又一个神游机iQue Player破解指南

2023-03-31

> 简介
> 为了Project Unmask的发布，特地写了一篇胎教级神游机破解指南。

目录

本文更新地址：https://github.com/chasedream1129/project-unmask (https://github.com/chasedream1129/project-unmask)

准备条件

hacking_utils.zip

- 其中提供了以下文件：
- **iQue@Home-standard.rar** 神游在线
- **ique_cbc_attack.exe** 注入程序（Linux/macOS需自行编译）
- **iQueDiagExtend** 命令行实用工具
- **ticket.sys_editor.exe** ticket编辑器（便携版，无需额外安装Python环境）
- **ticket.sys_editor.py** ticket编辑器（需要安装Python3环境）

32位Windows系统

- 运行着Windows XP或Windows 7 32位版的PC或虚拟机
- 安装了 **iQue@Home神游在线**（iQue@Home-standard.rar (https://web.archive.org/web/20170225044741/https://www.ique.com/prod standard.rar) ）
- 安装了**MSVC 运行时库**，**iQueDiagExtend**依赖它。(vc_redist.x86.exe (https://aka.ms/vs/17/release/vc_redist.x86.exe))

- **iQueDiagExtend** 命令行实用工具
  - 文件名与iQue@Home内置工具相同，同样是ique_diag.exe，但iQueDiagExtend为拓展版，注意不要混淆。
- 在32位Windows系统与主系统间传输文件的方式
  - 若是实体机，可用U盘
  - 若是虚拟机，可用共享文件夹
  - 局域网或互联网传输，也是可行的

主系统

- 本文假设是Windows 10（Linux/macOS亦可）
- **ique_cbc_attack.exe** 注入程序（Linux/macOS需自行编译）
- **ticket.sys_editor.exe** ticket编辑器
  - 或**ticket.sys_editor.py**（需要安装Python3环境）

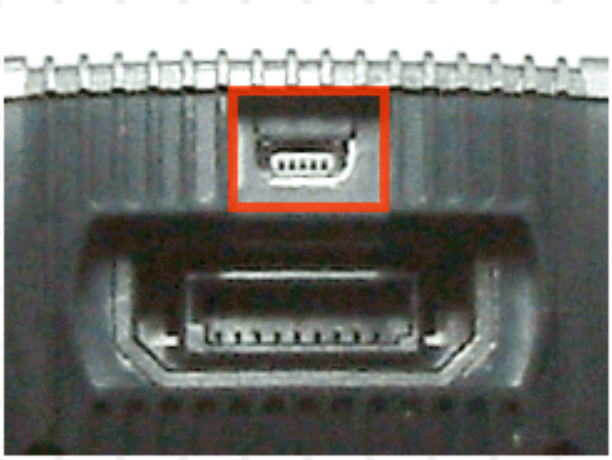
关于iQue Player与PC的USB连接

> ATTENTION
> 在此之前，请确认PC已安装**iQue@Home神游在线**。
>
> iQue Player驱动程序只支持32位Windows系统，请使用Windows XP或Windows 7 32位版。

> ATTENTION
> 只有2004年9月更新后的SKSA固件才支持USB连接，否则无法进行破解。主页左上角有**神游在线**标识则代表支持。
>
> 关于如何升级SKSA固件以支持USB连接，请阅读附录：SKSA固件升级 (#附录sksa固件升级) 。

