



[调试逆向] [原创]关于QQ读取Chrome历史记录的澄清

qwqdanchun

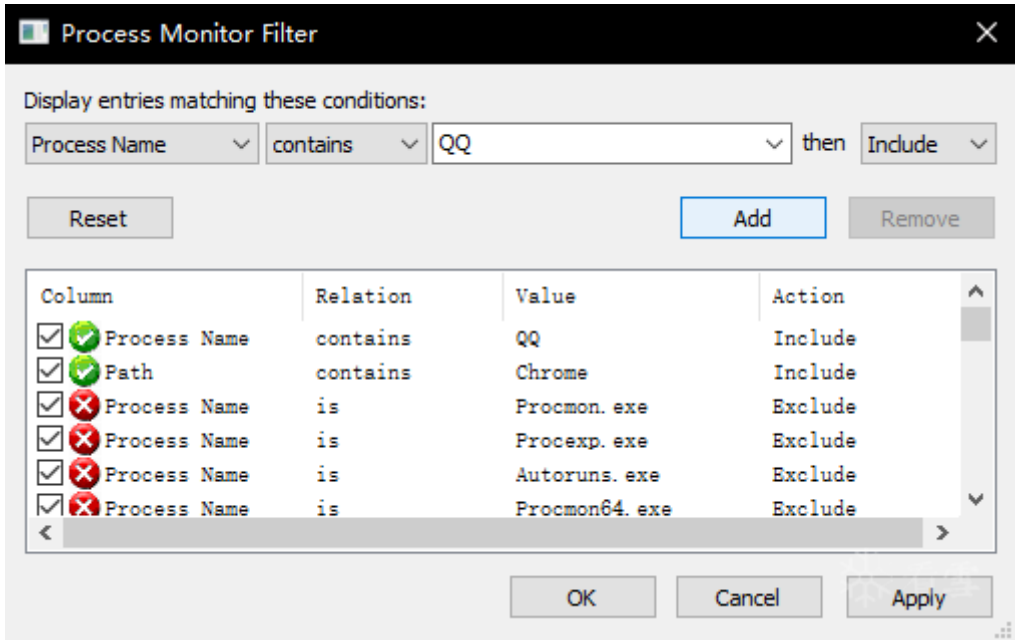
极客

19小时前

16769

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，但是他说他复现了，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。



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

Time of Day	Process Name	PID	Operation	Path	Result
13:44:46.7439208	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	QueryEAFil...	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
13:34:46.6409423	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
13:44:46.7439208	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

