

## 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

目标类型: 应用程序  
目标位置: system32  
目标 (T): est\AppData\Local\dxdd11\_6.dll',DllEntry  
起始位置 (S): C:\Windows\system32  
快捷键 (O): 无  
运行方式 (U): 常规用户  
备注 (N):  
打开文件位置 (F) 更改图标 (C)... 高级 (A)...