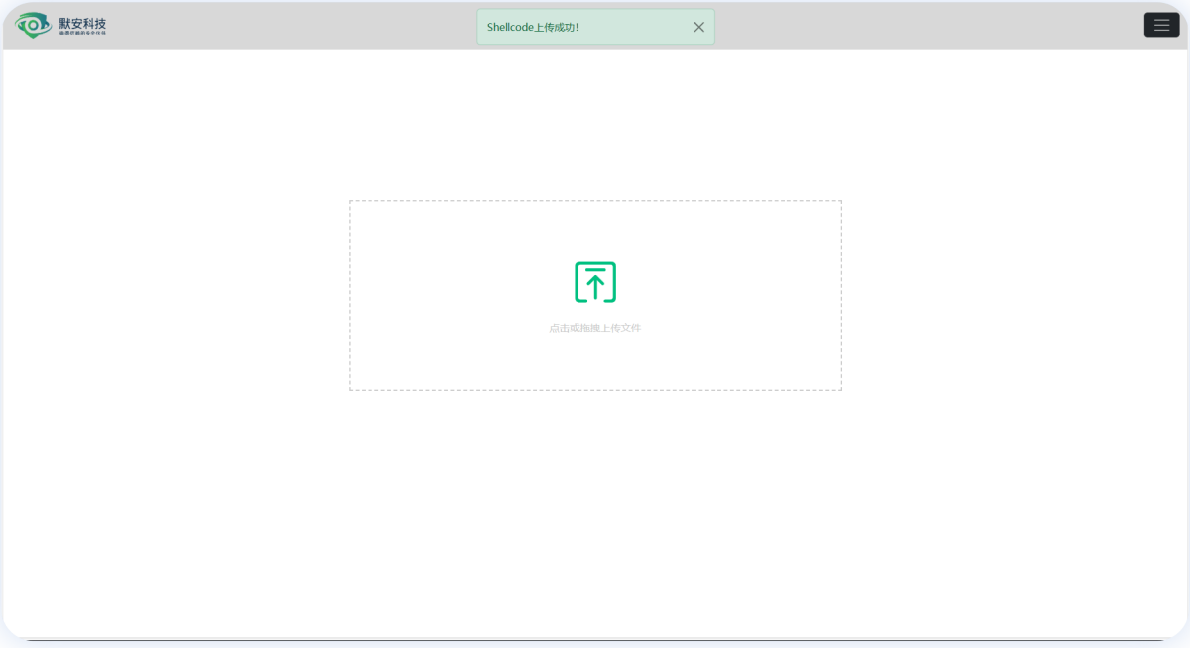
平台基本使用方法

> **注意：**64位shellcode或可执行文件使用前三个免杀模板，32位shellcode或可执行文件使用后两个免杀模板，如果免杀模板选择错误会导致生成的木马无法免杀。32位免杀模板免杀性较弱，必须配合添加图标或标签才能实现免杀。如果32位的shellcode或可执行文件是较大文件，则必须使用“幻阵测试”这个模板进行免杀。

