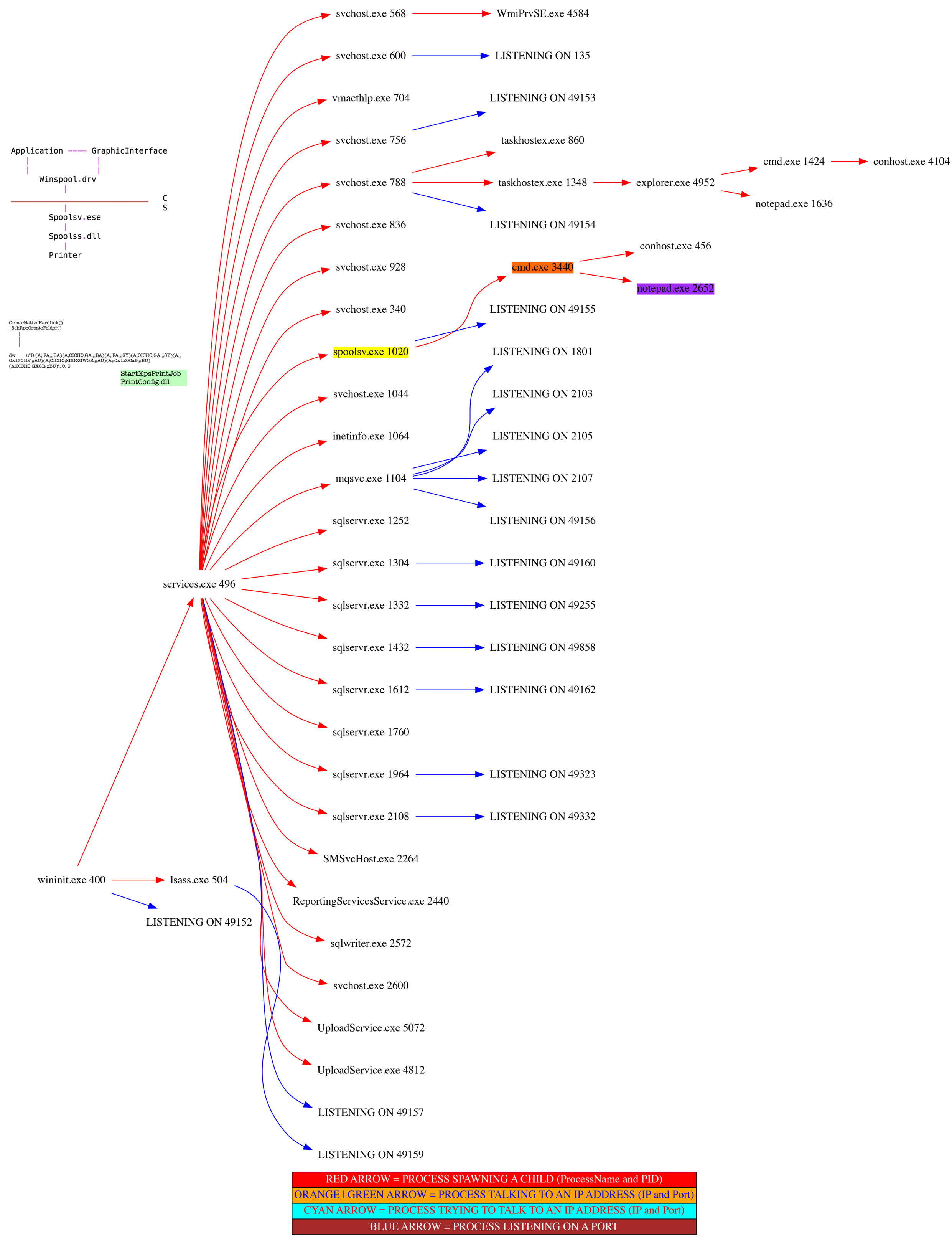
Application ---- GraphicInterface
Winspool.drv
C
S
Spoolsv.ese
Spoolss.dll
Printer
CreateNativeHardlink()
_SchRpcCreateFolder()
dw u"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x13301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;;0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)", 0, 0
StartXpsPrintJob
PrintConfig.dll
svchost.exe 568
WmiPrvSE.exe 4584
svchost.exe 600
LISTENING ON 135
vmacthlp.exe 704
LISTENING ON 49153
svchost.exe 756
taskhostex.exe 860
svchost.exe 788
taskhostex.exe 1348
explorer.exe 4952
cmd.exe 1424
conhost.exe 4104
notepad.exe 1636
LISTENING ON 49154
svchost.exe 836
svchost.exe 928
cmd.exe 3440
conhost.exe 456
notepad.exe 2652
svchost.exe 340
LISTENING ON 49155
spoolsv.exe 1020
LISTENING ON 1801
svchost.exe 1044
LISTENING ON 2103
inetinfo.exe 1064
LISTENING ON 2105
mqsvc.exe 1104
LISTENING ON 2107
sqlservr.exe 1252
LISTENING ON 49156
sqlservr.exe 1304
LISTENING ON 49160
services.exe 496
sqlservr.exe 1332
LISTENING ON 49255
sqlservr.exe 1432
LISTENING ON 49858
sqlservr.exe 1612
LISTENING ON 49162
sqlservr.exe 1760
sqlservr.exe 1964
LISTENING ON 49323
sqlservr.exe 2108
LISTENING ON 49332
SMSvcHost.exe 2264
wininit.exe 400
lsass.exe 504
LISTENING ON 49152
ReportingServicesService.exe 2440
sqlwriter.exe 2572
svchost.exe 2600
UploadService.exe 5072
UploadService.exe 4812
LISTENING ON 49157
LISTENING ON 49159
RED ARROW = PROCESS SPAWNING A CHILD (ProcessName and PID)
ORANGE | GREEN ARROW = PROCESS TALKING TO AN IP ADDRESS (IP and Port)
CYAN ARROW = PROCESS TRYING TO TALK TO AN IP ADDRESS (IP and Port)
BLUE ARROW = PROCESS LISTENING ON A PORT