Assignment – 5

Name : Ishan Aakash Patel

Student ID : 146151238

Course : CYT-245

MITRE ATT&CK Navigator

I have selected the following two threat groups:

1) Bronze Butler : BRONZE BUTLER is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry

2) DragonFly: Dragonfly is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16. Active since at least 2010, Dragonfly has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.

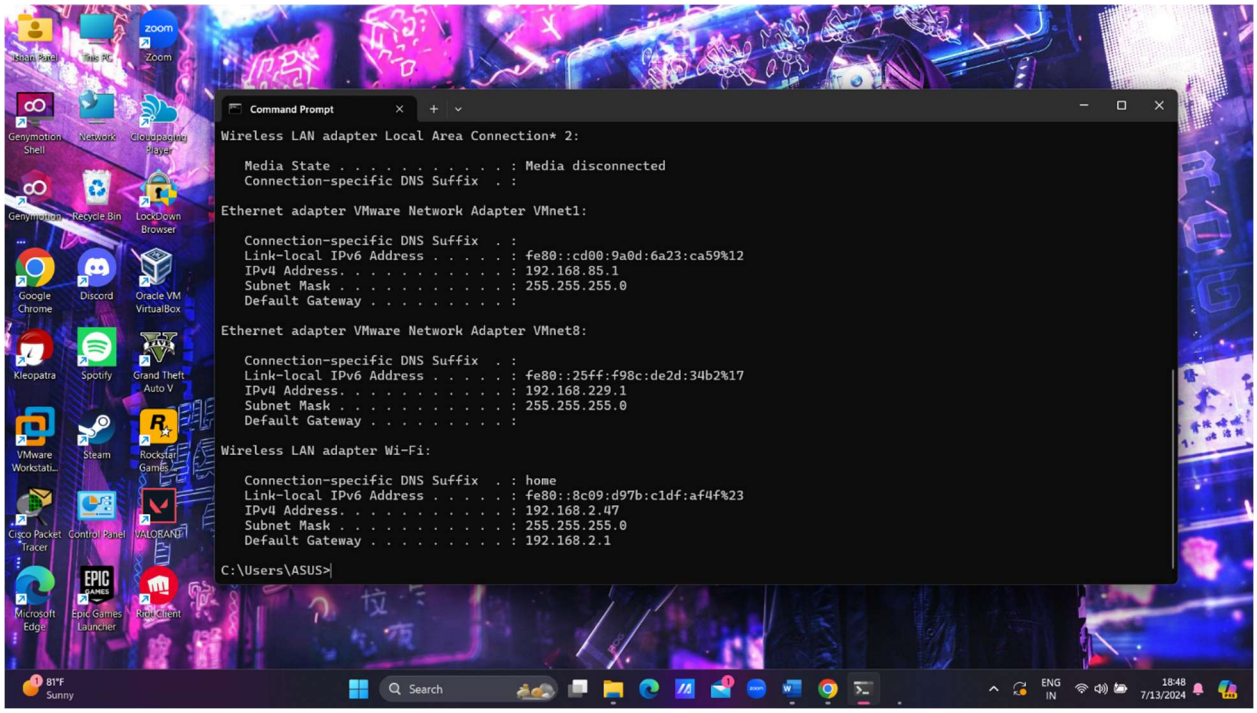

Figure 1: Screenshot zero

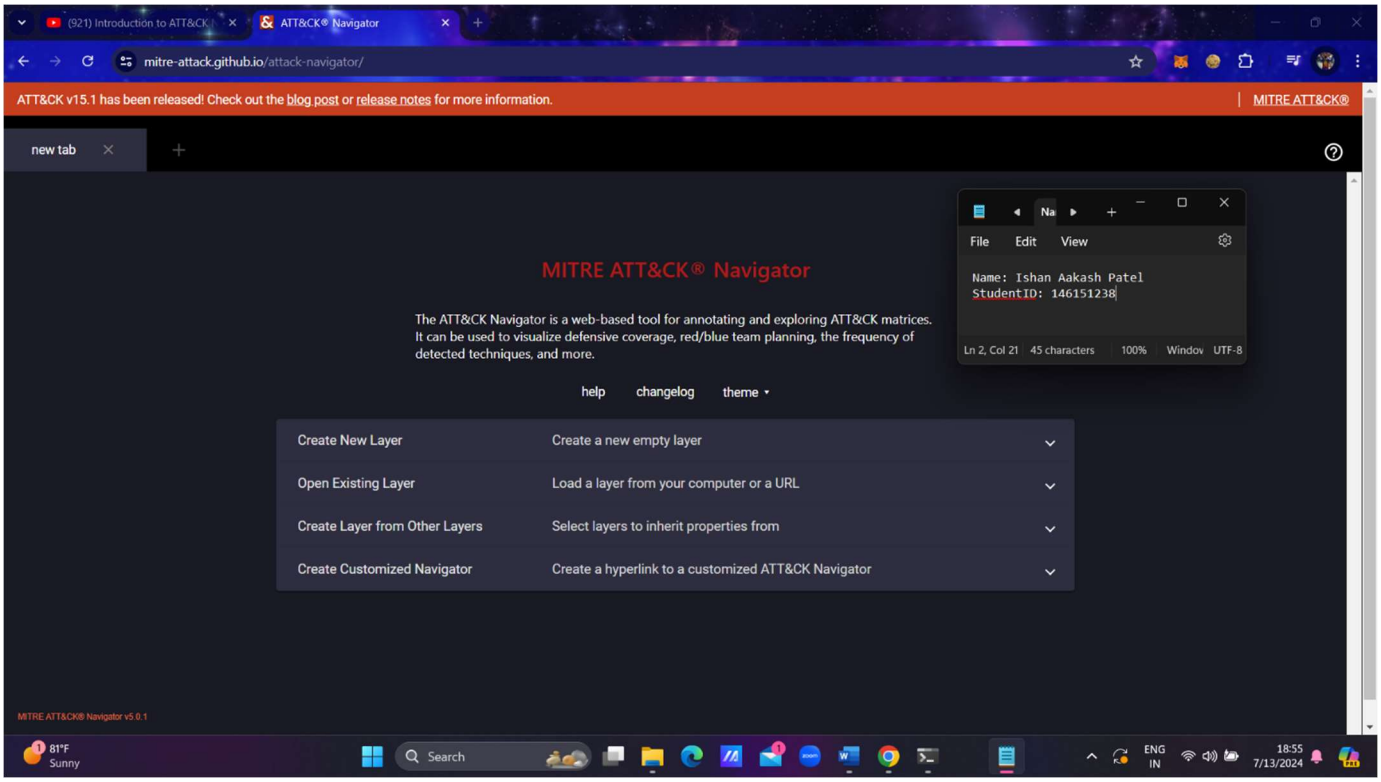

Figure 2: MITRE Attack Navigator

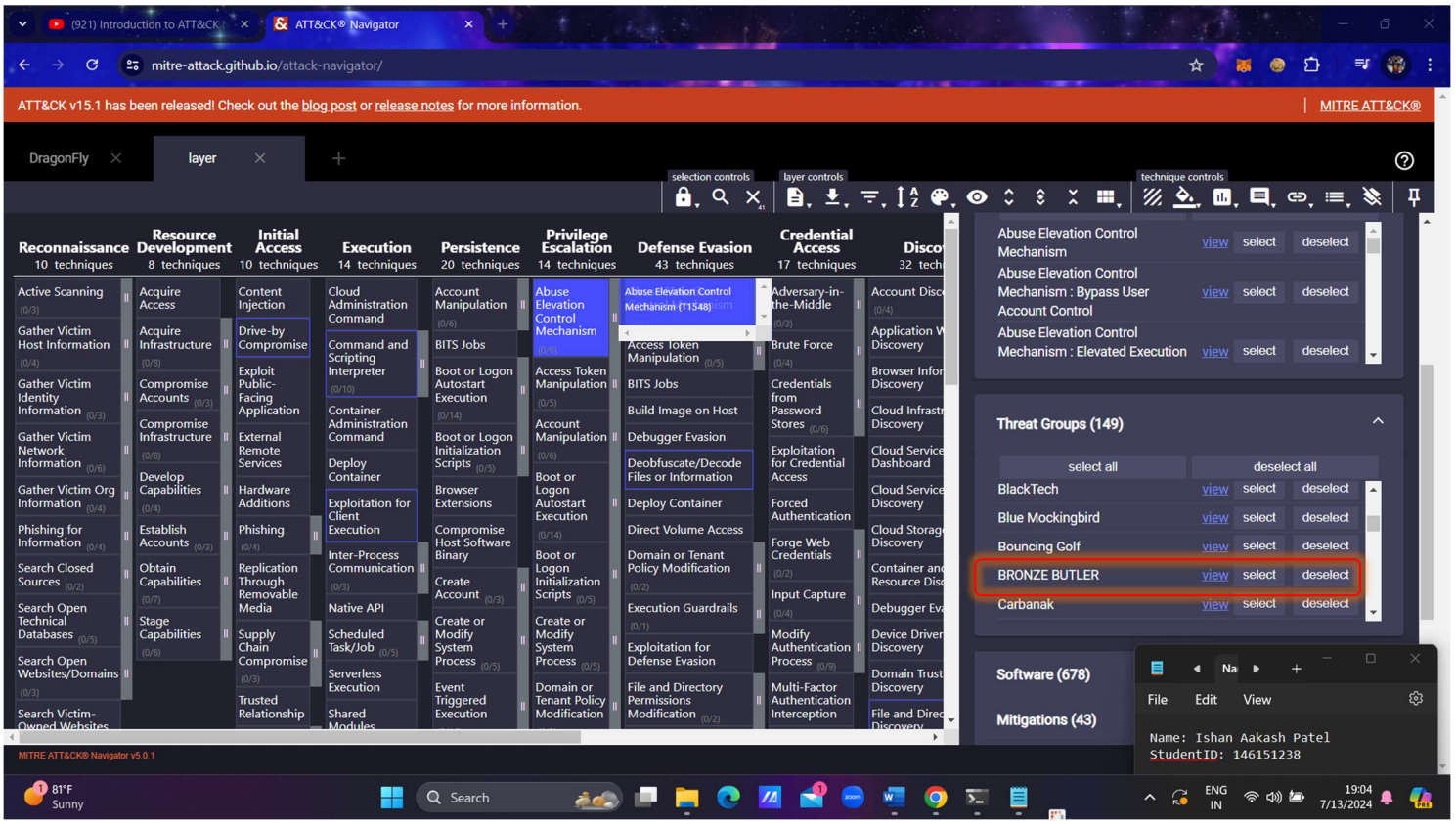

Figure 3 : Selecting 1st Threat Group (Bronze Butler)