1. 在断电的情况下，用**Mini（B型）USB数据线**连接iQue Player与PC。

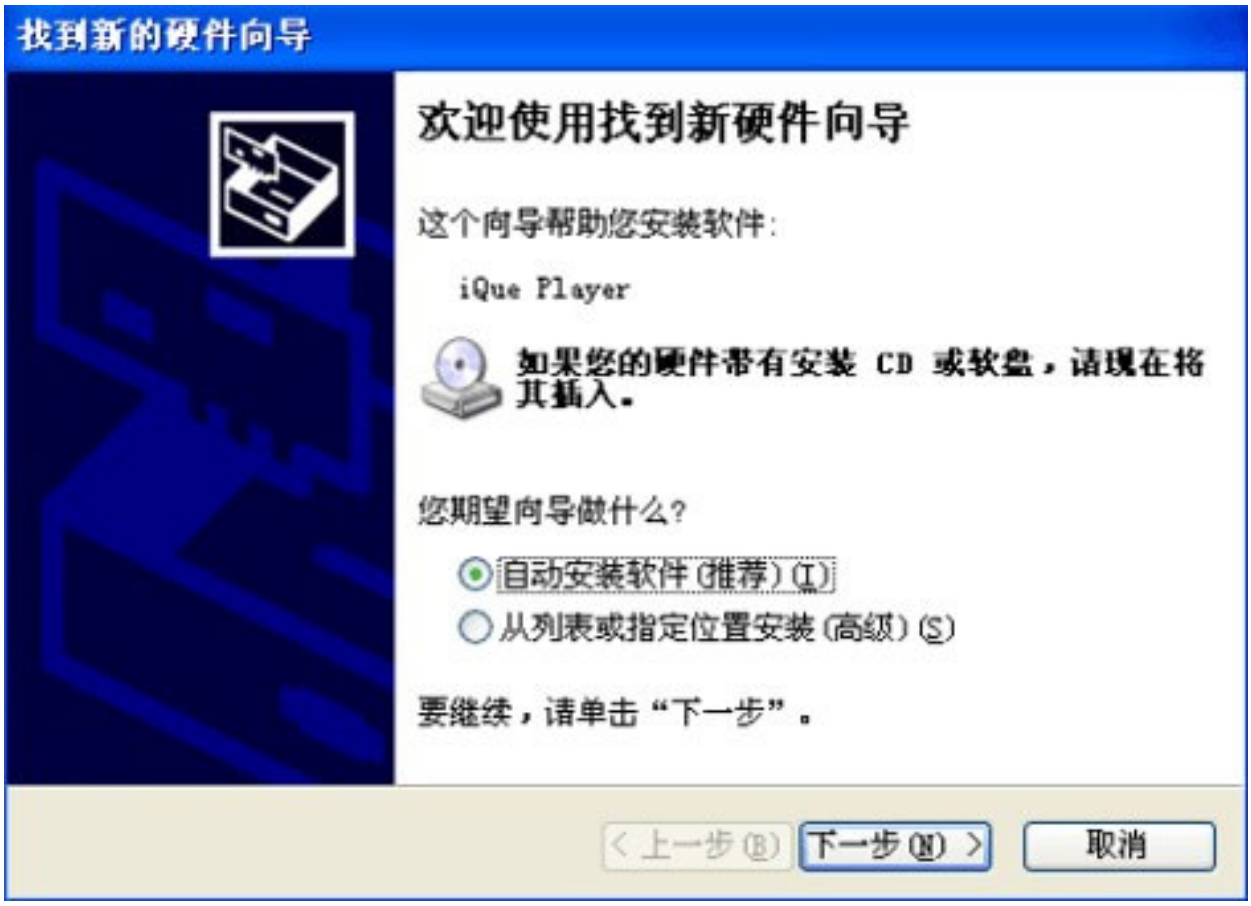
↑ USB连接线



↑ 神游机上的USB连接线插口

2. 插电，启动iQue Player，若绿色电源指示灯亮起则说明连接正确，将会显示以下画面。

3. 第一次连接时系统会自动弹出”找到新的硬件向导”，选择”自动安装软件”即可。



注入代码执行

此步骤将使用stuckpixel的**ique_cbc_attack** 注入程序，给《马力欧医生》打上补丁，以实现代码执行。

- 在此之前，请确认主机中已安装《马力欧医生》，并至少运行过一次。
- 《马力欧医生》游戏存档将被覆盖。

1. 将iQue Player连接到32位Windows系统，打开**ique_diag**。执行命令 `B` 初始化连接。
2. 在**ique_diag**中执行命令 `3 005d1870.rec` ，提取《马力欧医生》的加密ROM。
3. 将提取的**005d1870.rec**复制到主系统中**ique_cbc_attack**所在的文件夹中。
4. 在主系统中打开**命令行工具**（cmd），进入到**ique_cbc_attack**和**005d1870.rec**所在文件夹，并执行以下命令（完整长命令，不要换行）：

```
ique_cbc_attack -p 3C088001350818E03C09000135298ED0 -r 005d1870.rec -d 081F0000000000000000000000000000 -o 1000
```

若成功将显示以下信息：

```
  AES-CBC attack, by stuckpixel
  successfully injected 1 blocks!
```

1. 将注入后的**005d1870.rec**复制到32位Windows系统中的**iQueDiagExtend**文件夹。
2. 在**ique_diag**中执行命令 `4 005d1870.rec` ，将注入后的《马力欧医生》加密ROM写入到主机。

安装Jbop的HackIt破解菜单补丁

1. 将**hackit_patcher.sta**重命名为**005d1870.sta**。
2. 将**005d1870.sta**复制到32位Windows系统中的**iQueDiagExtend**文件夹。

