

科技资讯 ~

软件资讯

Windows 10

技术教程、

软件工具 ~

正版软件

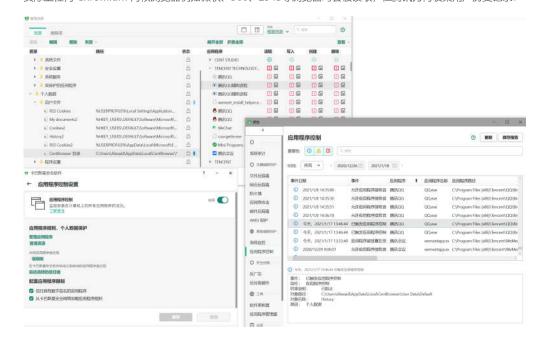
网址导航

膏 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



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Q Q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



This advertisement has not beer the Monetary Authority of Singa Leveraged trading is high risk. L exceed deposits.

不怕蓝屏不怕挂! Window 备份和还原(SiB)介绍和





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 beer the Monetary Authority of Singa Leveraged trading is h exceed deposits.

> > 繁

本月热读





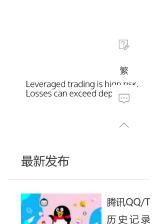


目前验证此问题最简单的方法就是安装火绒安全然后配置自定义拦截规则,随后登录QQ/TIM即可看到拦截提示。 火绒安全本身并没有尝试对腾讯系列软件进行高级拦截,不过火绒论坛提供类似规则可以帮助用户进行访问拦截。 同时用户亦可使用进程管理软件例如火绒安全附带的火绒剑,利用火绒剑进行监视时也可以发现腾讯的定时访问。 理论上说只要用户使用谷歌系列内核浏览器就会被腾讯窃取历史记录,即用户访问的某些网站会被腾讯悄悄收集。 浏览器历史记录对用户来说是极其私密的内容,因为通过访问记录可以分辨用户喜好甚至窥探用户的隐私信息等。 至于腾讯为何要未经用户同意私自收集用户的历史记录暂时还不清楚,而腾讯官方目前尚未就此事发布任何回应。 注:微软商店版的腾讯QQ虽然没有安装 Q盾 但也会读取用户历史记录,所以使用商店版不能规避隐私泄露问题。

#### 推荐用户配置规则进行拦截:

点击这里下载安装火绒安全软件,安装完成后点击右上角菜单转到安全设置页面,然后点击左侧的高级防护选项。 在高级防护选项里点击自定义防护然后点击底部的导入规则,点击这里下载规则然后通过导入选项进行导入即可。 导入完成后火绒将自动拦截腾讯 QQ或腾讯 TIM尝试读取浏览器数据目录行为,如果拦截用户也会看到火绒提醒。

#### 腾讯似乎监控投资类关键词:



安全资讯。利



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

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。



H3C 推 出 5400M鲸[ 硬件设备, 雨

微软修





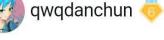


黑客泄露丝 苗数据 主 安全资讯,科

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 历史记录的澄清









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

旦州沿州与刊フ

五日旦00癸丑10公钟



科技资讯 ~

软件资讯

Windows 10

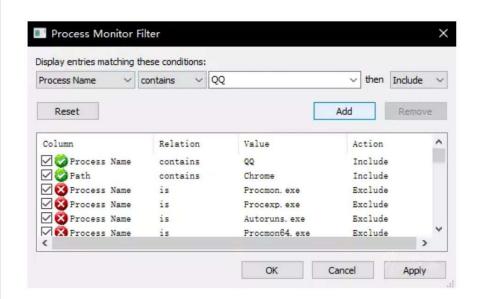
技术教程~

软件工具 ~

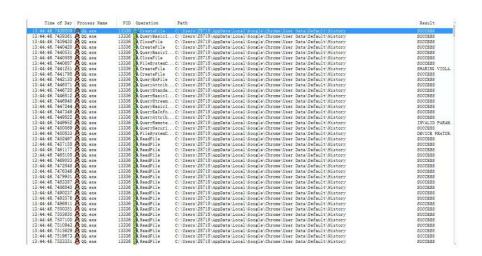
正版软件

网址导航

这我就想去验证下了,开虚拟机装QQ、C hrome,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\Chinome\User Data\Default\History等目录的操作。



而且时间也是恰到好处的十分钟。





爲首页

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

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。



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,C hrome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x32dbq,动态调试找到位置。