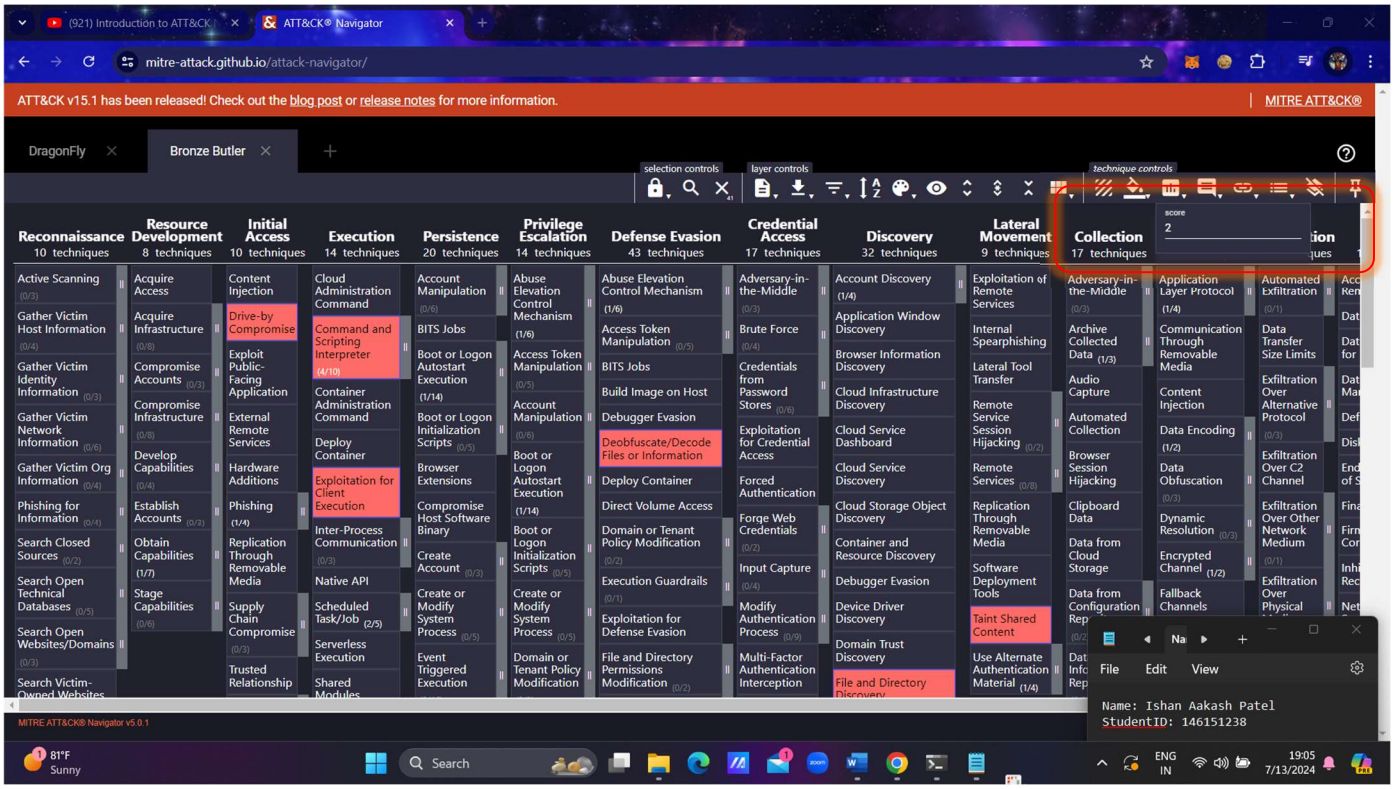

Figure 4 : Scoring the Threat Group (SCORE-2)

