

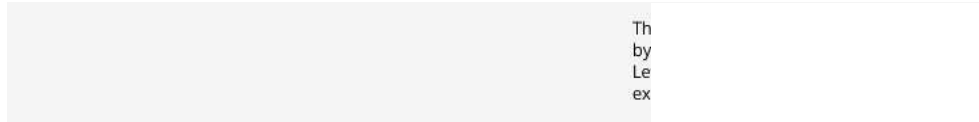
首页 - 文章 - 安全资讯, 科技资讯 - 正文

腾讯QQ/TIM被爆监控用户历史记录 涉及谷歌/微软/360/猎豹等多款浏览器



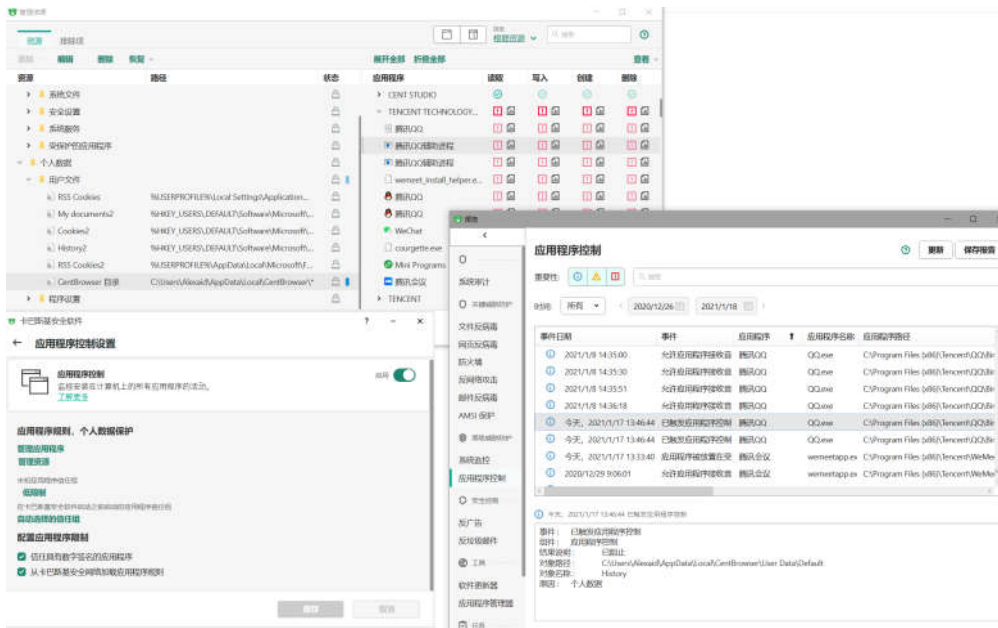
山外的鸭子哥 安全资讯, 科技资讯 2021年1月17日 19:58:48

0 0



据V2EX网友爆料腾讯QQ登录后被火绒高级防护拦截，用户配置的自定义拦截规则发现腾讯QQ读取浏览器位置。这里的浏览器位置指的是谷歌等浏览器数据存储位置，更具体来说腾讯相关进程是直接读取浏览器历史记录目录。例如谷歌浏览器数据目录：C:\Users\用户名称\AppData\Local\Google\Chrome\User Data\Default\History

经过多名网友测试和验证确定腾讯QQ以及腾讯TIM均有上述行为，而且读取的也不仅仅是谷歌浏览器历史记录。实际上任何 Chromium 内核浏览器例如微软、360、2345等浏览器均会被读取，但腾讯为何收集用户历史记录？



Trade with a broker with integrity

OANDA

This advertisement has not been the Monetary Authority of Singapore. Leveraged trading is high risk. Loss may exceed deposits.

不怕蓝屏不怕挂! Windows 备份和还原(SiB)介绍

百度网盘突然良心了? 不开会员下载速度也能

微信解释为何撤回原因还真得每

阿里云 teambition 网盘 内测体验 不限速 高速下载 点击申请公测

This advertisement has not been the Monetary Authority of Singapore. Leveraged trading is high risk. Loss may exceed deposits.