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

```
Lall doord 1.502.55587

Or 8b.eb. 20

Or 8b.
                                  33C0
66:8985 14F8FFF
68 10FF2F5C
80:80 98F4FFF
FF15 20B62E5C
50
80:85 14F8FFFF
50
FF15 74B02E5C
80:85 14F8FFFF
jne apputil.SC24FDEE
xor eax,eax
mov word ptr ss:[ebp-210],ax
lea eax,dword ptr ss:[ebp-210]
                                                                                                                                                                                                                                                                                                                                          push eax

push 104

[all dword ptr ds:[cdgettempPath

push apput1].5C2FFF44

push 104

lea eax,dword ptr ss:[ebp-210]

push eax

[all dword ptr ds:[cdwcscat_s>]

add esp,c

push edd dword ptr ss:[ebp-210]
                                  8085 E4FDFFFF
50
FF15 80C02E5C
83C4 0C
57
8085 E4FDFFFF
50
8D85 14FBFFFF
```

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

```
DIA View-A DE Passdoord-A Decorations of: User Date Decoration Decorations of: User Date Decoration Decoration
                                         CTXStringW::CTXStringW((CTXStringW *)&v32, (const struct CTXStringW *)pszFile); sub_510F5562(&v21, pszFile);
                                   sub_510F5562(&v21, psrFile);
pszDest = 0;
v3 = (const UCMAR *)CTXStringMr:oper
PathCombineN(&pszDest, v3, v4);
v5 = GetFileAttributesN(&pszDest);
if ( PathFileExistsN(&pszDest))
{

                                                                                                                                                                                                          rator wchar_t const "(&v32, L"User Data\\Default\\History");
                                           if ( !(v5 & 0x10) && !(v5 & 0x400) )
{
                                                          Buffer = 0;

GetTempPathw(@x104u, &Buffer);

wcscat_s(&Buffer, 0x104u, E^remphis.db");

if ( CopyFileW(&pszDest, &Buffer, 0) );

{w40 = 0;

w6 = (fwlltiSOLite3DB ")operator new(0x
                                                              v6 = (CMultisQLite3D8 *)operatur
if ( v6 )
v7 = (CMultisQLite3D8 *)CMultisQLite3D8::CMultisQLite3D8(v6);
                                                                if (v)
(*void (_stdcall **)(CMultiSQLite30B *))(*(_DMORD *)v7 + 4))(v7);
v24 = 0;
v25 = 0;
v8 = vtil::Convert::utf8FromMS(&v23, &ouffer, -1);
v8 = (const char *)CTNStringA::operator char const *(v8);
v19 = CfultiSQLite20B::open(v7, v9) (const struct CTNSuffer *)&v25, &v24);
cTNStringA::mCTNStringA(*CTNStringA*, 8v22);
if (void (_stdcall **)(int))(*(_DMORD *)v25 + 8))(v25);
if (vid >= 0)
CNNLItSQLite20B::execQuery(v7, &v26, "select url from urls");
                                                                                                                 (_stdcall **)(CMultiSQLite3DB *))(*(_DWORD *)v7 + 4))(v7);
                                                                            CMultiSQLite3D8::execQuery(v7, &v20, "select url from urls"); while ( !CppSQLite3Query::eof((CppSQLite3Query *)&v20) && GetTickCount() - v31 < 0xEA60 )
                                                                                   vii = CppSQLite3Query::fleldValue((CppSQLite3Query ")&v20, "url");
CTXStringA::CTXStringA((CTXStringA ")&v33, vii);
vii = CTXStringA::operato char const "(&v33);
Util::Convert::Utf6Tols(&v29, vi2);
vii = CTXStringB::operato wchar_t const "(&v29, vi9);
                                                                                        sub_510EECC2(v13);
if ( dword_51212668 == (void *)dword_5121266C )
                                                                                      {
    CTXStringW::~CTXStringW((CTXStringW *)&v29);
    CTXStringA::~CTXStringA((CTXStringA *)&v33);
```

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。



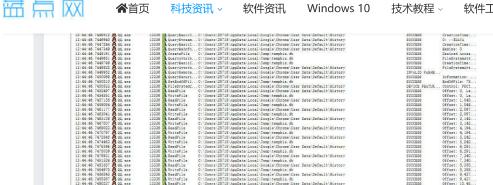
爲首页

科技资讯 >

Windows 10 技术教程 v 软件工具 v

正版软件

网址导航



软件资讯

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、Chr omium、360极速、360安全、猎豹、234 5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。



屈鼠図

☆首页

科技资讯 ~

技术教程、

软件工具 ~

正版软件

网址导航



软件资讯

Windows 10

# 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)

本文来源 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: 💊 f 🔰 💰

上一篇:微软更新Windows 10语音控制隐私政策 不再强...



发表评论

ď	田豆豆	爲首页	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
	昵称 (必填)			曲	『箱(必填)				
	网址								
	发表评论								

首页 版权声明 侵删联系 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

?