# 样本分析报告

文件名称： steam_api.dll

SHA256： 4a922bb19075e350badd30366de1f065f76aefc0e563a3d10ef94b07858ea24c

文件大小： 1.67 MB

文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 5 sections

分析环境： Win10(1903 64bit,Office2016)

微步判定： 未知

云沙箱

# 目录

# steam_api.dll

首次提交: 2018/03/25　末次提交: 2026/01/03　末次分析: 2026/01/03 21:01:21

文件大小： 1.67 MB　文件类型： PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 5 sections

引擎检出： 0 / 28　分析环境： Win10(1903 64bit,Office2016)

未知

HASH

SHA256: 4a922bb19075e350badd30366de1f065f76aefc0e563a3d10ef94b07858ea24c

MD5: e8dc9c44155356d1712776b8cae0923d

SHA1: 674825cbd0b7890b0cdf54462cf44e5654b66be6

## 行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **0** 条技术指标。

Win10(1903 64bit,Office2016)

**通用行为 (1)**

一般行为　这个可执行文件存在调试数据库文件（PDB）路径

## 多引擎检测

检出率：**0** / 28

最近检测时间：2026-01-03 21:00:31

| 引擎 | 检出 | 引擎 | 检出 |
|---|---|---|---|
| 微软（MSE） | 无检出 | ESET | 无检出 |
| 卡巴斯基（Kaspersky） | 无检出 | 小红伞（Avira） | 无检出 |
| IKARUS | 无检出 | 大蜘蛛（Dr.Web） | 无检出 |
| Avast | 无检出 | AVG | 无检出 |
| GDATA | 无检出 | K7 | 无检出 |
| 安天（Antiy） | 无检出 | 江民（JiangMin） | 无检出 |
| 360（Qihoo 360） | 无检出 | Baidu | 无检出 |
| NANO | 无检出 | Trustlook | 无检出 |
| 瑞星（Rising） | 无检出 | 熊猫（Panda） | 无检出 |
| Sophos | 无检出 | ClamAV | 无检出 |
| WebShell专杀 | 无检出 | Baidu-China | 无检出 |
| MicroAPT | 无检出 | OneAV | 无检出 |
| OneStatic | 无检出 | MicroNonPE | 无检出 |
| OneAV-PWSH | 无检出 | ShellPub | 无检出 |

收起全部

## 静态分析

### 基础信息

| | |
|---|---|
| 文件名称 | 4a922bb19075e350badd30366de1f065f76aefc0e563a3d10ef94b07858ea24c |
| 文件格式 | DLLx86 |
| 文件类型(Magic) | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| 文件大小 | 1.67MB |
| SHA256 | 4a922bb19075e350badd30366de1f065f76aefc0e563a3d10ef94b07858ea24c |
| SHA1 | 674825cbd0b7890b0cdf54462cf44e5654b66be6 |
| MD5 | e8dc9c44155356d1712776b8cae0923d |
| CRC32 | 1D7C05EE |
| SSDEEP | 24576:sAZXxm59MtDFbkBM+Lwm5NJ/jOKkCf6myCCrO:s0t5bkBMWwS/JfdCy |
| TLSH | T1918529CA96F18B12C45E4378594FBFB8B12486868D3ACDD78F99B8F434106A3659F334 |
| peHashNG | 21f71d45ff840801445e30ae2e7fcce43e99f3d4695cbd6f8740ff47ddac053c |
| RichHash | 8480323f498a4c2c0e456728985f567d |
| impfuzzy | 24:l33HuOuFV4WBZV4QV4WCPlJcrv45bUOXYV4WCX+xtt+f1k/DZ3bJ3rvYMqlLUYpB:f79JcrvOnX+xttmkdbadjfSSrj |
| ImpHash | 2a73c9edce20e4a69d16f40b045696f2 |
| ExpHash | 988f0c476e976ef4c47da6cb984224d4 |
| Tags | dll,tls_callback,pdb_path,lang_chinese |

### 元数据

**ExifTool**

| | |
|---|---|
| CharacterSet | Unicode |
| CodeSize | 842240 |
| CompanyName | Valve Corporation |
| EntryPoint | 0xc7c4b |
| FileDescription | Steam Client API |
| FileFlags | (none) |
| FileFlagsMask | 0x003f |
| FileOS | Windows NT 32-bit |
| FileSubtype | 0 |
| FileType | Win32 DLL |
| FileTypeExtension | dll |
| FileVersion | 03.92.72.58 |
| FileVersionNumber | 1.0.0.1 |
| ImageFileCharacteristics | Executable, 32-bit, DLL |
| ImageVersion | 0.0 |
| InitializedDataSize | 1208832 |
| InternalName | Steam Client API |
| LanguageCode | Chinese (Simplified) |
| LegalCopyright | Copyright (C) 2017 |
| LinkerVersion | 14.13 |
| MIMEType | application/octet-stream |
| MachineType | Intel 386 or later, and compatibles |
| OSVersion | 6.0 |
| ObjectFileType | Dynamic link library |
| OriginalFileName | steam_ap.dll |
| PEType | PE32 |
| ProductName | Steam Client API |
| ProductVersion | 01.00.00.01 |
| ProductVersionNumber | 1.0.0.1 |
| Subsystem | Windows GUI |
| SubsystemVersion | 6.0 |
| TimeStamp | 2018:03:09 17:14:07+08:00 |
| UninitializedDataSize | 0 |