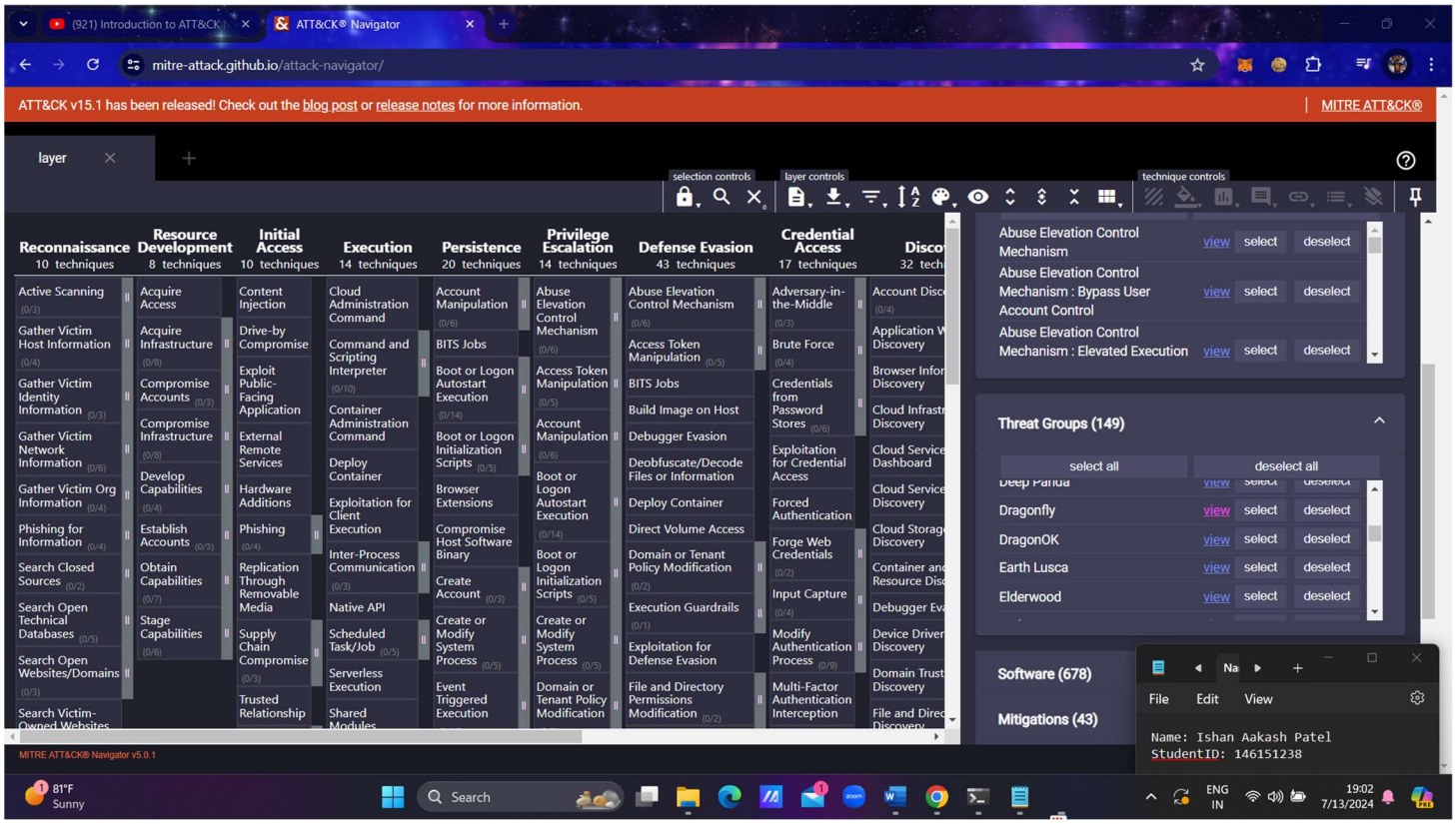

Figure 5 : Selecting the 2nd Threat Group (DragonFly)

