubDesktop\packages                          SUCCESS           0: .., 1: .be...
13:44:46.7435215  QQ.exe  13336  QueryDirectoryC:\Users\28718\AppData\Local\GitHubDesktop\packages                          NO MORE FILES
13:44:46.7435288  QQ.exe  13336  CloseFile       C:\Users\28718\AppData\Local\GitHubDesktop\packages                          SUCCESS
13:44:46.7436366  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\GOG.com\Galaxy\User Data\Default\History        PATH NOT FOUND    Desired Acces...
13:44:46.7437001  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\GOG.com\Galaxy\User Data\Default\History        PATH NOT FOUND    Desired Acces...
13:44:46.7437485  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\GOG.com\Galaxy                                  SUCCESS           Desired Acces...
13:44:46.7437679  QQ.exe  13336  QueryDirectoryC:\Users\28718\AppData\Local\GOG.com\Galaxy\*                                SUCCESS           Filter: *, 1:...
13:44:46.7437808  QQ.exe  13336  QueryDirectoryC:\Users\28718\AppData\Local\GOG.com\Galaxy                                  SUCCESS           0: .., 1: App...
13:44:46.7437949  QQ.exe  13336  QueryDirectoryC:\Users\28718\AppData\Local\GOG.com\Galaxy                                  NO MORE FILES
13:44:46.7438014  QQ.exe  13336  CloseFile       C:\Users\28718\AppData\Local\GOG.com\Galaxy                                  SUCCESS
13:44:46.7439209  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Desired Acces...
13:44:46.7439361  QQ.exe  13336  QueryBasicI...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           CreationTime:...
13:44:46.7439430  QQ.exe  13336  CloseFile       C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS
13:44:46.7440420  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Desired Acces...
13:44:46.7440531  QQ.exe  13336  QueryBasicI...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           CreationTime:...
13:44:46.7440588  QQ.exe  13336  CloseFile       C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS
13:44:46.7440687  QQ.exe  13336  FileSystemC...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Control: FSCT...
13:44:46.7441251  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SHARING VIOLA...  Desired Acces...
13:44:46.7441798  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Desired Acces...
13:44:46.7442130  QQ.exe  13336  QueryEAFile     C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS
13:44:46.7446571  QQ.exe  13336  QueryAttrib...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Attributes: A...
13:44:46.7446720  QQ.exe  13336  QueryStanda...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           AllocationSiz...
13:44:46.7446812  QQ.exe  13336  QueryBasicI...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           CreationTime:...
13:44:46.7446940  QQ.exe  13336  QueryStream...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           0: ::$DATA
13:44:46.7447244  QQ.exe  13336  QueryBasicI...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           CreationTime:...
13:44:46.7447349  QQ.exe  13336  QueryEaInfo...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           EaSize: 0
13:44:46.7448161  QQ.exe  13336  CreateFile      C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Desired Acces...
13:44:46.7449651  QQ.exe  13336  QueryAttrib...C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           FileSystemAtt...
13:44:46.7449749  QQ.exe  13336  QueryBasicI...C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           CreationTime:...
13:44:46.7449822  QQ.exe  13336  QueryAttrib...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           FileSystemAtt...
13:44:46.7449952  QQ.exe  13336  QueryRemote...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         INVALID PARAM...
13:44:46.7450069  QQ.exe  13336  QuerySecuri...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Information: ...
13:44:46.7450210  QQ.exe  13336  SetEndOfFil...C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           EndOfFile: 78...
13:44:46.7450833  QQ.exe  13336  FileSystemC...C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         DEVICE FEATUR...  Control: FSCT...
13:44:46.7452497  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 0, Le...
13:44:46.7454551  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 0, Le...
13:44:46.7457158  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 1,048...
13:44:46.7459084  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 1,048...
13:44:46.7461177  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 2,097...
13:44:46.7463041  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 2,097...
13:44:46.7465108  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 3,145...
13:44:46.7467007  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 3,145...
13:44:46.7469023  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 4,194...
13:44:46.7470797  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 4,194...
13:44:46.7472848  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 5,242...
13:44:46.7474463  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 5,242...
13:44:46.7476346  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 6,291...
13:44:46.7478039  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 6,291...
13:44:46.7479931  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 7,340...
13:44:46.7481526  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 7,340...
13:44:46.7483387  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 8,388...
13:44:46.7484970  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 8,388...
13:44:46.7486845  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 9,437...
13:44:46.7488367  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 9,437...
13:44:46.7490237  QQ.exe  13336  ReadFile        C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History         SUCCESS           Offset: 10,48...
13:44:46.7491703  QQ.exe  13336  WriteFile       C:\Users\28718\AppData\Local\Temp\temphis.db                                 SUCCESS           Offset: 10,48...
