Atitt info scry pc prvt scrt setting 信息安全pc机隐私安全设置

目录

[1. 隐藏 伪装技术 脱敏 2](#_Toc31944)

[1.1. 隐藏文件夹设置 2](#_Toc20754)

[1.2. ntfs权限设置 多用户隔离 2](#_Toc10671)

[1.3. 隱藏分區 2](#_Toc14616)

[1.4. 隐藏文件技术 2](#_Toc12813)

[2. 加密 2](#_Toc14543)

[2.1. Ntfs权限隔离 用户隔离。。 2](#_Toc23067)

[2.2. Efs加密 2](#_Toc30261)

[2.3. Bitlock 加密 3](#_Toc32730)

[2.4. Disk lock ，bios lock 3](#_Toc28481)

[2.5. Vpn +https tor浏览器 3](#_Toc18813)

[2.6. 各种重要加密 3](#_Toc6433)

[2.6.1. 隱寫術 3](#_Toc18456)

[2.7. VeraCrypt 分区加密 4](#_Toc30393)

[3. 資料定时抹除技术 4](#_Toc14520)

[3.1. 蹤跡混淆 4](#_Toc18379)

[3.2. 自动断电关机 4](#_Toc8018)

[4. 授权隔离 5](#_Toc16046)

[4.1. USB Key 5](#_Toc4659)

[4.2. USBGuard和USBKill般的軟件会採用USB認證策略。 5](#_Toc22664)

[4.3. 可信计算模块（Trusted Computing Module, TPM）](#_Toc463)[[5]](#_Toc463)[等。 5](#_Toc463)

[4.4. 3.4 其他身份认证技术 5](#_Toc5205)

[4.5. 受信任访问 设备管理 6](#_Toc26657)

[4.6. 各种app的俩步验证开启 6](#_Toc26448)

[4.7. 加固路由器密码 与白名单策略 6](#_Toc25598)

[5. 检测预警演习 6](#_Toc371)

[5.1. 渗透测试”。 漏洞扫码工具 6](#_Toc10246)

[5.2. 取证工具搜索 everthing 以即全文检索工具anytxt 6](#_Toc19242)

[5.3. 防火墙 杀毒软件 优化软件 6](#_Toc8728)

[6. Ref 7](#_Toc3440)

# 隐藏 伪装技术 脱敏

## 隐藏文件夹设置

## ntfs权限设置 多用户隔离

## 隱藏分區

## 隐藏文件技术

# 加密

## Ntfs权限隔离 用户隔离。。

重要app 资料不要安装在d盘这样的公共区域。。放入各自用户文件夹种。。

建立多个用户，，娱乐，工作等区分开

## Efs加密

开启efs加密敏感文件。。

包括金融敏感文件（身份证件

各种临时cache文件夹

Atitit impt sstv fldr 重要敏感的文件夹加密 与权限。。

目录

1.1. 权限使用多用户系统模式隔离。。 1

2. 文档 图文编辑软件的缓存文件夹 1

2.1. Wps零食文件夹 1

2.2. 看图库零食文件夹 2

3. Im email 网盘等重要信息系统重要资料 2

3.1. Email目录加密 2

3.2. Im tg零食文件夹。+tg 数据库dir 2

3.3. Tg export 数据备份ChatExport\_xxx 2

3.4. 网盘敏感文件夹加密 2

3.5. 备用u盘重要文件夹加密 2

3.6. 密钥u盘全盘加密（ntfs格式 2

4. 按照内容分类的敏感文件目录 2

4.1. 敏感文件和目录要增加机密tag方便区分 2

4.2. 工作文件目录inr 2

4.3. 政治类文件目录 3

4.4. 金融类敏感文件目录 （身份证件 银行卡类信息文件。。 3

## Bitlock 加密

## Disk lock ，bios lock

## Vpn +https tor浏览器

Vpn软件（在公共场所 机场 酒店 咖啡馆必备使用vpn

## 各种重要加密

浏览器数据文件 历史记录

數據隱藏（data hiding）、資料抹除（artifact wiping）、蹤跡混淆（trail obfuscation

### 隱寫術

[隱寫術](https://zh.wikipedia.org/wiki/%E9%9A%B1%E5%AF%AB%E8%A1%93" \o "隱寫術)指的是將資訊或檔案隱藏在另一個檔案之下的技術，這能讓它不被鑑證人員察覺。「隱寫術所產生的黑暗數據，通常埋藏於明面數據之下。（好比如埋藏在數碼照片當中的浮水印）」[[9]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-berghel-9)。一些專家認為會用到隱寫術的人十分稀少，故不值得花費精力去對付。但大多專家都會同意，若果使用得当，隱寫術本身也能夠破壞鑑證過程[[3]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-berinato-3)。