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



首页

论坛

课程

招聘

发现

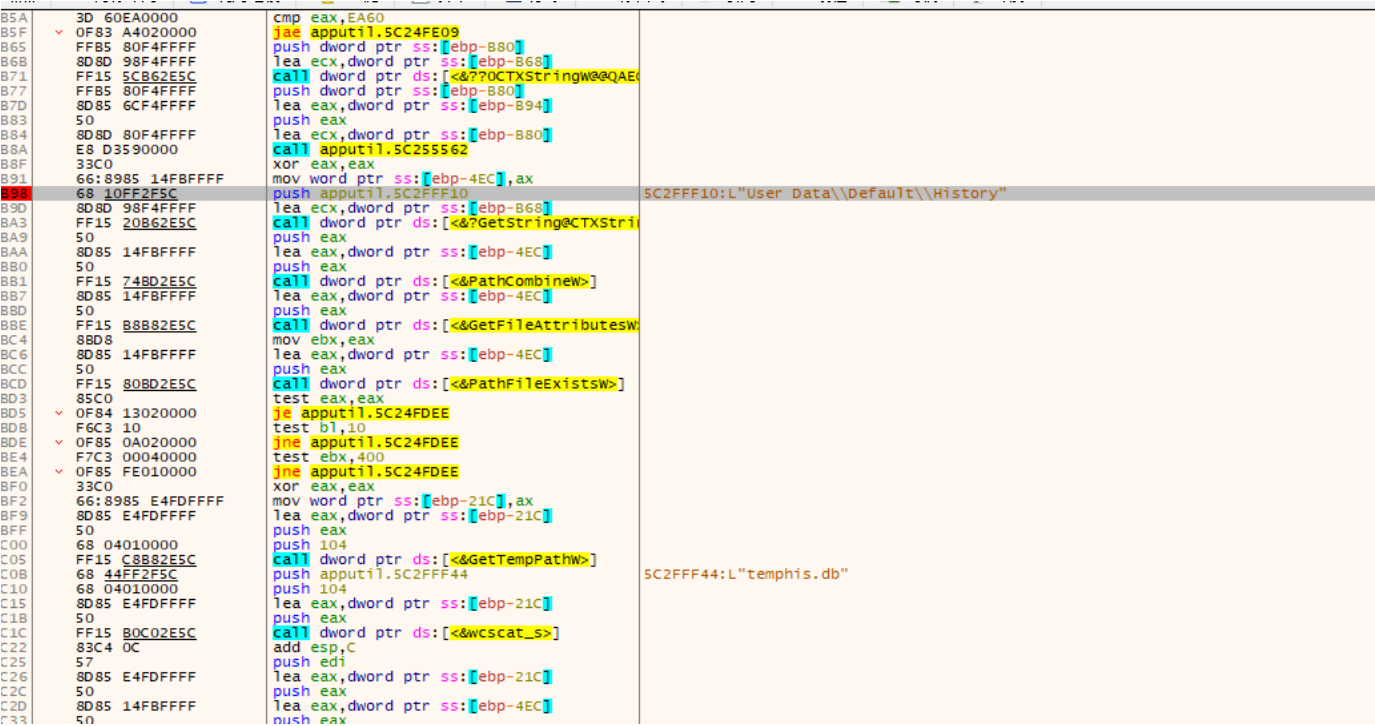


Time of Day	Process Name	PID	Operation	Path	Result	Detail
13:44:46.7168240	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\IdentityNexusIntegration\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7168344	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\IsolatedStorage\User 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\profile-updater\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7174633	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\profile-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...
13:44:46.7179003	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\NVIDIA\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7179818	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...
13:44:46.7182223	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...
13:44:46.7184926	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\Package Cache\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7191342	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\Package Cache\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...
13:44:46.7233554	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\PeerDistRepub\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7233561	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...
13:44:46.7244691	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...
13:44:46.7247304	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...
13:44:46.7258661	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\SquirrelTemp\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7260985	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...
13:44:46.7268846	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...
13:44:46.7288790	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...
13:44:46.7293046	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\UNP\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7295693	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\UNP\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...
13:44:46.7311261	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\Xamarin\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7313823	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\AdConfigurations\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7317036	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\IdentityService\AdConfigurations\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7319075	qq.exe	13336	CreateFile	C:\Users\28718\AppData\Local\IdentityService\AzureServiceAuth\User Data\Default\History	PATH NOT FOUND	Desired Acces...
13:44:46.7319689	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\SBClient\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\SBClient\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。



