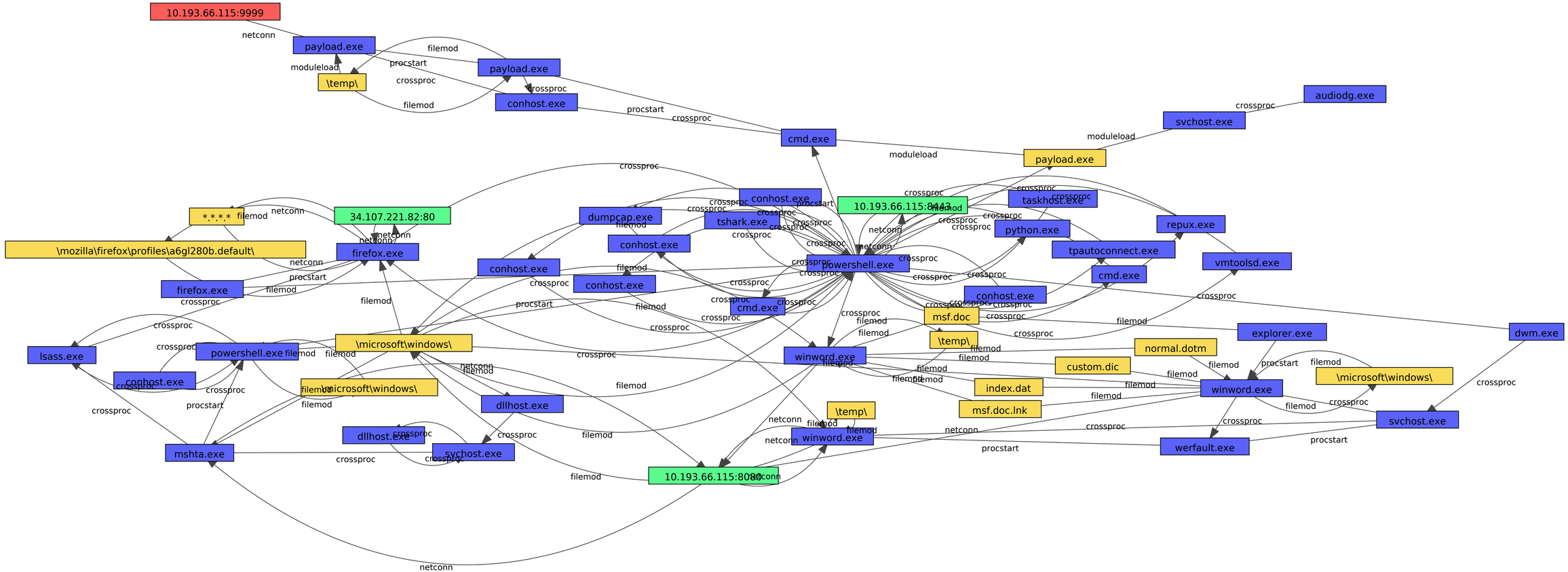
10.193.66.115:9999
netconn
payload.exe
filemod
moduleload
procstart
\temp\
crossproc
payload.exe
crossproc
conhost.exe
filemod
procstart
crossproc
cmd.exe
moduleload
payload.exe
moduleload
svchost.exe
crossproc
audiodg.exe
crossproc
..*.*
filemod
netconn
34.107.221.82:80
netconn
\mozilla\firefox\profiles\a6gl280b.default\
firefox.exe
netconn
firefox.exe
procstart
filemod
crossproc
filemod
conhost.exe
dumpcap.exe
filemod
tshark.exe
crossproc
conhost.exe
crossproc
conhost.exe
crossproc
conhost.exe
crossproc
cmd.exe
crossproc
powershell.exe
netconn
crossproc
10.193.66.115:8443
filemod
taskhost.exe
crossproc
python.exe
crossproc
repux.exe
tpautoconnect.exe
cmd.exe
vmtoolsd.exe
conhost.exe
crossproc
msf.doc
crossproc
filemod
crossproc
filemod
\temp\
filemod
normal.dotm
filemod
custom.dic
filemod
index.dat
filemod
msf.doc.lnk
filemod
winword.exe
filemod
filemod
filemod