**TrID**

| | |
|---|---|
| 32.2% (.EXE) | Win64 Executable (generic) (10523/12/4) |
| 20.1% (.DLL) | Win32 Dynamic Link Library (generic) (6578/25/2) |
| 15.4% (.EXE) | Win16 NE executable (generic) (5038/12/1) |
| 13.7% (.EXE) | Win32 Executable (generic) (4505/5/1) |
| 6.2% (.EXE) | OS/2 Executable (generic) (2029/13) |

**DIE**

| | |
|---|---|
| 链接器 | Microsoft Linker(14.13.26128) |
| 编译器 | Microsoft Visual C/C++(19.13.26128)[LTCG/C++] |
| 工具 | Visual Studio(2017 version 15.6) |
| 字节序 | LE |
| 模式 | 32 |
| 程序类型 | DLL |
| 文件类型 | PE32 |
| 熵 | 6.177903657470595 |
| 语言 | C/C++ |
| 操作系统 | Windows(Vista)[I386, 32位, DLL] |

**Magika**

| | |
|---|---|
| Mime_type | application/x-dosexec |
| 分类 (Group) | executable |
| 描述信息 (Description) | PE Windows executable |

## 格式深度分析

文档分析

**PE头信息**

| | |
|---|---|
| 平台 | Intel 386 or later processors and compatible processors |
| 子系统 | Windows graphical user interface (GUI) subsystem |
| 编译时间戳 | 2018-03-09 17:14:07 |
| 入口点(OEP) | 0xc7c4b |
| 入口所在段 | .text |
| 镜像基地址 | 0x10000000 |
| 节区数量 | 5 |
| LinkerVersion | 14 |

**PE版本信息**

| | |
|---|---|
| 文件说明 | Steam Client API |
| 文件版本 | 03.92.72.58 |
| 产品名称 | Steam Client API |
| 产品版本 | 01.00.00.01 |
| 内部名称 | Steam Client API |
| 原始文件名 | steam_ap.dll |
| 语言 | 0x0804 0x04b0 |
| 版权 | Copyright (C) 2017 |

**调试信息**

| | |
|---|---|
| PDB | D:\localize\libs\steam\steam_api_new\Release\steam_api.pdb |
| GUID | - |

**签名信息**

| | |
|---|---|
| 签名验证 | NotSigned |

**TLS结构**

| | |
|---|---|
| AddressOfCallBacks | 0x100cf1d4 |
| AddressOfIndex | 0x1019a72c |
| Characteristics | 0x00300000 |
| EndAddressOfRawData | 0x10188b88 |
| SizeOfZeroFill | 0x00000000 |
| StartAddressOfRawData | 0x10188b80 |

**导入表(3)**

| DLL | DLL描述 | 函数数量 | |
|---|---|---|---|
| SHLWAPI.dll | - | 1 | 展开 |
| WS2_32.dll | - | 2 | 展开 |
| KERNEL32.dll | - | 98 | 展开 |

**导出表(100+)**

| 函数名 | 函数地址 | 函数序号 |
|---|---|---|
| CAssociateWithClanResult_t_RemoveCallResult | 0x100010e0 | 1 |
| CAssociateWithClanResult_t_SetCallResult | 0x100010e0 | 2 |
| CCheckFileSignature_t_RemoveCallResult | 0x100010e0 | 3 |
| CCheckFileSignature_t_SetCallResult | 0x100010e0 | 4 |
| CClanOfficerListResponse_t_RemoveCallResult | 0x100010e0 | 5 |

**PE节区(5)**

| 节名 | 虚拟地址 | 虚拟大小 | 物理地址 | 物理大小 | 节权限 | 熵值 | 节哈希 |
|---|---|---|---|---|---|---|---|
| .text | 0x00001000 | 0x000cd94a | 0x00000400 | 0x000cda00 | R-E | 6.427267808177346 | 6fa348c2a3dfb66e65e309ee0648a86b |
| .rdata | 0x000cf000 | 0x000c606e | 0x000cde00 | 0x000c6200 | R-- | 5.118021828847528 | b3e0d58888224db2e662440b7f39bb1c |
| .data | 0x00196000 | 0x0004d598 | 0x00194000 | 0x00003a00 | RW- | 4.198938383298816 | 99ee37b985907d3686d274a234a1f639 |
| .rsrc | 0x001e4000 | 0x00000518 | 0x00197a00 | 0x00000600 | R-- | 3.7242495310419192 | 7866450ffc965c2f613c |