```

再之后的操作就简单了，SQLite读取数据库，然后“select url from urls”，这是在干什么大家都懂哈。

后面就不接着讲了，有兴趣的可以自己接着看。

结论，QQ并不是特意读取Chrome的历史记录的，而是会试图读取电脑里所有谷歌系浏览器的历史记录并提取链接，确认会中招的浏览器包括但不限于Chrome、Chromium、360极速、360安全、猎豹、2345等浏览器。

晚上来编辑一下，刚才去试了下TIM，果然经典重现，而且比QQ还离谱，不多说直接上图。

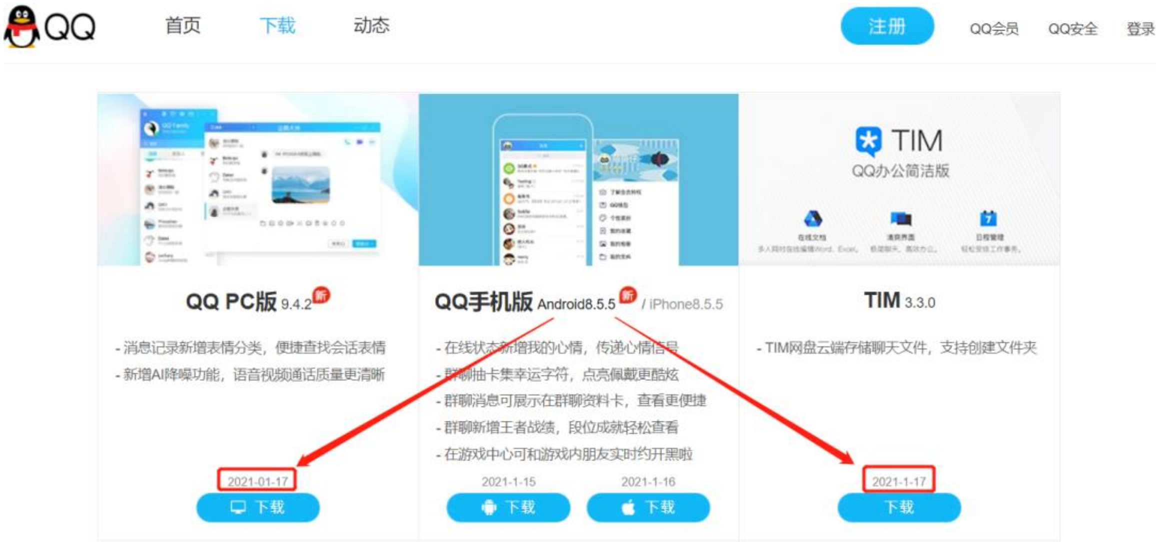


```
22:50:52.3193963  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3194034  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3195021  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Desired Acces...
22:50:52.3195137  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3195208  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3195852  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SHARING VIOLA...  Desired Acces...
22:50:52.3196467  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Desired Acces...
22:50:52.3196847  TIM.exe  9592  QueryEAFile    C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3277144  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Attributes: A...
22:50:52.3277278  TIM.exe  9592  QueryStanda... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           AllocationSiz...
22:50:52.3277351  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3277494  TIM.exe  9592  QueryStream... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           0: ::$DATA
22:50:52.3277643  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3277756  TIM.exe  9592  QueryEaInfo... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           EaSize: 0
22:50:52.3279006  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Desired Acces...
22:50:52.3281095  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           FileSystemAtt...
22:50:52.3281213  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           CreationTime:...
22:50:52.3281298  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           FileSystemAtt...
22:50:52.3281443  TIM.exe  9592  QueryRemote... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            INVALID PARAM...
22:50:52.3281563  TIM.exe  9592  QuerySecuri... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Information: ...
22:50:52.3281729  TIM.exe  9592  SetEndOfFil... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           EndOfFile: 11...
22:50:52.3282563  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Offset: 0, Le...
22:50:52.3282802  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Offset: 69,63...
22:50:52.3288975  TIM.exe  9592  SetBasicInf... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           CreationTime:...
22:50:52.3289536  TIM.exe  9592  QueryRemote... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     INVALID PARAM...
22:50:52.3289652  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS
22:50:52.3294792  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3297047  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Desired Acces...
22:50:52.3297282  TIM.exe  9592  QueryNetwor... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           CreationTime:...
22:50:52.3297360  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS
22:50:52.3298100  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Desired Acces...
22:50:52.3298606  TIM.exe  9592  QueryEAFile    C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS
22:50:52.3301959  TIM.exe  9592  LockFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Exclusive: Tr...
22:50:52.3302057  TIM.exe  9592  QueryStanda... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           AllocationSiz...
22:50:52.3302143  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Offset: 0, Le...
22:50:52.3302327  TIM.exe  9592  UnlockFileS... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Offset: 31, L...
22:50:52.3302574  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Offset: 0, Le...