3. 在**ique_diag**中执行命令 `4 005d1870.sta` ，将破解菜单补丁写入到主机。

提取ticket.sys程序数据库

1. 在**ique_diag**中执行命令 `3 ticket.sys` ，提取主机的ticket文件。
2. 将**ticket.sys**复制到主系统中。

编辑ticket.sys文件并安装游戏。

> ATTENTION
> 此处以《塞尔达传说：魔力面具》（Project Unmask）的ROM文件**00201741.app**与ticket文件**00201741-project-unmask.dat**为例。

1. 在主系统上运行**ticket.sys_editor.exe**
   - 或**ticket.sys_editor.py**（需要安装Python3环境）
2. *File –> Open file*，然后找到刚才从主机中提取的**ticket.sys**文件，并选择*Open*。
3. *Edit –> Import ticket.dat*，然后选择**00201741-project-unmask.dat**文件。
4. *File –> Save as*，然后命名为**hackit.sys**，并按下*Save*，保存编辑后的文件。
5. 将**hackit.sys**文件复制到32位Windows系统中的**iQueDiagExtend**文件夹。
6. 在**ique_diag**中执行命令 `4 hackit.sys` ，将修改后的**程序数据库**写入你的主机。
7. 在**ique_diag**中执行命令 `4 00201741.app` ，将ROM文件写入你的主机。

   00201741.app需占用128格，若出现以下错误：

```
ERROR fcreate fails ... deallocate
ERROR __bbc_write_file create temp.tmp fails -3
```

则代表神游卡剩余空间不足，请阅读附录：使用ique_diag删除游戏 (#附录使用ique_diag删除游戏) 。

8. 在**ique_diag**中执行命令 `Q` ，断开iQueDiagExtend与iQue Player的连接。
9. 关闭iQue Player。

进入HackIt破解菜单

1. 重新打开主机（不插入Mini USB数据线），启动到主菜单。
2. 启动游戏列表中的《马力欧医生》。游戏启动后应该是黑屏状态。
3. 在黑屏中**短按电源键**，返回到主菜单。
4. 当主菜单加载完毕后，进入游戏列表。
5. 若一切顺利，将能够看到Project Unmask的《塞尔达传说：魔力面具》。

尾声

至此，你已成功完成神游机iQue Player的破解。

今后，每次进入**HackIt菜单**都需要先启动《马力欧医生》，再按下电源键回到菜单。

很遗憾，《马力欧医生》将作为破解引导器，无法再正常游玩，除非重新安装正常的版本。

附录：SKSA固件升级

准备条件

- **SKSA_upgrader.zip** 包含了升级工具与SKSA 1106。
  - 依赖**.NET Framework 4.0**，Windows 10有自带。
- 一台**支持**USB的iQue Player，以下简称*新机*。
- 一台需要升级SKSA的iQue Player，以下简称*旧机*。
- 上文需求的**32位Windows系统** (#32位windows系统)
- 上文需求的**主系统** (#主系统)

升级流程

1. 将**新机**连接到32位Windows系统，并插电启动。
2. 热交换：在**启动状态**下，拔出**新机神游卡**，将**旧机神游卡**插入**新机**。
3. 打开**ique_diag**，执行命令 `B` 初始化连接。
4. 在**ique_diag**中执行命令 `1` ，提取**旧机神游卡**的NAND并等待其完成。
5. 将提取的**nand.bin**与**spare.bin**放到主系统中的SKSA_upgrader文件夹。
6. 运行do_upgrade.bat并等待其完成。

7. 打开output文件夹，将完成升级的**1106.nand.bin**与**1106.spare.bin**文件重命名为**nand.bin**与**spare.bin**。
8. 将升级后的**nand.bin**与**spare.bin**复制到iQueDiagExtend文件夹。
9. 在**ique_diag**中执行命令 `2` ，将升级后的NAND写入**旧机神游卡**。
10. 在**ique_diag**中执行命令 `Q` ，断开iQueDiagExtend与iQue Player的连接。
11. 关闭iQue Player，将**旧机神游卡**插回**旧机**。

附录：使用ique_diag删除游戏

1. 将iQue Player连接到32位Windows系统，打开**ique_diag**。执行命令 `B` 初始化连接。
2. 执行命令 `L` ，列出神游卡中安装的游戏。
   - 格式为 `cid [CID(十六进制)], size [容量(字节)]`
   - 对应关系请见下表。
3. 执行命令 `R CID(十六进制)` ，删除游戏。

