

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): test\AppData\Local\dsd11_6.dll",DllEntry

起始位置 (S): C:\Windows\system32

快捷键 (O): 无

运行方式 (O): 常规窗口

备注 (O):

打开文件位置 (O)

更改图标 (C)...

高级 (O)...