22:50:52.3303050  TIM.exe  9592  LockFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Exclusive: Tr...
22:50:52.3303114  TIM.exe  9592  QueryStanda... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           AllocationSiz...
22:50:52.3303181  TIM.exe  9592  UnlockFileS... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Offset: 31, L...
22:50:52.3303238  TIM.exe  9592  LockFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Exclusive: Tr...
22:50:52.3303290  TIM.exe  9592  QueryStanda... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           AllocationSiz...
22:50:52.3303341  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Offset: 0, Le...
22:50:52.3303404  TIM.exe  9592  UnlockFileS... C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Offset: 31, L...
22:50:52.3303556  TIM.exe  9592  LockFile       C:\Users\qwqdanchun\AppData\Local\Temp\temphis.db                                                     SUCCESS           Exclusive: Tr...
22:50:52.3052252  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Comms\UnistoreDB\User Data\Default\History                          PATH NOT FOUND    Desired Acces...
22:50:52.3055179  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\ConnectedDevicesPlatform\L.qwqdanchun\User Data\Default\History    PATH NOT FOUND    Desired Acces...
22:50:52.3055827  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\ConnectedDevicesPlatform\L.qwqdanchun\User Data\Default\History    PATH NOT FOUND    Desired Acces...
22:50:52.3057997  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\D3DSCache\e8010882af4f153f\User Data\Default\History                PATH NOT FOUND    Desired Acces...
22:50:52.3058700  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\D3DSCache\e8010882af4f153f\User Data\Default\History                PATH NOT FOUND    Desired Acces...
22:50:52.3066652  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           Desired Acces...
22:50:52.3069865  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           CreationTime:...
22:50:52.3069949  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS
22:50:52.3071074  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           Desired Acces...
22:50:52.3071212  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           CreationTime:...
22:50:52.3071268  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS
22:50:52.3071916  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           Desired Acces...
22:50:52.3072356  TIM.exe  9592  QueryEAFile    C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS
22:50:52.3149855  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           Attributes: A...
22:50:52.3150007  TIM.exe  9592  QueryStanda... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           AllocationSiz...
22:50:52.3150082  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           CreationTime:...
22:50:52.3150223  TIM.exe  9592  QueryStream... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           0: ::$DATA
22:50:52.3150467  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           CreationTime:...
22:50:52.3150563  TIM.exe  9592  QueryEaInfo... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           EaSize: 0
22:50:52.3154066  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           FileSystemAtt...
22:50:52.3154246  TIM.exe  9592  QueryRemote... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             INVALID PARAM...
22:50:52.3154368  TIM.exe  9592  QuerySecuri... C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           Information: ...
22:50:52.3155957  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS           Offset: 0, Le...
22:50:52.3162698  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History                             SUCCESS
22:50:52.3186918  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Google\CrashReports\User Data\Default\History                       PATH NOT FOUND    Desired Acces...
22:50:52.3187771  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Google\CrashReports\User Data\Default\History                       PATH NOT FOUND    Desired Acces...
22:50:52.3190240  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Credentials\User Data\Default\History                     PATH NOT FOUND    Desired Acces...
22:50:52.3190897  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Credentials\User Data\Default\History                     PATH NOT FOUND    Desired Acces...
22:50:52.3193554  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Desired Acces...
22:50:52.3193963  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3194034  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3195021  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Desired Acces...
22:50:52.3195137  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3195208  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3195852  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SHARING VIOLA...  Desired Acces...
22:50:52.3196467  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Desired Acces...
22:50:52.3196847  TIM.exe  9592  QueryEAFile    C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3277144  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Attributes: A...
22:50:52.3277278  TIM.exe  9592  QueryStanda... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           AllocationSiz...
22:50:52.3277351  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3277494  TIM.exe  9592  QueryStream... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           0: ::$DATA
22:50:52.3277643  TIM.exe  9592  QueryBasicI... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           CreationTime:...
22:50:52.3277756  TIM.exe  9592  QueryEaInfo... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           EaSize: 0
22:50:52.3281298  TIM.exe  9592  QueryAttrib... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           FileSystemAtt...
22:50:52.3281443  TIM.exe  9592  QueryRemote... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            INVALID PARAM...
22:50:52.3281563  TIM.exe  9592  QuerySecuri... C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Information: ...
22:50:52.3282563  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Offset: 0, Le...
22:50:52.3282802  TIM.exe  9592  ReadFile       C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS           Offset: 69,63...
22:50:52.3294792  TIM.exe  9592  CloseFile      C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History                            SUCCESS
22:50:52.3329908  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Feeds\User Data\Default\History                           PATH NOT FOUND    Desired Acces...
22:50:52.3330868  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Feeds\User Data\Default\History                           PATH NOT FOUND    Desired Acces...