文件上传

平台支持由主流渗透工具生成的`.c`、`.bin`和`.exe`三种格式的文件，文件大小不得超过5MB。

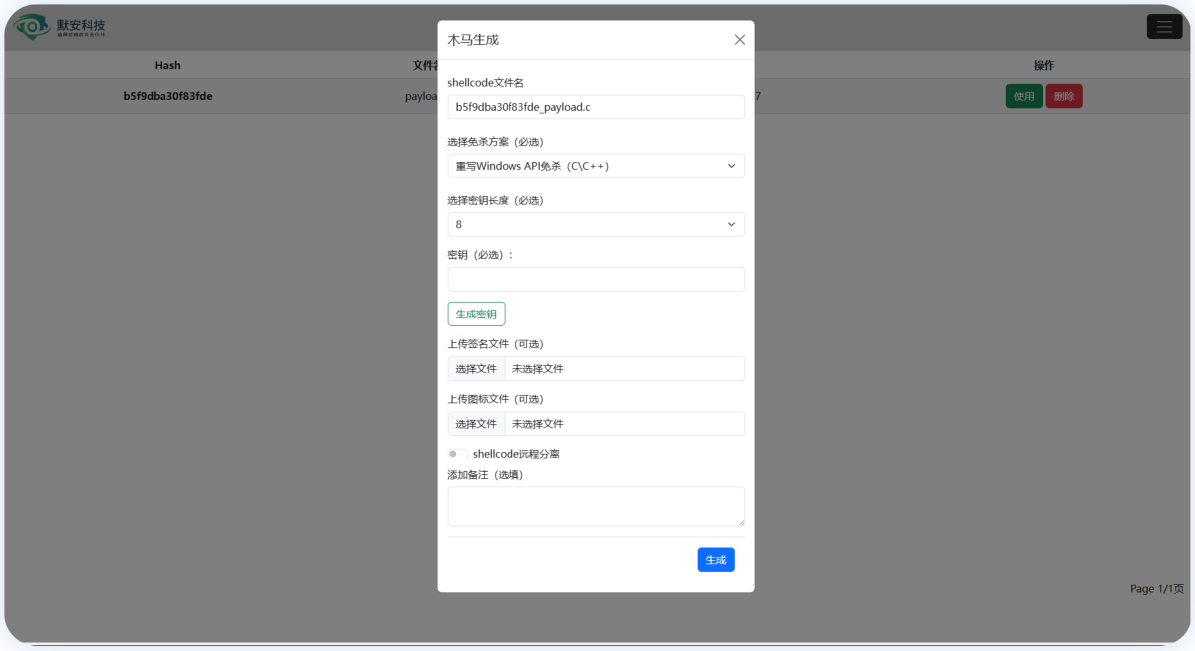
点击或拖拽至下图中的框内即可上传，返回成功信息则表示上传成功



木马生成

进入个人中心下的`Shellcode`页面即可进行木马生成

在对应的文件右边点击**生成**按钮即可定义木马生成方案，页面如下：



根据需要选择免杀方案，具体不同的免杀方案所采用的技术详见免杀模板。

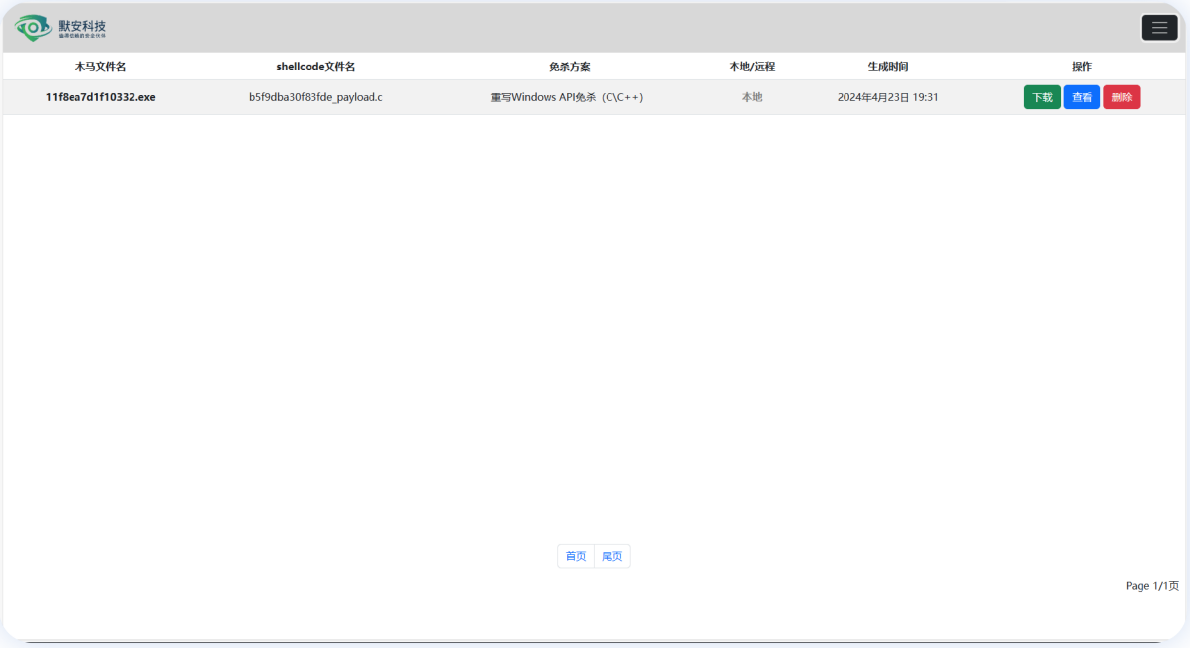
选择密钥长度后点击**生成密钥**可以生成随机的指定长度的密钥。上传签名文件或图标文件可以给生成的木马添加签名或图标，签名文件仅支持带签名的 `exe` 文件，图标文件仅支持 `ico` 文件。

最后点击生成后木马会在后台进行编译，时间较长需耐心等待，出现弹窗提示则表示编译成功。

> 远程分离免杀还在测试阶段，目前无论怎么选择都是默认不分离

木马管理

进入个人中心下的 `Trojan` 页面即可进行木马管理



木马文件名取的是前15位hash，shellcode文件名则是uuid+上传文件名，点击查看可以查询生成木马时添加的备注。木马生成后存储在平台上，建议使用后及时删除。

个人信息编辑

点击ID可以进入到个人信息页面，如下图：

如果不需要更改密码则让新密码和新密码（确认）都为空即可，平台登录采用用户名+密码的形式，所以用户名也为平台账号，请慎重修改。

免杀模板

重写Windows API免杀（C\C++）

- 仅支持64位shellcode或可执行文件
- 加密方式：`Rc4+Xor`
- 加载器：重写 了`VirtualAlloc`和`CreatThread` Windows API
- 反沙箱：检测程序有无被调试、检测磁盘是否小于2、判断程序有无被加速、定时执行加载器代码
- 自动添加混淆代码：√

UUID加密shellcode（C\C++）

- 仅支持64位shellcode或可执行文件
- 加密方式：`UUID+Xor`
- 加载器：重写 了`VirtualAlloc`和`CreatThread` Windows API
- 反沙箱：检测程序有无被调试、定时执行加载器代码
- 自动添加混淆代码：√

Rc4_Base64加密（Rust）

- 仅支持64位shellcode或可执行文件
- 加密方式：**Rc4+Base64**
- 加载器：基本的动态申请内存然后创建线程执行
- 反沙箱：检测程序有无被调试、判断程序有无被加速
- 自动添加混淆代码：√

动态获取Windows API 32位专用（C\C++）

- 仅支持32位shellcode或可执行文件
- 加密方式：`Rc4+Xor`
- 加载器：动态获取了`VirtualAlloc`等API
- 反沙箱：检测程序有无被调试、检测磁盘是否小于2、判断程序有无被加速、定时执行加载器代码
- 自动添加混淆代码：√

幻阵测试

- 仅支持32位shellcode或可执行文件
- 加密方式：`Rc4+Xor`
- 加载器：动态获取了`VirtualAlloc`等API
- 反沙箱：检测程序有无被调试、检测磁盘是否小于2、判断程序有无被加速、定时执行加载器代码
- 自动添加混淆代码：√