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
59 CTXStringW::~CTXStringW((CTXStringW *)&v33);
60 while ( dword_51212668 != (void *)dword_5121266C && (v27 - (_DWORD)pszFile) & 0xFFFFFFFF && v1() - v31 < 0xEA60 )
61 {
62     CTXStringW::CTXStringW((CTXStringW *)&v32, (const struct CTXStringW *)pszFile);
63     sub_510F5562(&v21, pszFile);
64     pszDest = 0;
65     v3 = (const WCHAR *)CTXStringW::operator wchar_t const *(&v32, L"User Data\\Default\\History");
66     PathCombineW(&pszDest, v3, v4);
67     v5 = GetFileAttributesW(&pszDest);
68     if ( PathFileExistsW(&pszDest) )
69     {
70         if ( !(v5 & 0x10) && !(v5 & 0x400) )
71         {
72             Buffer = 0;
73             GetTempPathW(0x104u, &Buffer);
74             wscat_s(&Buffer, 0x104u, L"temphis.db");
75             if ( CopyFileW(&pszDest, &Buffer, 0) )
76             {
77                 v40 = 0;
78                 v6 = (CMultiSQLite3DB *)operator new(0x44u);
79                 if ( v6 )
80                     v7 = (CMultiSQLite3DB *)CMultiSQLite3DB::CMultiSQLite3DB(v6);
81                 else
82                     v7 = 0;
83                 v22 = v7;
84                 if ( v7 )
85                     (*(void (__stdcall **)(CMultiSQLite3DB *)))(*(__DWORD *)v7 + 4)(v7);
86                 v24 = 0;
87                 v25 = 0;
88                 v8 = Util::Convert::Utf8FromW5(&v23, &Buffer, -1);
89                 v9 = (const char *)CTXStringA::operator char const *(&v8);
90                 v10 = CMultiSQLite3DB::open(v7, v9, (const struct CTXBuffer *)&v25, &v24);
91                 CTXStringA::~CTXStringA((CTXStringA *)&v23);
92                 if ( v25 )
93                     (*(void (__stdcall **)(int)))(*(__DWORD *)v25 + 8)(v25);
94                 if ( v10 >= 0 )
95                 {
96                     CMultiSQLite3DB::execQuery(v7, &v20, "select url from urls");
97                     while ( !CppSQLite3Query::eof((CppSQLite3Query *)&v20) && GetTickCount() - v31 < 0xEA60 )
98                     {
99                         v11 = CppSQLite3Query::fieldValue((CppSQLite3Query *)&v20, "url");
100                         CTXStringA::CTXStringA((CTXStringA *)&v33, v11);
101                         v12 = CTXStringA::operator char const *(&v33);
102                         Util::Convert::Utf8ToW5(&v29, v12);
103                         v13 = CTXStringW::operator wchar_t const *(&v29, v19);
104                         sub_510EECC2(v13);
105                         if ( dword_51212668 == (void *)dword_5121266C )
106                         {
107                             CTXStringW::~CTXStringW((CTXStringW *)&v29);
108                             CTXStringA::~CTXStringA((CTXStringA *)&v33);
109                             break;
110                         }
111                     }
112                 }
113             }
114         }
115     }
116 }
117 0003EF98 sub_510EFA54:74 (510EFB98)
```

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。

13:44:46.7434890 QO.exe 13336 QueryDirectoryC:\Users\28718\AppData\Local\GitHubDesktop\packages*	SUCCESS Filter: *, l...
13:44:46.7435065 QO.exe 13336 QueryDirectoryC:\Users\28718\AppData\Local\GitHubDesktop\packages	SUCCESS 0: ..., 1: be...
13:44:46.7435215 QO.exe 13336 QueryDirectoryC:\Users\28718\AppData\Local\GitHubDesktop\packages	NO MORE FILES
13:44:46.7435285 QO.exe 13336 CloseFile C:\Users\28718\AppData\Local\GitHubDesktop\packages	SUCCESS
13:44:46.7436366 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	PATH NOT FOUND Desired Acces...
13:44:46.7437001 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	PATH NOT FOUND Desired Acces...
13:44:46.7437485 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Desired Acces...
13:44:46.7437679 QO.exe 13336 QueryDirectoryC:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Filter: *, l...
13:44:46.7437808 QO.exe 13336 QueryDirectoryC:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS 0: ..., 1: App...
13:44:46.7437949 QO.exe 13336 QueryDirectoryC:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	NO MORE FILES
13:44:46.7438014 QO.exe 13336 CloseFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS
13:44:46.7439209 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Desired Acces...
13:44:46.7439361 QO.exe 13336 QueryBasicI... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS CreationTime:...
13:44:46.7439430 QO.exe 13336 CloseFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS
13:44:46.7440420 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Desired Acces...
13:44:46.7440531 QO.exe 13336 QueryBasicI... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS CreationTime:...
13:44:46.7440588 QO.exe 13336 CloseFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS
13:44:46.7440687 QO.exe 13336 FileSystemEm... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Control: FSCT...
13:44:46.7441251 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SHARING VIOLA... Desired Acces...