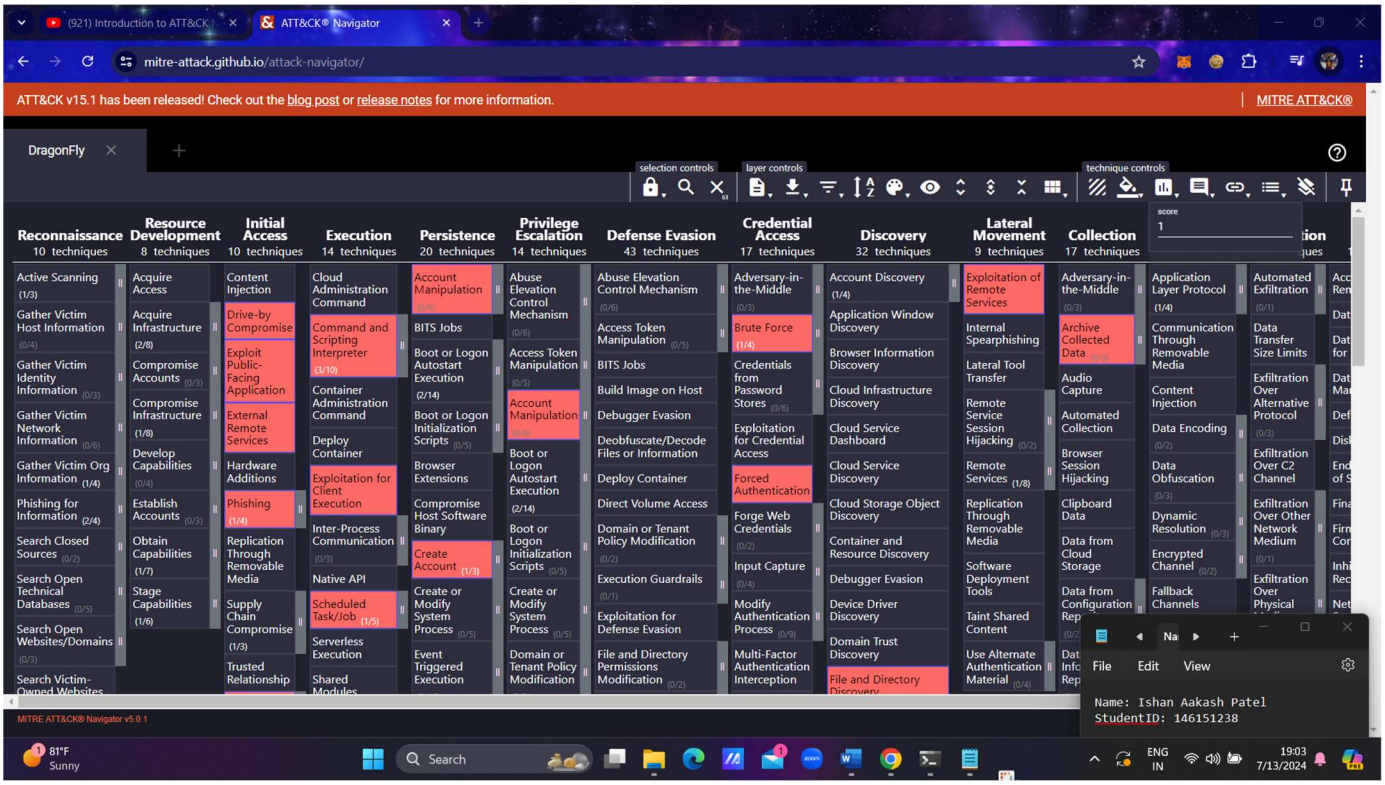

Figure 6 : Scoring DragonFly - 1

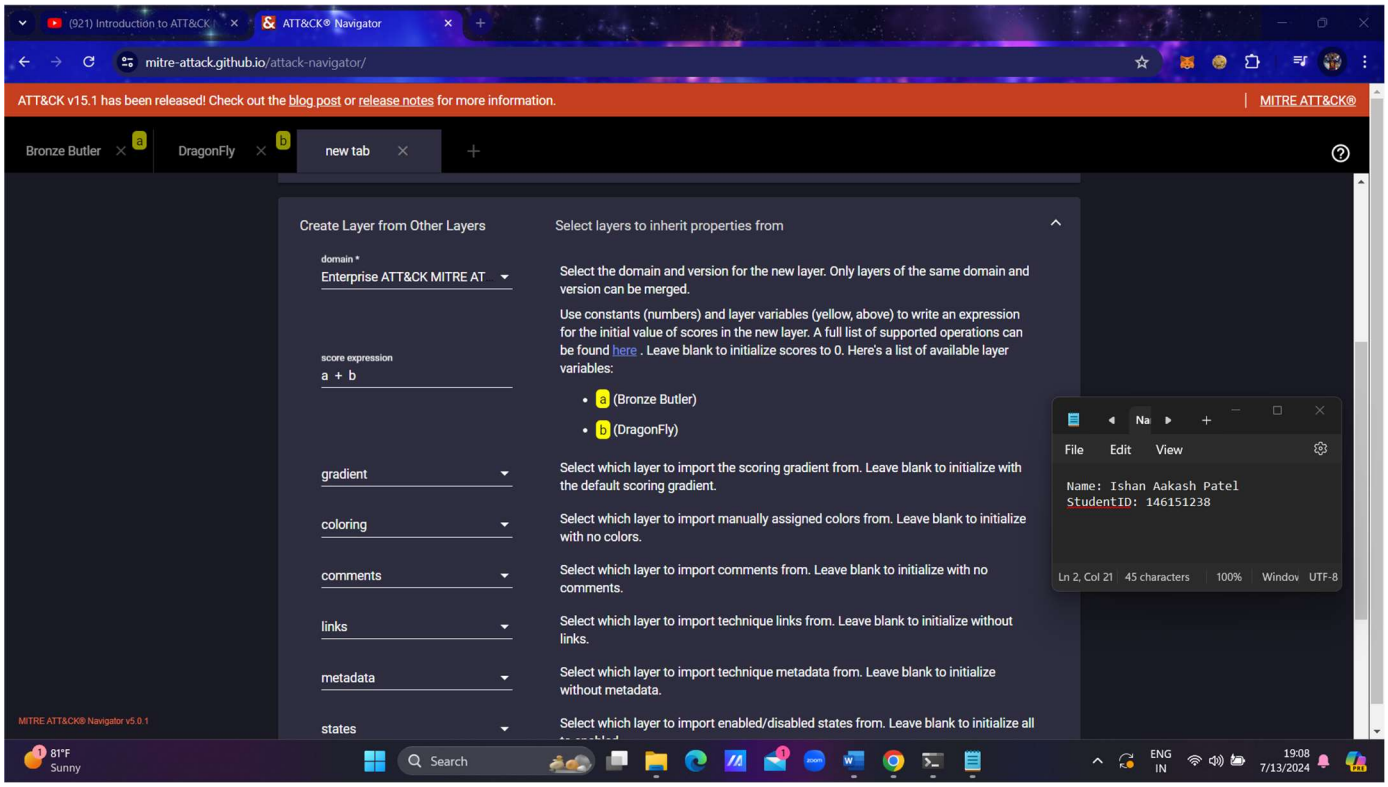