杰弗里·卡尔（Jeffrey Carr）稱，2007年版的恐怖主义双月刊《技术圣战者》（Technical Mujahid）講述了使用隱寫術程式「圣战者的秘密」（Secrets of the Mujahideen）的重要性。支持者認為該一款程式能夠透過隱寫術和文件壓縮，來反制隱寫分析程式[[10]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-10)。

## VeraCrypt 分区加密

与 EFS 相比，Bitlocker 因此代表了一种更先进的解决方案，因为它是作为解决方案提供的“ 安顿下来，忘记 »：配置该功能后，硬盘驱动器的内容将自动完全加密，无需任何进一步的用户干预。

然而，如上所述，那些宁愿避免使用 Microsoft 解决方案和 TPM 芯片的人可以求助于优秀的工具，例如 **VeraCrypt**， 非常感激 ” 叉“通过 TrueCrypt。

VeraCrypt 不仅允许您打开其前身 TrueCrypt 的档案，还允许您加密整个硬盘驱动器、单个分区或创建加密的“容器文件”，只有授权用户才能访问。

## 肯辛通电脑锁

加密可以有效防止盗窃。至少要对整个用户帐户加密，而不只是局限于几个文件。虽然会影响性能，但绝对有必要。Truecrypt适用于Windows、OS X、Linux，FreeOTFE适用于Windows和Linux

# 資料定时抹除技术

有些资料有时效性，可以设置定时抹除技术

## 蹤跡混淆

蹤跡混淆的目的在於矇騙和迷惑鑑證人員/工具，或轉移其焦點。能夠達至蹤跡混淆效果的工具和技巧有「記錄消除器、[欺骗](https://zh.wikipedia.org/wiki/IP%E5%9C%B0%E5%9D%80%E6%AC%BA%E9%AA%97" \o "IP地址欺骗)、[錯誤資訊](https://zh.wikipedia.org/wiki/%E9%8C%AF%E8%AA%A4%E8%B3%87%E8%A8%8A" \o "錯誤資訊)、骨幹跳躍、殭屍帳號、木馬指令」[[1]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-rogers-1)。

Timestomp為一款著名的蹤跡混淆工具[[11]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-bfmafia-11)，它能夠修改跟存取、建立、修改時間有關的檔案[元数据](https://zh.wikipedia.org/wiki/%E5%85%83%E6%95%B0%E6%8D%AE" \o "元数据)[[3]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-berinato-3)。

Transmogrify是另一款較常應用的蹤跡混淆軟件[[11]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-bfmafia-11)。大多文件的表頭包含了識別資訊，比方說[.jpg](https://zh.wikipedia.org/wiki/JPEG" \o "JPEG)即表示檔案為jpg檔，[.doc](https://zh.wikipedia.org/wiki/.doc" \o ".doc)則表示檔案為doc檔。Transmogrify使得用戶能夠修改檔案的表頭資訊，比如可由.jpg表頭修改成.doc表頭，令鎖定圖像格式的鑑證工具不把它視為圖像，繼而跳過之[[3]](https://zh.wikipedia.org/wiki/%E5%8F%8D%E9%9B%BB%E8%85%A6%E9%91%91%E8%AD%89" \l "cite_note-berinato-3)。

## 自动断电关机

可拆下手提電腦的電池，使之只能在連接到電源時運作。一旦切断電源，其便會關機，造成數據丟失。

# 授权隔离

## USB Key

## USBGuard和USBKill般的軟件会採用USB認證策略。

一旦連接的USB設備不符合條件，它便會開始執行特定操作

## 可信计算模块（Trusted Computing Module, TPM）[5]等。

## 3.4 其他身份认证技术

#### 3.4.1 智能卡

智能卡通常和信用卡大小一样，它所提供的抗篡改存储能保证用户的证书和私钥。Windows 2000系统引入了智能卡验证，它是基于用户持有凭证的身份认证技术，通过智能卡进行身份验证相比传统的用户名&口令的认证方式在安全性上有了极大的提高。 目前，使用智能卡及关联个人标记（PIN）的组合验证形式越来越受到人们的关注并广泛应用于金融、军事等安全级别要求较高的环境，它主要有以下优势[11]：

