Windows Process Genealogy

youtube.com/13cubed

```
                        System
                          |
                       smss.exe
      ┌───────────────────┼─────────────────────────┐
  csrss.exe[1]        wininit.exe[1]            winlogon.exe[1]
             ┌────────────┼────────────┐             |
        services.exe  lsaiso.exe[3]  lsass.exe    userinit.exe
             |                                        ┊
        svchost.exe                              explorer.exe[2]
       ┌─────┴─────┐
  runtimebroker.exe  taskhostw.exe
```
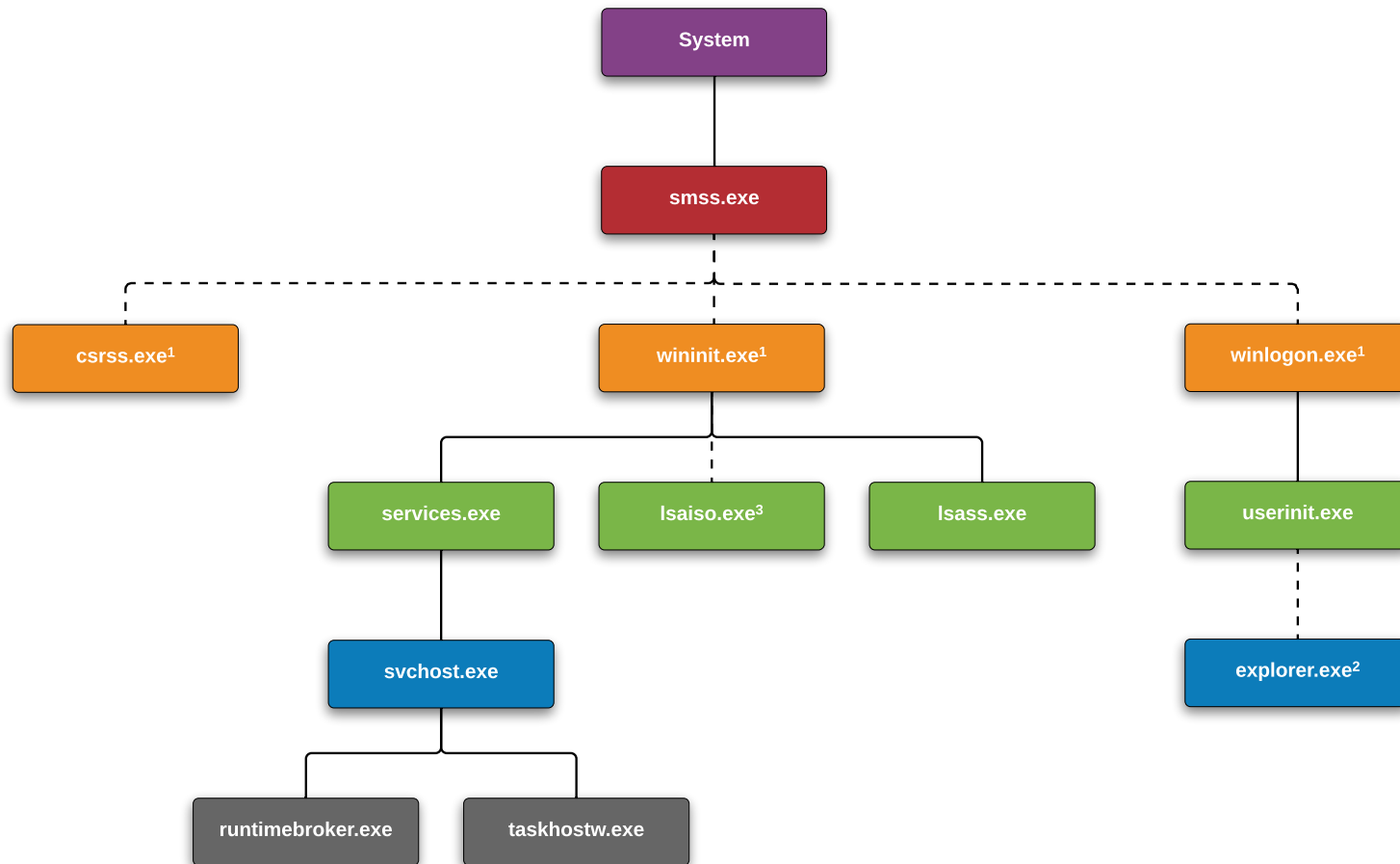
[1] Created by an instance of **smss.exe** that exits, so analysis tools usually do not provide the parent process name.

[2] Created by an instance of **userinit.exe** that exits, so analysis tools usually do not provide the parent process name.

[3] Present only when **Credential Guard** is enabled. Functionality of lsass.exe is split between itself and this process.