13:44:46.7441798 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Desired Acces...
13:44:46.7442130 QO.exe 13336 QueryBAFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS
13:44:46.7446571 QO.exe 13336 QueryAttrib... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Attributes: A...
13:44:46.7446720 QO.exe 13336 QueryStandar... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS AllocationSiz...
13:44:46.7446812 QO.exe 13336 QueryBasicI... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS CreationTime:...
13:44:46.7446940 QO.exe 13336 QueryStream... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS 0: ::\$DATA
13:44:46.7447244 QO.exe 13336 QueryBasicI... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS CreationTime:...
13:44:46.7447349 QO.exe 13336 QueryBasicI... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS EaSize: 0
13:44:46.7448161 QO.exe 13336 CreateFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Desired Acces...
13:44:46.7448651 QO.exe 13336 QueryAttrib... C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS FileSystemAtt...
13:44:46.7449749 QO.exe 13336 QueryBasicI... C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS CreationTime:...
13:44:46.7449822 QO.exe 13336 QueryAttrib... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS FileSystemAtt...
13:44:46.7449952 QO.exe 13336 QueryRemote... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	INVALID PARAM...
13:44:46.7450069 QO.exe 13336 QuerySecuri... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Information: ...
13:44:46.7450210 QO.exe 13336 SetEndOfFile... C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS EndOfFile: 78...
13:44:46.7450833 QO.exe 13336 FileSystemEm... C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Control: FSCT...
13:44:46.7452497 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS DEVICE FEATUR... Offset: 0, Le...
13:44:46.7454551 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 0, Le...
13:44:46.7457158 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 1,048...
13:44:46.7459084 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 1,048...
13:44:46.7461177 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 2,097...
13:44:46.7463041 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 2,097...
13:44:46.7465108 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 3,145...
13:44:46.7467007 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 3,145...
13:44:46.7469023 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 4,194...
13:44:46.7470797 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 4,194...
13:44:46.7472848 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 5,242...
13:44:46.7474463 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 5,242...
13:44:46.7476346 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 6,291...
13:44:46.7478039 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 6,291...
13:44:46.7479931 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 7,340...
13:44:46.7481526 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 7,340...
13:44:46.7483357 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 8,388...
13:44:46.7484970 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 8,388...
13:44:46.7486845 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 9,437...
13:44:46.7488367 QO.exe 13336 WriteFile C:\Users\28718\AppData\Local\Temp\temphis.db	SUCCESS Offset: 9,437...
13:44:46.7490237 QO.exe 13336 ReadFile C:\Users\28718\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS Offset: 10,48...
13:44:46.7491703 QO.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。



22:50:52.3194034	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	CreationTime:...
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	CreationTime:...
22:50:52.3195352	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SHARING VIOLA...	Desired Acces...
22:50:52.3196407	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3196547	TIM.exe	9592	QueryEAFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	CreationTime:...
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	QuerySalInfo...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	SalSize: 0
22:50:52.3279006	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Desired Acces...
22:50:52.3281095	TIM.exe	9592	QueryAttrib...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	FileSystemAtt...
22:50:52.3281213	TIM.exe	9592	QueryBasicI...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	CreationTime:...
22:50:52.3281295	TIM.exe	9592	QueryAttrib...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	FileSystemAtt...
22:50:52.3281443	TIM.exe	9592	QueryRemote...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	INVALID PARAM...	Information: ...
22:50:52.3281563	TIM.exe	9592	QuerySecuri...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	EndOfFile: 11...