提高了攻击者的破解难度。由于智能卡使用难以伪造的电子证书作为凭证，黑客必须窃取智能卡并同时获取PIN才可以通过身份验证。

无法抵赖。由于智能卡能识别登录用户信息，所以降低了用户抵赖责任的可能性。

#### 3.4.2 生物特征认证

利用人类特征进行身份认证也是一种安全性较高的认证方法。口令和信物都有泄漏和复制的可能，但是生物特征具有无法复制的特点。因此，在对于安全性要求较高的系统，可使用这种费用相对比较昂贵的身份鉴别系统。这些鉴别系统利用授权用户的人类特征作为鉴别依据，主要有语音、指纹、视网膜及DNA等。 对于生物特征的认证程序目前大部分都是由第三方开发的，微软在Windows Vista中内置了指纹识别的认证程序[1]。

## ****受信任访问**** 设备管理

—— 移动设备或应用访问受策略限制，阻止未经授权的设备或应用访问业务数据。

## 各种app的俩步验证开启

## 加固路由器密码 与白名单策略

# 检测预警演习

## 渗透测试”。 漏洞扫码工具

## 运行入侵检测软件（HIDS），如ossec、tripwire或rkhunter。

## 取证工具搜索 everthing 以即全文检索工具anytxt

## 防火墙 杀毒软件 优化软件

Ms 默认防火墙，，路由器，可以把它当成硬件防火墙

杀毒软件antivirus free版本，，

优化软件 cclearner

**安装好用的杀毒软件（特别是你要使用P2P的话）。**杀毒软件可以处理各种最新的恶意软件，包括病毒、木马、键盘记录程序、rootkit（提权软件包）和蠕虫。弄清楚杀毒软件是否提供实时扫描、实时监控或手动扫描。同时也要弄清楚它是否是启发式软件。Avast[[3]](https://zh.wikihow.com/%E4%BF%9D%E6%8A%A4%E7%94%B5%E8%84%91%E7%9A%84%E5%AE%89%E5%85%A8" \l "_note-3) and AVG[[4]](https://zh.wikihow.com/%E4%BF%9D%E6%8A%A4%E7%94%B5%E8%84%91%E7%9A%84%E5%AE%89%E5%85%A8" \l "_note-4) 是非常好用的免费版本。选择其中一个，下载并安装，然后定期扫描。还要记得定期更新，让病毒库保持最新。

**下载并安装软件来处理间谍软件，如Spybot Search&Destroy（间谍软件清除器）、HijackThis[[5]](https://zh.wikihow.com/%E4%BF%9D%E6%8A%A4%E7%94%B5%E8%84%91%E7%9A%84%E5%AE%89%E5%85%A8" \l "_note-5) 或Ad-aware[[6]](https://zh.wikihow.com/%E4%BF%9D%E6%8A%A4%E7%94%B5%E8%84%91%E7%9A%84%E5%AE%89%E5%85%A8" \l "_note-6) ，记得定期扫描。**这样还不够——如果你经常访问网页，那还需要运行一个好用的反间谍软件和反恶意软件程序，如Spybot。许多网站会利用Microsoft Explorer的弱点和安全漏洞，在不知不觉的情况下将恶意代码植入到电脑里，发现时为时已晚！

**下载并安装防火墙。**ZoneAlarm[[7]](https://zh.wikihow.com/%E4%BF%9D%E6%8A%A4%E7%94%B5%E8%84%91%E7%9A%84%E5%AE%89%E5%85%A8" \l "_note-7) 或Comodo Firewall[[8]](https://zh.wikihow.com/%E4%BF%9D%E6%8A%A4%E7%94%B5%E8%84%91%E7%9A%84%E5%AE%89%E5%85%A8" \l "_note-8) （Kerio、WinRoute或者带iptables 的Linux）。如果你使用路由器，可以把它当成硬件防火墙来增加安全性。

# Ref

V2计算机取证