Exécution de code à distance

5. Remote File Access

Ex. :`xcopy executabletorun.exe "\\REMOTECOMPUTERNAME\C$ \ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\e.exe"`

Writing to remote administrative shares using SMB. (`TCP port 139 or 445` owned by kernel)

6. Remote Desktop

Ex. : `rdesktop 1.2.3.4`

Hosted by the TermService service (“Remote Desktop Services”) in `svchost.exe` by a server socket listening on `TCP port 3389`.

7. Windows Remote Management

Ex. : `winrs -r:REMOTECOMPUTERNAME` command to run

Hosted by Windows Remote Management service (`svchost.exe`), listens on `TCP/80 or TCP/5985` and can share port with `IIS`

Récupération d'informations locales