**[Windows 证书签名的伪造](https://www.cnblogs.com/LyShark/p/11347609.html)**

# 简介

Windows 系统中的一些非常重要文件通常会被添加数字签名，其目的是用来防止被篡改，能确保用户通过互联网下载时能确信此代码没有被非法篡改和来源可信，从而保护了代码的完整性、保护了用户不会被病毒、恶意代码和间谍软件所侵害，而一些杀毒软件也是通过检测程序中的证书来实现查杀判定的。

Sigthief是一个由python编写的，可以用于劫持合法的数字签名并绕过Windows的哈希验证机制的脚本工具。也可被红队用于将恶意二进制文件以及PowerShell脚本与本机操作系统文件相混淆，以逃避检测并绕过设备的安全防护。

# 工具下载

Github：<https://github.com/secretsquirrel/SigThief>

# 使用

执行以下命令即可（将consent.exe的数字签名赋给test.exe）

python sigthief.py -i c:\Windows\System32\consent.exe -t Desktops.exe -o test.exe