Figure 7 : Comparison between both Threat groups

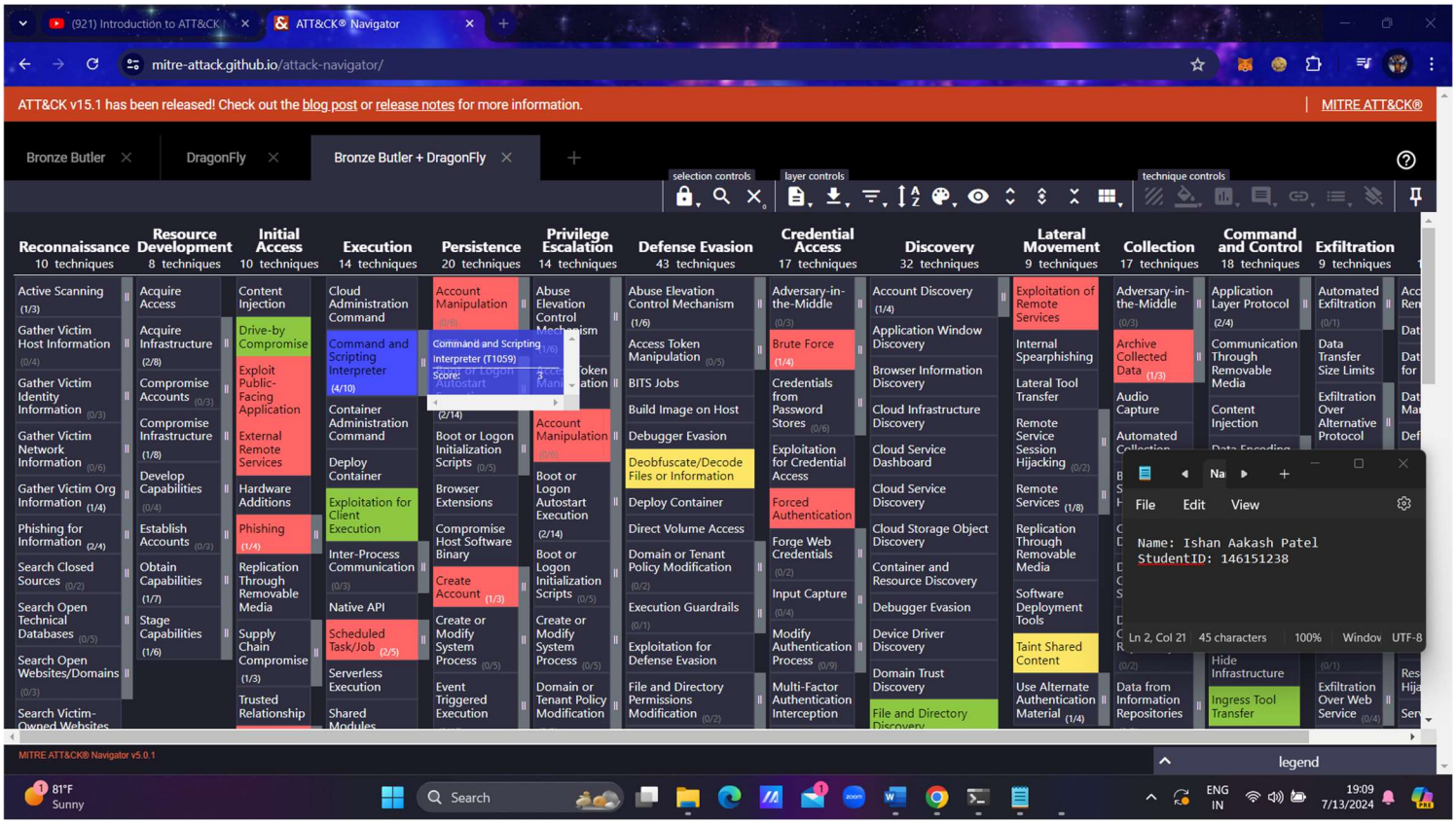

Figure 8 : Layer3 (Bronze Butler + DragonFly)