CID	CID(十六进制)	名称	容量(字节)	容量(MB)	容量(格)
2103105	201741	塞尔达传说：魔力面具 (Project Unmask)	33554432	32	128
1101104	10CD30	神游马力欧	8060928	7.69	31
1101902	10D04E	神游马力欧 (操作指南)	212992	0.2	1
1101906	10D052	神游马力欧 (操作指南)	409600	0.39	2

CID	CID(十六进制)	名称	容量(字节)	容量(MB)	容量(格)
1102101	10D115	耀西故事	16023552	15.28	62
1102902	10D436	耀西故事 (操作指南)	196608	0.19	1
1102904	10D438	耀西故事 (操作指南)	245760	0.23	1
1102906	10D43A	耀西故事 (操作指南)	425984	0.41	2
1201105	1253D1	任天堂明星大乱斗	16793600	16.02	65
1201901	1256ED	任天堂明星大乱斗 (操作指南)	294912	0.28	2
2101104	200F70	塞尔达传说：时光之笛	29868032	28.48	114
2101902	20128E	塞尔达传说：时光之笛 (操作指南)	278528	0.27	2
2101904	201290	塞尔达传说：时光之笛 (操作指南)	425984	0.41	2
2102104	201358	纸片马力欧	41943040	40	160
2102902	201676	纸片马力欧 (操作指南)	376832	0.36	2
2102904	201678	纸片马力欧 (操作指南)	376832	0.36	2
2104108	201B2C	动物森林	16138240	15.39	62

CID	CID(十六进制)	名称	容量(字节)	容量(MB)	容量(格)
2105103	201F0F	组合机器人	16793600	16.02	65
2106101	2022F5	塞爾達傳說：時光之笛	29868032	28.48	114
4101104	3E93F0	星际火狐	11829248	11.28	46
4101105	3E93F1	星际火狐	11829248	11.28	46
4101902	3E970E	星际火狐 (操作指南)	163840	0.16	1
4101904	3E9710	星际火狐 (操作指南)	229376	0.22	1
4102103	3E97D7	罪与罚-地球的继承者-	33636352	32.08	129
4102901	3E9AF5	罪与罚-地球的继承者- (操作指南)	245760	0.23	1
5101104	4DD630	水上摩托	8159232	7.78	32
5101902	4DD94E	水上摩托 (操作指南)	311296	0.3	2
5101904	4DD950	水上摩托 (操作指南)	491520	0.47	2
5102108	4DDA1C	越野摩托	16072704	15.33	62
5102902	4DDD36	越野摩托 (操作指南)	262144	0.25	1
5201104	4F5CD0	马力欧卡丁车	12533760	11.95	48

CID	CID(十六进制)	名称	容量(字节)	容量(MB)	容量(格)
5201105	4F5CD1	马力欧卡丁车	12533760	11.95	48
5201902	4F5FEE	马力欧卡丁车 (操作指南)	245760	0.23	1
5201906	4F5FF2	马力欧卡丁车 (操作指南)	425984	0.41	2
5202103	4F60B7	F-Zero X 未来赛车 未来赛车	16334848	15.58	63
5202902	4F63D6	F-Zero X 未来赛车 (操作指南)	180224	0.17	1
5202904	4F63D8	F-Zero X 未来赛车 (操作指南)	294912	0.28	2
6101104	5D1870	马力欧医生	3358720	3.2	13
6101902	5D1B8E	马力欧医生 (操作指南)	294912	0.28	2
6101904	5D1B90	马力欧医生 (操作指南)	393216	0.38	2

参见

- iQue@Home-standard.rar (https://web.archive.org/web/20170225044741/https://www.ique.com/prodstandard.rar) iQue

- ique_cbc_attack (https://gist.github.com/pixel-stuck/e6e6d2148102b62b527d2777acefbf70) stuckpixel
- iQueDiagExtend (https://github.com/emoose/iQueDiagExtend) emoose
- ticket.sys_editor (https://github.com/iQueBrew/ticket.sys-editor) iQueBrew
- SKSA_upgrader(iQueTool) (https://github.com/emoose/iQueTool) emoose

About

16岁，是学生。

Related Posts

Project Unmask：运行情况及模拟器须知 (/2023-04-01-project-unmask-emu/)

关于Project Unmask的ROM运行情况及模拟器须知

Project Unmask (/2023-04-01-project-unmask/)

-Project Unmask- 神游未发售游戏——塞尔达传说：魔力面具 沉寂19年首次披露！

Random Posts

Hello, World! (/2022-02-04-hello-world/) 2022-02-04

Project Unmask (/2023-04-01-project-unmask-print/) 2023-04-01

多种手段，教你辨别NS卡盒真伪 (/2020-02-05-nintendo-switch-card-case-check/) 2020-02-05