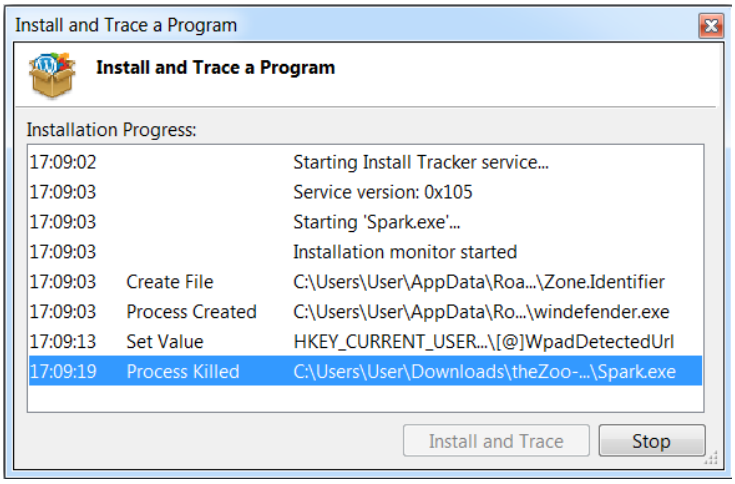
Lab № 1

Dynamic malware analysis

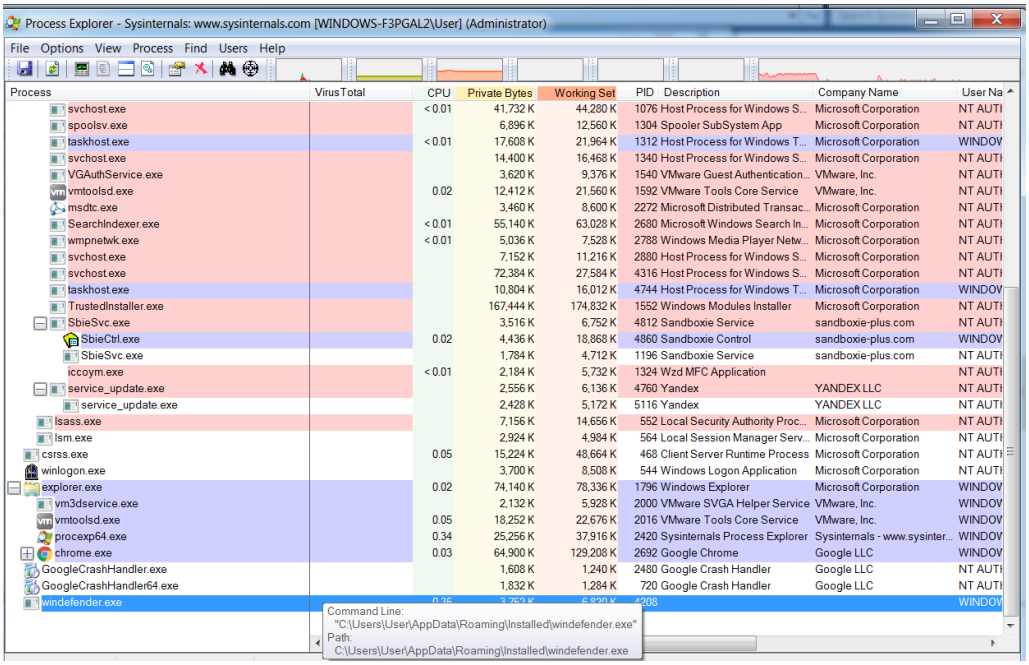
Sample 1: Alina Spark – PoS(point of sale)