22:50:52.3334103  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Feeds Cache\User Data\Default\History                     PATH NOT FOUND    Desired Acces...
22:50:52.3334741  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\Feeds Cache\User Data\Default\History                     PATH NOT FOUND    Desired Acces...
22:50:52.3337037  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\GameDVR\User Data\Default\History                         PATH NOT FOUND    Desired Acces...
22:50:52.3337632  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\GameDVR\User Data\Default\History                         PATH NOT FOUND    Desired Acces...
22:50:52.3343880  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\input\User Data\Default\History                           PATH NOT FOUND    Desired Acces...
22:50:52.3344645  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\input\User Data\Default\History                           PATH NOT FOUND    Desired Acces...
22:50:52.3356750  TIM.exe  9592  CreateFile     C:\Users\qwqdanchun\AppData\Local\Microsoft\InputPersonalization\User Data\Default\History            PATH NOT FOUND    Desired Acces...
```

上文部分素材来源看雪论坛，作者qwqdanchun，原帖地址如下：

https://bbs.pediy.com/thread-265359.htm

QQ和Tim客户端已于2021年1月17日更新 👍



QQ PC版 9.4.2 新

- 消息记录新增表情分类，便捷查找会话表情
- 新增AI降噪功能，语音视频通话质量更清晰

2021-01-17

QQ手机版 Android8.5.5 新 / iPhone8.5.5

- 在线状态新增我的心情，传递心情信号
- 群聊抽卡集幸运字符，点亮佩戴更酷炫
- 群聊消息可展示在群聊资料卡，查看更便捷
- 群聊新增王者战绩，段位成就轻松查看
- 在游戏中心可和游戏内朋友实时约开黑啦

2021-1-15　2021-1-16

TIM 3.3.0

- TIM网盘云端存储聊天文件，支持创建文件夹

2021-1-17

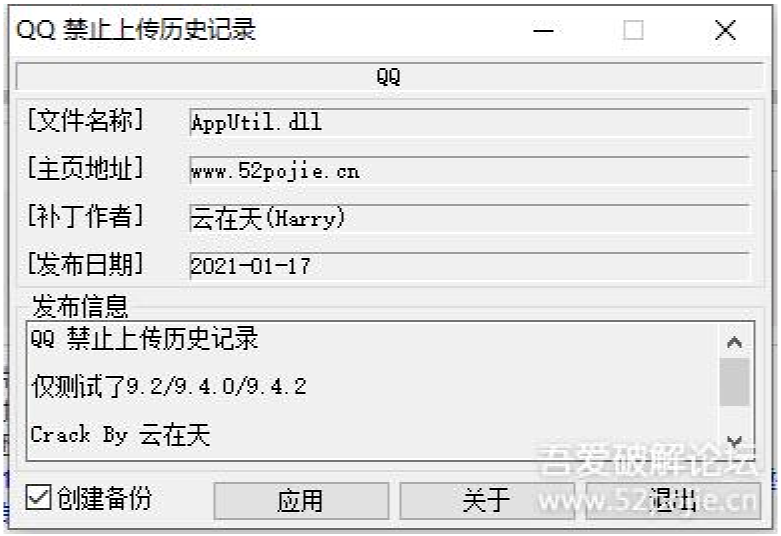
对于QQ读取用户历史浏览记录的问题，有小伙伴说这个好办，只需把文件夹设成只读或者用无痕模式浏览网页就可以了。

莫理觉得这真有点因噎废食了，到底是谁绑架了你？况且我们不会因为它的某些行为就不再用它，除非 🙄

唉，还是躺平接受吧，没有竞争无须挣扎。要反抗，就去 Tg。

火绒官方通告 ☞ 点我跳转，可以看看他们下面的留言，贼有趣 😼

解决办法



QQ 禁止上传历史记录

QQ

[文件名称] AppUtil.dll

[主页地址] www.52pojie.cn

[补丁作者] 云在天(Harry)

[发布日期] 2021-01-17

发布信息

QQ 禁止上传历史记录

仅测试了9.2/9.4.0/9.4.2

Crack By 云在天

☑创建备份

吾爱版主云在天今日编写了一款QQ禁止上传浏览器记录的软件，只适用于QQ9.0以后的版本。

软件地址：

https://www.52pojie.cn/forum.php?mod=viewthread&tid=1353110

歌事故里

薛之谦《一半》

由网友“□”点歌

视频来源：腾讯视频

可能喜欢

一个由刑警组织联合创办的网站！

真以为靠手速抢到茅台吗？

逆天的开源神器，简直不要太方便！

找到了！！四年前的版本用着才最爽！

鹅厂两款良心听歌神器，共享曲库版权！

两款珍藏好久的神器，安卓苹果都有！

到底了，顺手打个卡趴