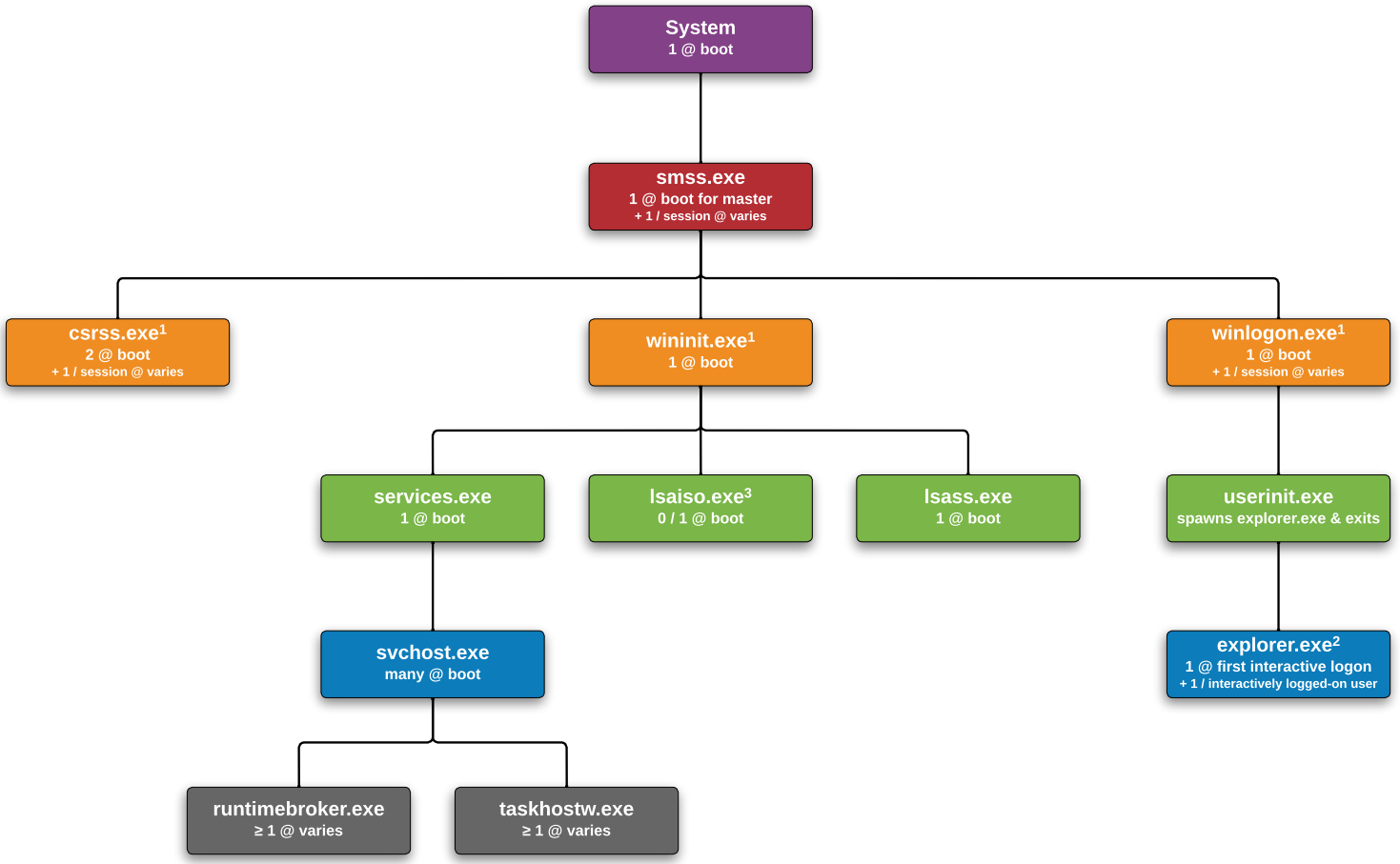
Version 2.2

Windows Process Genealogy

youtube.com/13cubed



Note: **Registry** and **MemCompression**, used for registry hive management and memory optimization respectively, are also child processes of **System**. Expect one of each at boot.

[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.