本月热读

本地 HEU_KMS 系统工具, 车

HEU KMS Activator™

微软 Windows 其他软件, 车




Official Site

目前发现的关键词包括：古着(即古装)、VINTAGE(老式)、融券、融资、炒股、股票，腾讯似乎会收集这些记录。
而涉及的网站主要是淘宝、天猫和京东，即用户在上述网站搜索过类似关键词，则腾讯会将其上报到腾讯服务器。

```

1 import json
2 import hashlib
3 import struct
4 import sys
5 import urllib.parse
6
7 tasks = {
8     # hard-code
9     # (23, 0x1C6389BA, 0xF2FA5666, 0xF2A2E0D3, 0xC892E7BA): b'', # ://S_TAobao.COM/SEARCH?
10    # (34, 0xB829484C, 0x520F7CC3, 0x94EC8A73, 0xD808E79): b'', # LIST_Tmall.COM/SEARCH_PRODUCT.HTM?
11    # (30, 0xDDA1029, 0x9E67F3BB, 0xB18ACC45, 0x597CF438): b'', #
12    # (21, 0x2564591C, 0x5B11347B, 0x846A0F72, 0xEF704A8): b'', # SEARCH.JD.COM/SEARCH?
13
14    # put on list
15    # (18, 0x8C2F8C3B, 0x9CA6DB69, 0x663C9537, 0xA0B64B58): b'', # 古着
16    # (7, 0x966DC59E, 0x592F2331, 0x6D2BF021, 0xA1D96C3C): b'', # VINTAGE
17    # (18, 0x7FACF63C, 0xBEC2FCB0, 0xBE8836F6, 0x167CC273): b'', # 融券
18    # (18, 0x4686D8D7, 0x8AA82723, 0xBE19FA24, 0x670E160C): b'', # 融资
19    # (18, 0xE235F85E, 0x5C924D20, 0xA61884AC, 0x4BC792DD): b'', # 炒股
20    # (18, 0x790888BEC, 0xF29CC9E8, 0xBF920D9, 0x455AE9ED): b'', # 股票
21 }
22
23 result = {}
24
25 for task in tasks:
26     _, a, b, c, d, = task
27     tasks[task] = struct.pack(b'<LLLL',
28                               a & 0xffffffff,
29                               b & 0xffffffff,
30                               c & 0xffffffff,
31                               d & 0xffffffff)
32