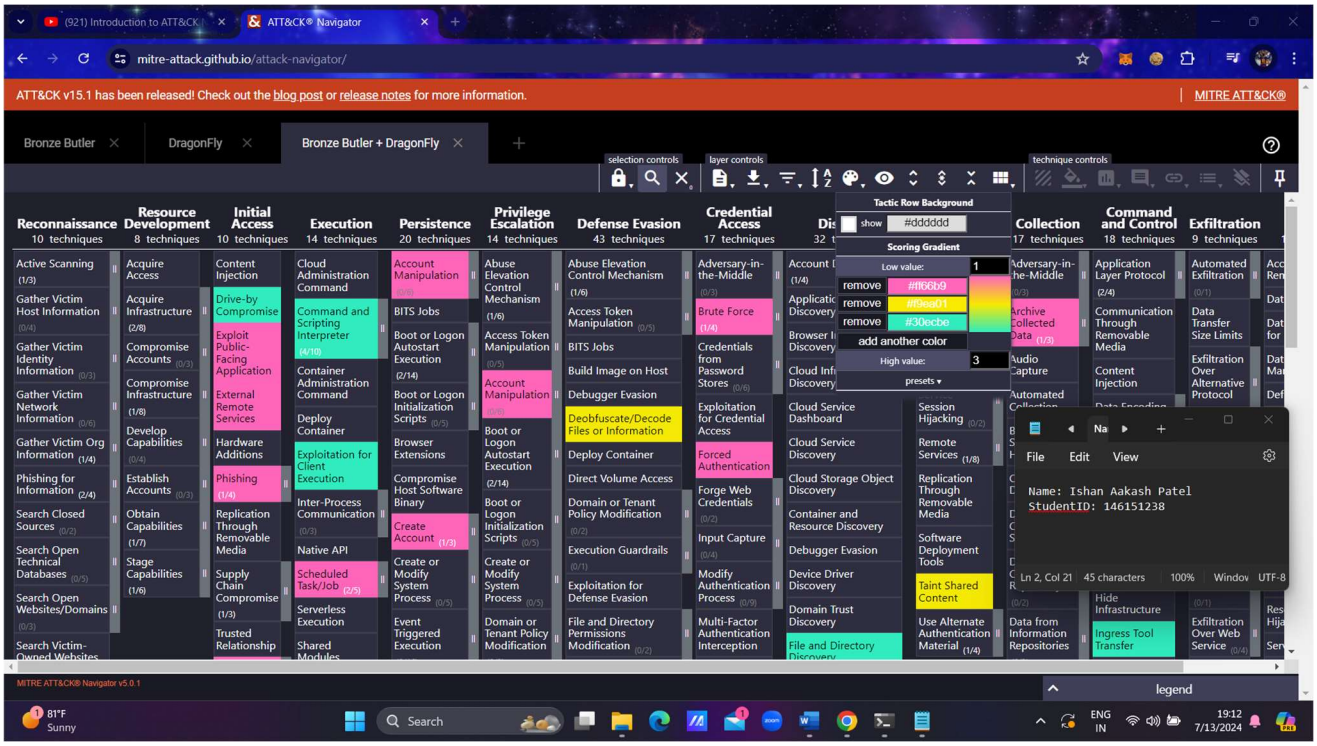

Figure 9 : Colouring the Score (1-3)

