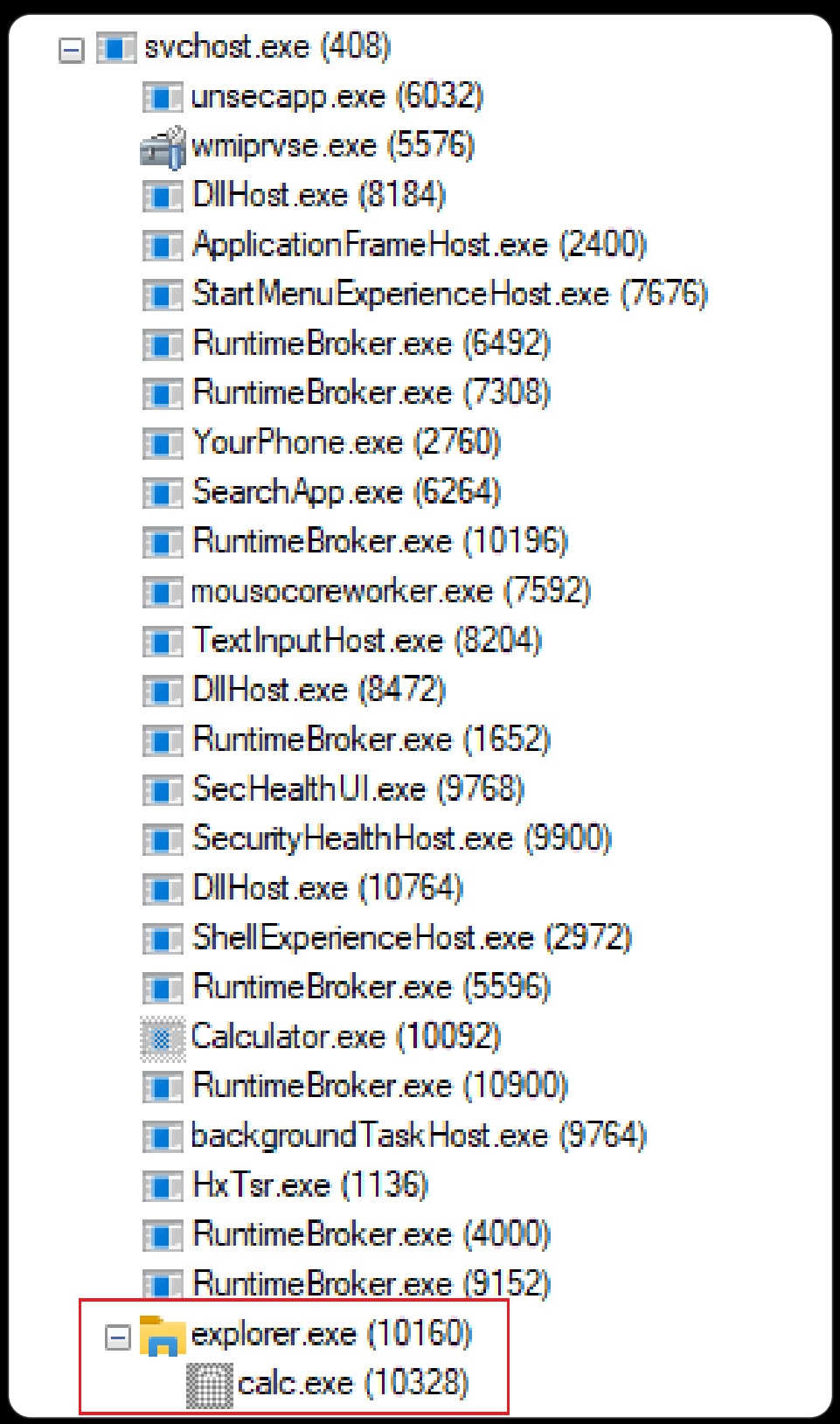
Nasreddine Bencherchali
@nas_bench

The payload is spawned from an explorer instance. Which in itself is spawned from svchost.exe.

The "explorer.exe" instance has the following command-line

explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding



8:06 PM · Jun 10, 2022

1 Repost **11** Likes **1** Bookmark