```

-  H3C 推出 5400M 硬件设备, 系统
-  微软修 Defender Microsoft
-  黑客泄露疫苗数据 主安全资讯, 系统

以下是看雪论坛网友原帖截图：

[调试逆向] [原创]关于QQ读取Chrome历史记录澄清

 qwqdanchun 





极客 

18小时前

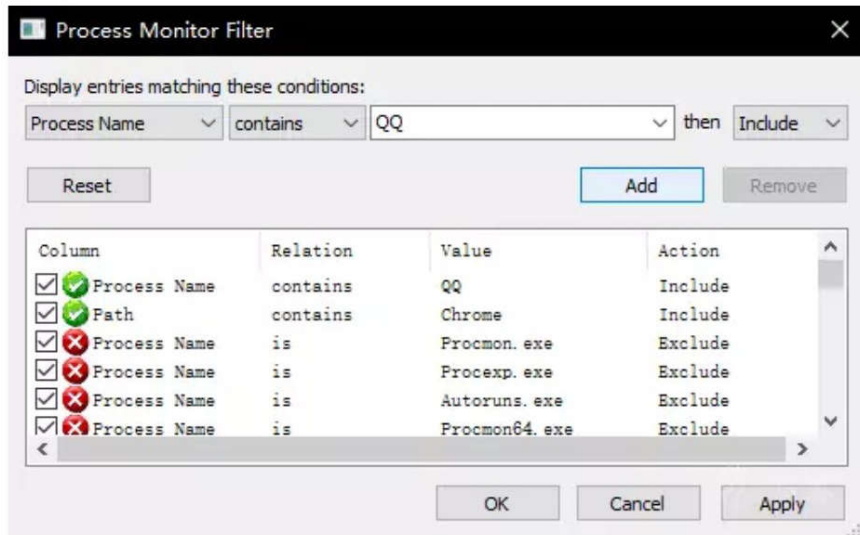
 11360

今天看到群里有同学发了一篇v2ex上的帖子

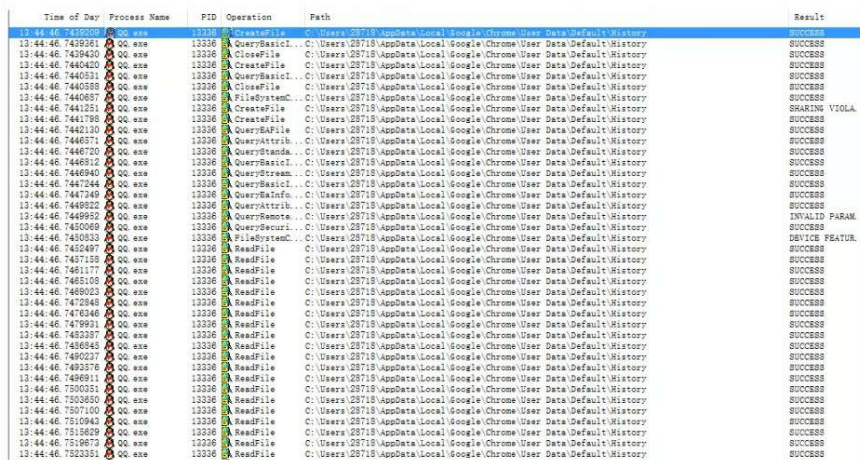
(<https://www.v2ex.com/t/745030>)，
说QQ会读取Chrome的历史记录，被火绒自定义规则拦截了，本来我是不信的，但
且他道他有现了。而且是QQ登录10分钟

- 
- 
- 
- 

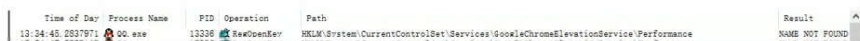
这我就想去验证下了，开虚拟机装QQ、Chrome，然后打开Process Monitor开始等。规则简单的过滤下。