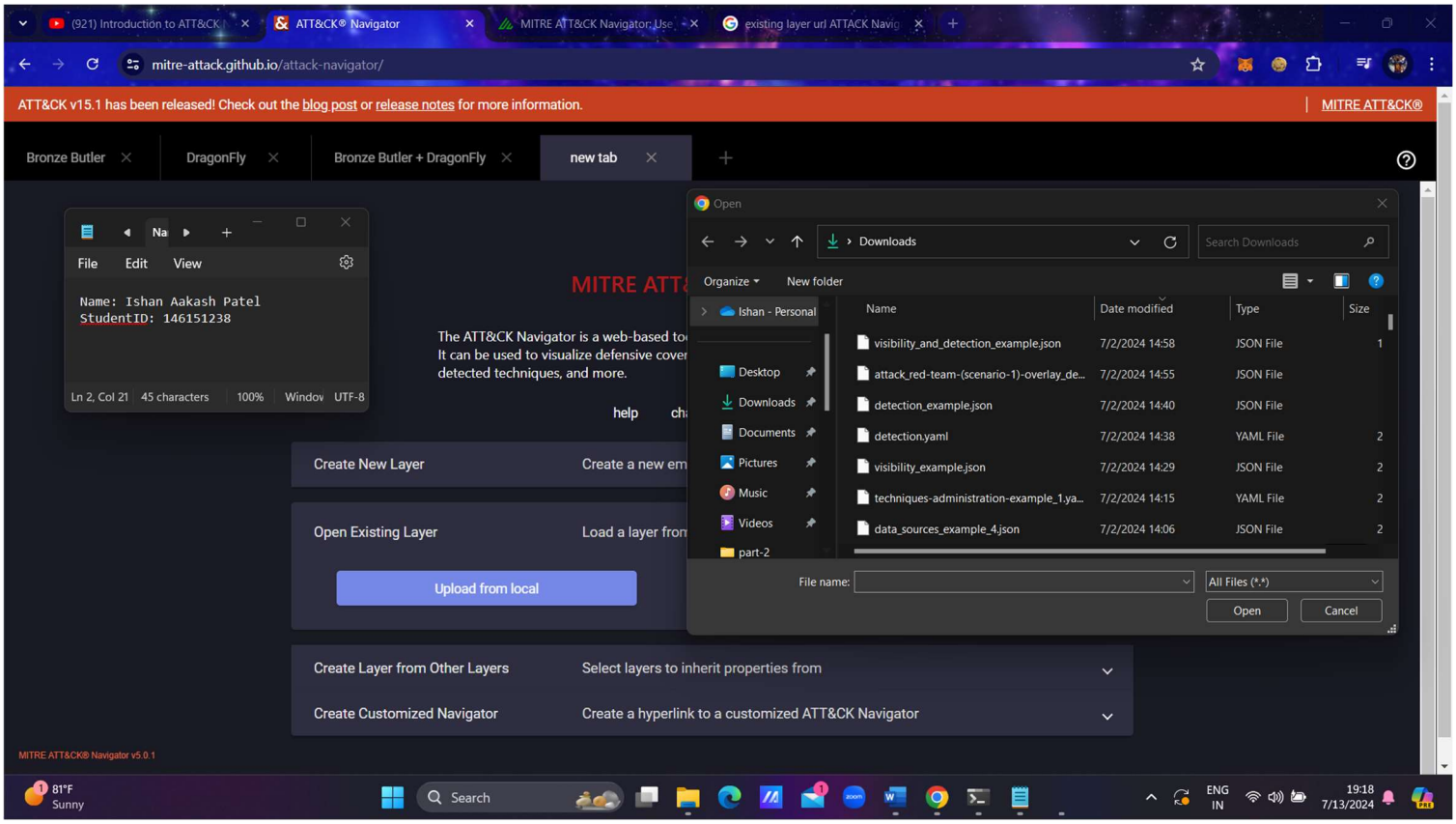

Figure 10 : Open an Existing Layer

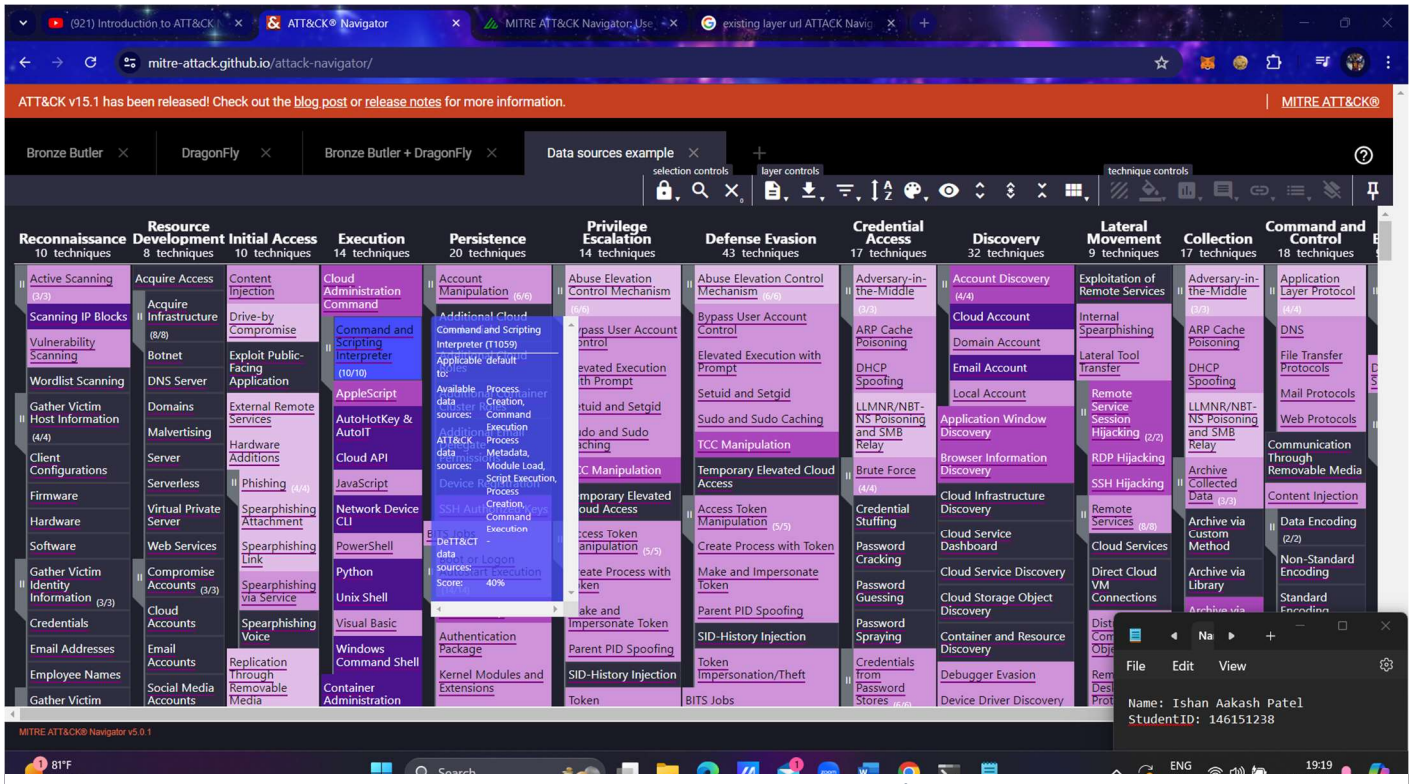

Figure 11 : Data-Sources Example