**PE资源(2)**

| 资源名 | 资源类型 | 资源大小 | 偏移地址 | 语言 | 子语言 |
|---|---|---|---|---|---|
| RT_VERSION | data | 0x000002f8 | 0x001e40a0 | LANG_CHINESE | SUBLANG_CHINESE_SIMPLIFIED |
| RT_MANIFEST | XML 1.0 document text | 0x0000017d | 0x001e4398 | LANG_ENGLISH | SUBLANG_ENGLISH_US |

文件内容

**字符串**

Unicode ASCII

输入搜索内容

```
scdocgo
az-AZ-Cyrl
quz-ec
sr-sp-latn
__crt_strtox::floating_point_value::as_double
api-ms-win-core-datetime-l1-1-1
```

复制 下载

## 沙箱动态检测

Win10(1903 64bit,Office2016)

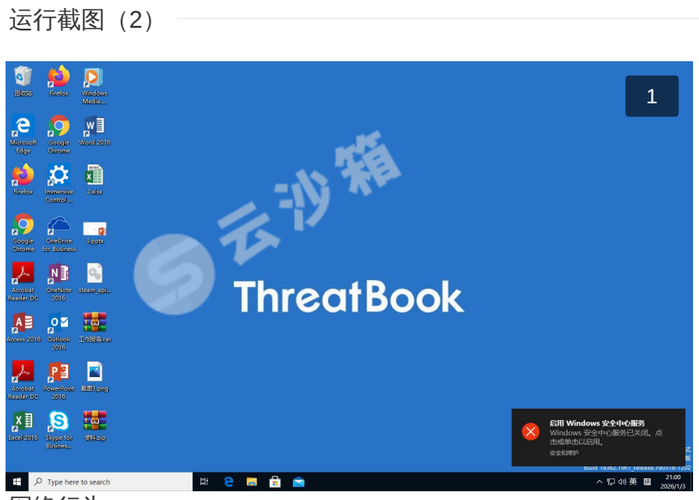
执行流程

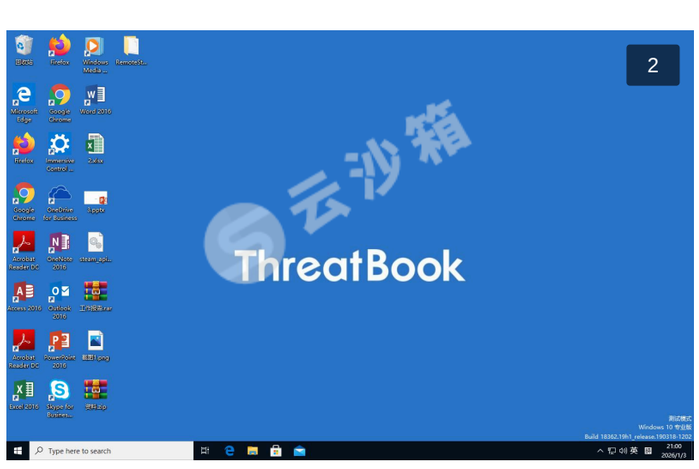

## 进程详情

共分析了15个进程

- rundll32.exe（PID：5020）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUGC_RemoveItemKeyValueTags
- rundll32.exe（PID：4532）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamScreenshots_TagPublishedFile
- rundll32.exe（PID：5264）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUGC_SetUserItemVote
- rundll32.exe（PID：4700）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUser_RequestEncryptedAppTicket
- rundll32.exe（PID：4536）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamRemoteStorage_FileWriteStreamCancel
- rundll32.exe（PID：5084）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamRemoteStorage_FileWriteStreamOpen
- rundll32.exe（PID：3864）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamGameServerStats_GetUserStat0
- rundll32.exe（PID：5664）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamHTMLSurface_ExecuteJavascript
- rundll32.exe（PID：2616）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamNetworking_CreateConnectionSocket
- rundll32.exe（PID：5404）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamMatchmakingServers_RefreshQuery
- rundll32.exe（PID：5672）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUGC_SuspendDownloads
- rundll32.exe（PID：5164）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUGC_SetReturnMetadata
- rundll32.exe（PID：6300）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUserStats_GetAchievementAndUnlockTime
- rundll32.exe（PID：6604）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUGC_SetItemTitle
- rundll32.exe（PID：6896）
  "C:\Windows\SysWOW64\rundll32.exe" C:\Users\Administrator\Desktop\steam_api.dll,SteamAPI_ISteamUtils_SetOverlayNotificationPosition

## 运行截图（2）




## 网络行为

| 指纹 | 域名 | DNS | HTTP | HTTPS | TCP | UDP | SMTP | ICMP | IRC | Hosts | Dead-Hosts |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## 释放文件

无释放文件