22:50:52.3281729	TIM.exe	9592	SetEndOffFil...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 0, Le...
22:50:52.3282563	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Offset: 69,63...
22:50:52.3282502	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	CreationTime:...
22:50:52.3289975	TIM.exe	9592	SetBasicInf...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	INVALID PARAM...	Desired Acces...
22:50:52.3289536	TIM.exe	9592	QueryRemote...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	CreationTime:...
22:50:52.3289652	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Desired Acces...
22:50:52.3294792	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3297047	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	CreationTime:...
22:50:52.3297232	TIM.exe	9592	QueryNetwor...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	CreationTime:...
22:50:52.3297260	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Desired Acces...
22:50:52.3298100	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Desired Acces...
22:50:52.3298606	TIM.exe	9592	QueryEAFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Exclusive: Tr...
22:50:52.3301959	TIM.exe	9592	LockFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	AllocationSiz...
22:50:52.3302057	TIM.exe	9592	QueryStanda...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 0, Le...
22:50:52.3302143	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 31, L...
22:50:52.3302327	TIM.exe	9592	UnlockFileS...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 0, Le...
22:50:52.3302574	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Exclusive: Tr...
22:50:52.3303050	TIM.exe	9592	LockFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	AllocationSiz...
22:50:52.3303114	TIM.exe	9592	QueryStanda...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 31, L...
22:50:52.3303181	TIM.exe	9592	UnlockFileS...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Exclusive: Tr...
22:50:52.3303235	TIM.exe	9592	LockFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	AllocationSiz...
22:50:52.3303290	TIM.exe	9592	QueryStanda...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 0, Le...
22:50:52.3303241	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 0, Le...
22:50:52.3303404	TIM.exe	9592	UnlockFileS...	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Offset: 31, L...
22:50:52.3303556	TIM.exe	9592	LockFile	C:\Users\qwqdanchun\AppData\Local\Temp\tempsh.db	SUCCESS	Exclusive: Tr...
22:50:52.3052252	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Comms\Unistore\B\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3055179	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\ConnecteDevicesPlatform\L\qwqdanchun\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3055827	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\ConnecteDevicesPlatform\L\qwqdanchun\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3057997	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\D3D0Cache\6010892af4f153f\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3058700	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\D3D0Cache\6010892af4f153f\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	CreationTime:...
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	Desired Acces...
22:50:52.3071074	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	CreationTime:...
22:50:52.3071212	TIM.exe	9592	QueryBasicI...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3071269	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3071916	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	Attributes: A...
22:50:52.3072356	TIM.exe	9592	QueryEAFile	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	AllocationSiz...
22:50:52.3146935	TIM.exe	9592	QueryAttrib...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	CreationTime:...
22:50:52.3150007	TIM.exe	9592	QueryStanda...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	0:::\$DATA
22:50:52.3150082	TIM.exe	9592	QueryBasicI...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	Exclusive: Tr...
22:50:52.3150223	TIM.exe	9592	QueryStream...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	SalSize: 0
22:50:52.3150467	TIM.exe	9592	QuerySalInfo...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	FileSystemAtt...
22:50:52.3150563	TIM.exe	9592	QueryAttrib...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	INVALID PARAM...	Information: ...
22:50:52.3154066	TIM.exe	9592	QueryRemote...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	Offset: 0, Le...
22:50:52.3154246	TIM.exe	9592	QuerySecuri...	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3154365	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3155957	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Google\Chrome\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3162698	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Google\CrashReports\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3168918	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\Microsoft\Credentials\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3190247	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	CreationTime:...