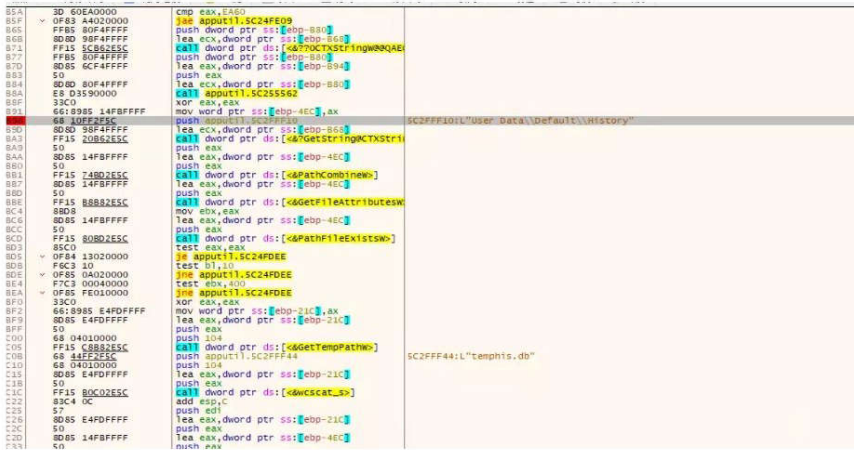


果然看到了读取AppData\Local\Google\Chrome\User Data\Default\History等目录的操作。

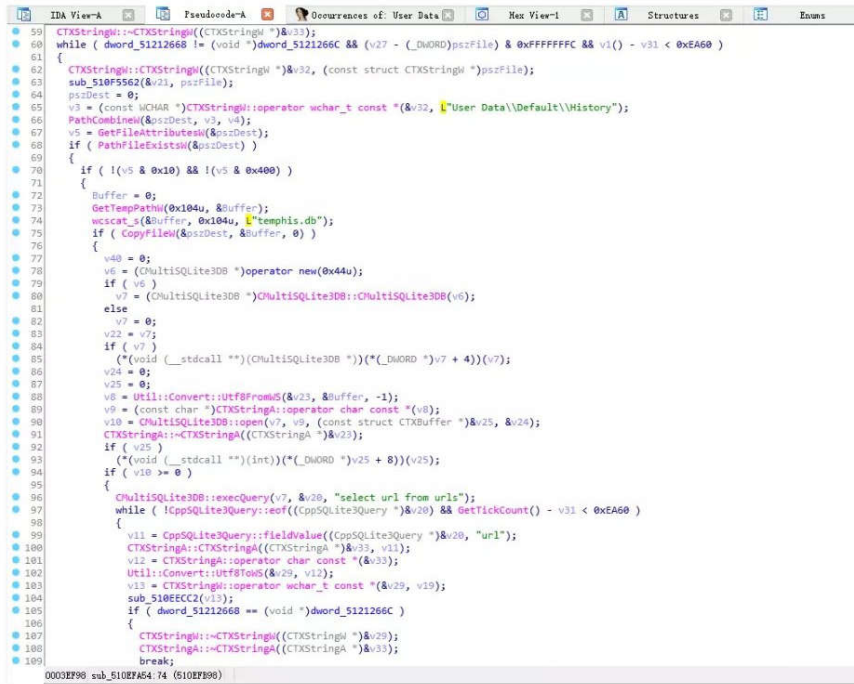


而且时间也是恰到好处的十分钟。





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



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。

Time	Process	Operation	Path	Result
13:44:40	qq.exe	QueryDirectory	C:\Users\28718\AppData\Local\Google\Desktop\package*	SUCCESS
13:44:40	qq.exe	QueryDirectory	C:\Users\28718\AppData\Local\Google\Desktop\package*	SUCCESS
13:44:40	qq.exe	CloseFile	C:\Users\28718\AppData\Local\Google\Desktop\package*	SUCCESS
13:44:40	qq.exe	CreateFile	C:\Users\28718\AppData\Local\Google\Default\History	PATH NOT FOUND
13:44:40	qq.exe	CreateFile	C:\Users\28718\AppData\Local\Google\Default\History	Desired Access...
13:44:40	qq.exe	QueryDirectory	C:\Users\28718\AppData\Local\Google\Default\History	SUCCESS
13:44:40	qq.exe	QueryDirectory	C:\Users\28718\AppData\Local\Google\Default\History	SUCCESS
13:44:40	qq.exe	CloseFile	C:\Users\28718\AppData\Local\Google\Default\History	SUCCESS
13:44:40	qq.exe	CreateFile	C:\Users\28718\AppData\Local\Google\Default\History	Desired Access...

Table with columns for timestamp, process name, path, and status. The table lists system events for various applications like QQ and TIM, including file operations and network connections.

安卓应用层抓包通杀脚本发布！《高研班》2021年3月班开始招生！

最后于 12小时前 被qwqdanchun编辑，原因：补充TIM

QQ(208) TIM(19) 历史记录(5) 安全隐私(8) 监控(8) 腾讯(419)

本文来自蓝点网综合，由山外的鸭子哥整理编辑，其版权均为蓝点网综合所有，文章内容系作者个人观点，不代表蓝点网对观点赞同或支持。如需转载，请注明文章来源。

分享: [Social sharing icons]

赞 0

上一篇: 微软更新Windows 10语音控制隐私政策 不再强...



发表评论



首页

科技资讯

软件资讯

Windows 10

技术教程

软件工具

正版软件

网址导航

Empty comment box

昵称 (必填)

邮箱 (必填)

网址

发表评论

首页 版权声明 侵权联系 商务合作 留言反馈 网址导航 友情链接 微信公众号 官方微博 网站地图

蓝点网使用Google QUIC传输层网络协议为您呈现精彩内容 ©2012 - 2020 蓝点网 版权所有 浙ICP备14021835号-1 合作伙伴: 正版软件商城 亚洲诚信

