Attribution

- Similar but different with another APT group “BlueMashroom”
  - same region
  - different ways of Execution & Persistence
    - hijacking shortcut file in startup paths
    - use regsvr32 to execute DLL