22:50:52.3193963	TIM.exe	9592	QueryBasicI...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3194034	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	CreationTime:...
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	Desired Acces...
22:50:52.3195352	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	Attributes: A...
22:50:52.3277144	TIM.exe	9592	QueryAttrib...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	AllocationSiz...
22:50:52.3277278	TIM.exe	9592	QueryStanda...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	CreationTime:...
22:50:52.3277351	TIM.exe	9592	QueryBasicI...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	0:::\$DATA
22:50:52.3277494	TIM.exe	9592	QueryStream...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	CreationTime:...
22:50:52.3277643	TIM.exe	9592	QueryBasicI...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	SalSize: 0
22:50:52.3277756	TIM.exe	9592	QuerySalInfo...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	FileSystemAtt...
22:50:52.3281296	TIM.exe	9592	QueryAttrib...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	INVALID PARAM...	Information: ...
22:50:52.3281443	TIM.exe	9592	QueryRemote...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Offset: 0, Le...
22:50:52.3281563	TIM.exe	9592	QuerySecuri...	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Offset: 69,63...
22:50:52.3282563	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	SUCCESS	Desired Acces...
22:50:52.3282802	TIM.exe	9592	ReadFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3284792	TIM.exe	9592	CloseFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Edge\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3329908	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Feeds\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3330988	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\Game DVR\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3337632	TIM.exe	9592	CreateFile	C:\Users\qwqdanchun\AppData\Local\Microsoft\Game DVR\User Data\Default\History	PATH NOT FOUND	Desired Acces...
22:50:52.3343380	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...

[招聘] 欢迎你加入看雪团队！

最后于 12小时前 被qwqdanchun编辑, 原因: 补充TIM

☆

收藏 · 2

👍

点赞 · 4

¥

打赏

↻

分享

最新回复 (22)

はつゆき 16小时前

2楼 0

澄清这个词用的好啊，哈哈哈

极客

hzqst 15小时前

3楼 0

你懂不懂什么叫《大 数据》啊！

大牛

最新回复 (22)

killleer 14小时前

4 楼

0

极客

hzqst 你懂不懂什么叫《大 数 据》啊!

gg, 看小黄片和看gayhub和谐内容被tx看的清清楚楚 😊

这个教训也告诉我们: 事实证明r3取证或者不用阴间api取证, 加上没有一个好的anti-debug是多么愚蠢的操作

最后于 14小时前 被killleer编辑, 原因:

killleer 14小时前

5 楼

0

极客

hzqst 你懂不懂什么叫《大 数 据》啊!

还有, 火绒hips永远滴神 😊

期待下次出一个bypass huorong hips的取证

最后于 14小时前 被killleer编辑, 原因:

dayang 14小时前

6 楼

0

极客

TIM 也有这个行为么?

最后于 14小时前 被dayang编辑, 原因:

qwqdanchun 14小时前

7 楼

0

极客

dayang TIM 也有这个行为么?

TIM没有试, 有兴趣的可以趁着电脑开机, 挂上TIM和procmon等着看

晚上来编辑一下, TIM也有

最后于 12小时前 被qwqdanchun编辑, 原因:

qwqdanchun 14小时前

8 楼

0

极客

killleer hzqst 你懂不懂什么叫《大 数 据》啊! gg, 看小黄片和看gayhub和谐内容被tx看的清清楚楚这个教训也告诉我们: 事实证明r3取证或者不用阴间api取证 ...

事实证明, 不止没有anti-debug, 而且字符串都是明文可以搜到的

月落之江 13小时前

9 楼

0

大侠

lz上个dll的样本或者给个hash值? PC QQ丢ida里没看到这块逻辑, 不是不相信, 是想看看他那这些数据干什么了

☆

2

👍

4

¥

最新回复 (22)

qwqdanchun 13小时前

10 楼

0

月落之江 lz上个dll的样本或者给个hash值？ PC QQ丢ida里没看到这块逻辑，不是不相信，是想看看他那这些数据干什么了

https://file.qwqdanchun.com/Temp/AppUtil.dll 就在qq安装目录就可以找到，IDA里直接看“.text:510EFB98”附近，或者搜索“User Data”就能找到文中图片位置

毅种循环 12小时前

11 楼

0

建议QQ重来

月落之江 11小时前

12 楼

0

qwqdanchun https://file.qwqdanchun.com/Temp/AppUtil.dll 就在qq安装目录就可以找到，IDA里直接看“.text:510EFB98”附近，或者搜索“User Dat ...

得，局域网开个主机只跑这垃圾软件吧，太强了，不愧是tx。
顺便我PCQQ 9.4.1的DLL跟你发的不一样，搜字符串也没这个逻辑，看起来锁定这个版本，废掉qqprotect是当务之急

boursonjane 11小时前

13 楼

0

只能unity了啊

qwqdanchun 11小时前

14 楼

0

月落之江 得，局域网开个主机只跑这垃圾软件吧，太强了，不愧是tx。顺便我PCQQ 9.4.1的DLL跟你发的不一样，搜字符串也没这个逻辑，看起来锁定这个版本，废掉qqprotect是当务之急

我用的是QQ9.4.2（27662），TIM是官网最新版。
刚找了9.4.1的发现是有的，如果你没有找到可以把这个dll打包发我看下

月落之江 10小时前

15 楼

0

sha1:11452A002088C24616B4AF8E8D2E0C2688FECB5C

上传的附件：

[AppUtil.dll](#) （1.50MB，1次下载）

hhkqqs 10小时前

16 楼

0

这个好办，把文件夹设成只读就不会更新浏览记录了，或者用无痕模式浏览网页

极客

大侠

极客

极客

大侠

大侠


最新回复 (22)

月落之江   10小时前

17 楼

 0

大侠

 [hhkqqs](#) 这个好办，把文件夹设成只读就不会更新浏览记录了，或者用无痕模式浏览网页

[em_86]

这就因噎废食了，是QQ/微信绑架了你，让你不得不用他们的产品，而作为用户，我没办法因为它收集个人隐私就不再使用它，也不可能因为它不在使用访问历史的功能，折中的办法是干掉这些行为

淡然他徒弟  10小时前

18 楼

 0

大侠


有没有办法屏蔽他这个行为

月落之江   10小时前

19 楼

 0

大侠

 [qwqdanchun](#) 我用的是QQ9.4.2（27662），TIM是官网最新版. 刚找了9.4.1的发现是有

的，如果你没有找到可以把这个dll打包发我看下


不好意思，刚用ALT + T全局搜索了一下，搜索到了，位于sub_510DFA17

qwqdanchun  9小时前

20 楼

 0

极客

 [淡然他徒弟](#) 有没有办法屏蔽他这个行为

比如v2ex那个帖子里，发现这个行为就是因为火绒hips的自定义规则，类似的软件都可以阻止行为


zbzb  9小时前

21 楼

 0

极客

哈哈，赞一个！企鹅家的日常操作。况且有qqprotect，能做得事情更多了

VNRKDOEA  25分钟前

22 楼

 0

极客

我不是针对你，我是说在座的各位我都读取😏

guozizheng  2分钟前

23 楼

 0

极客

9.2.3的AppUtil里面也查到了



游客

[登录](#) | [注册](#) 方可回帖

回帖

表情

 高级回复

返回