Hash(SHA-1): 553d1afa824c34f348f8c53d1b043d3b671d946a

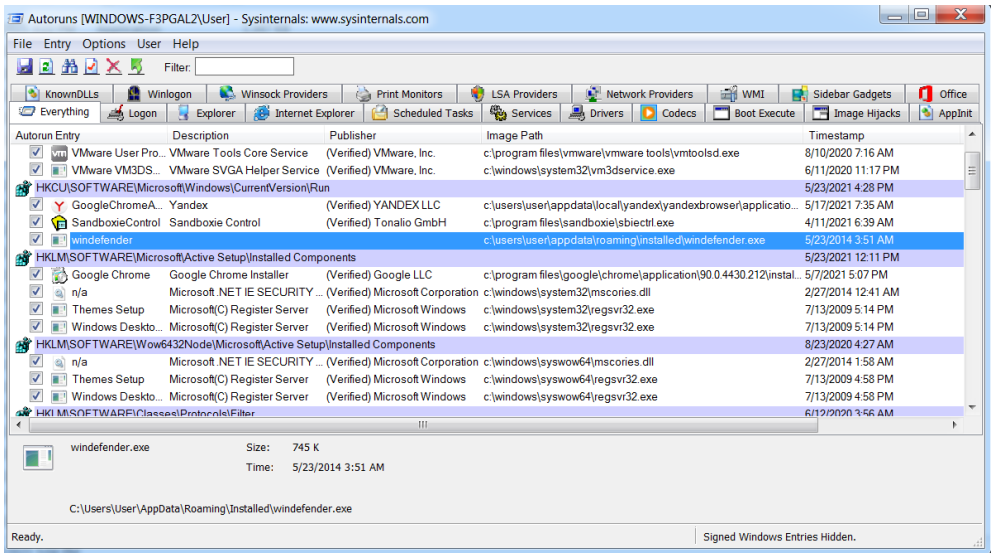
Running malware sample using Install&Trace shows steps completed by file during installation:



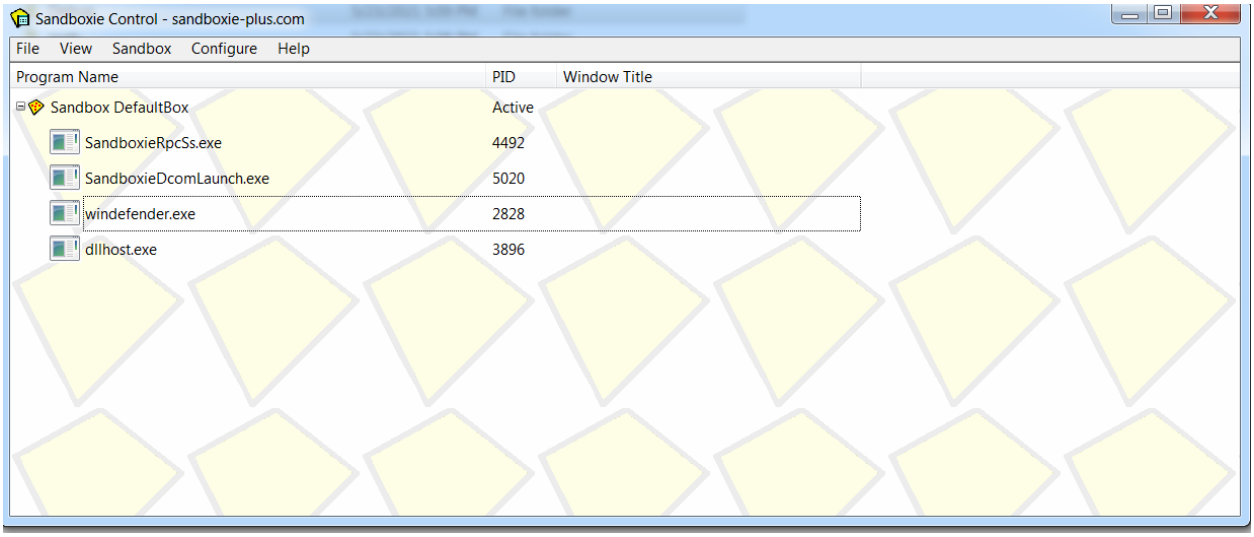
In "*Process Explorer*" window, we see file dropped running under the name "*windefender.exe*":



Dropped file also added to the *startup*:



Running into *sandboxie*:



Sample 2: Nullsoft self-extracting archive

Hash(SHA-1): 7a60598b33ca31627ab3767c6359ce81f8938785