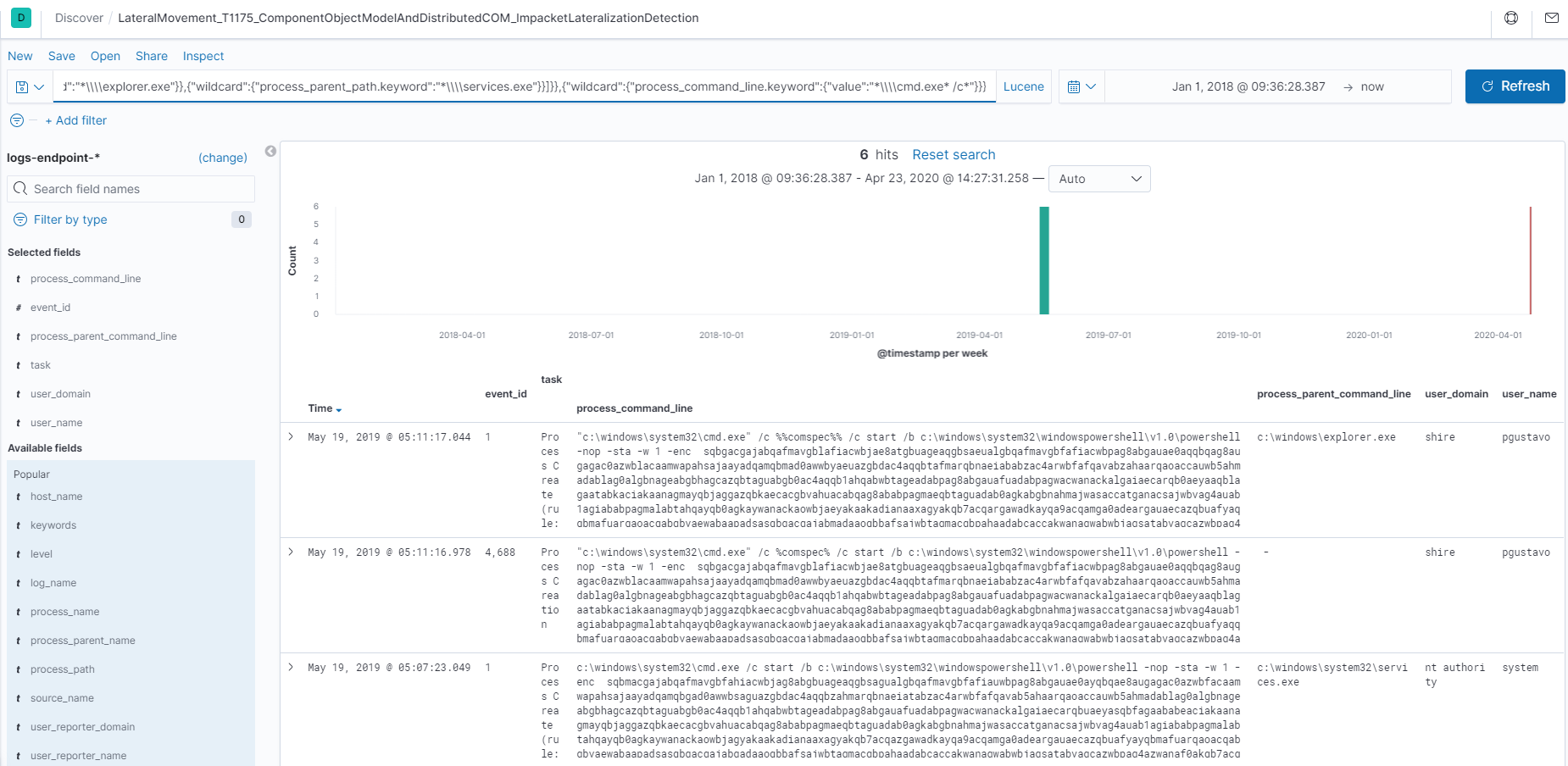
40.

此数据集表示攻击者通过在DCOM中的COM对象 MMC20.Application ，在远程主机上执行命令。



手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

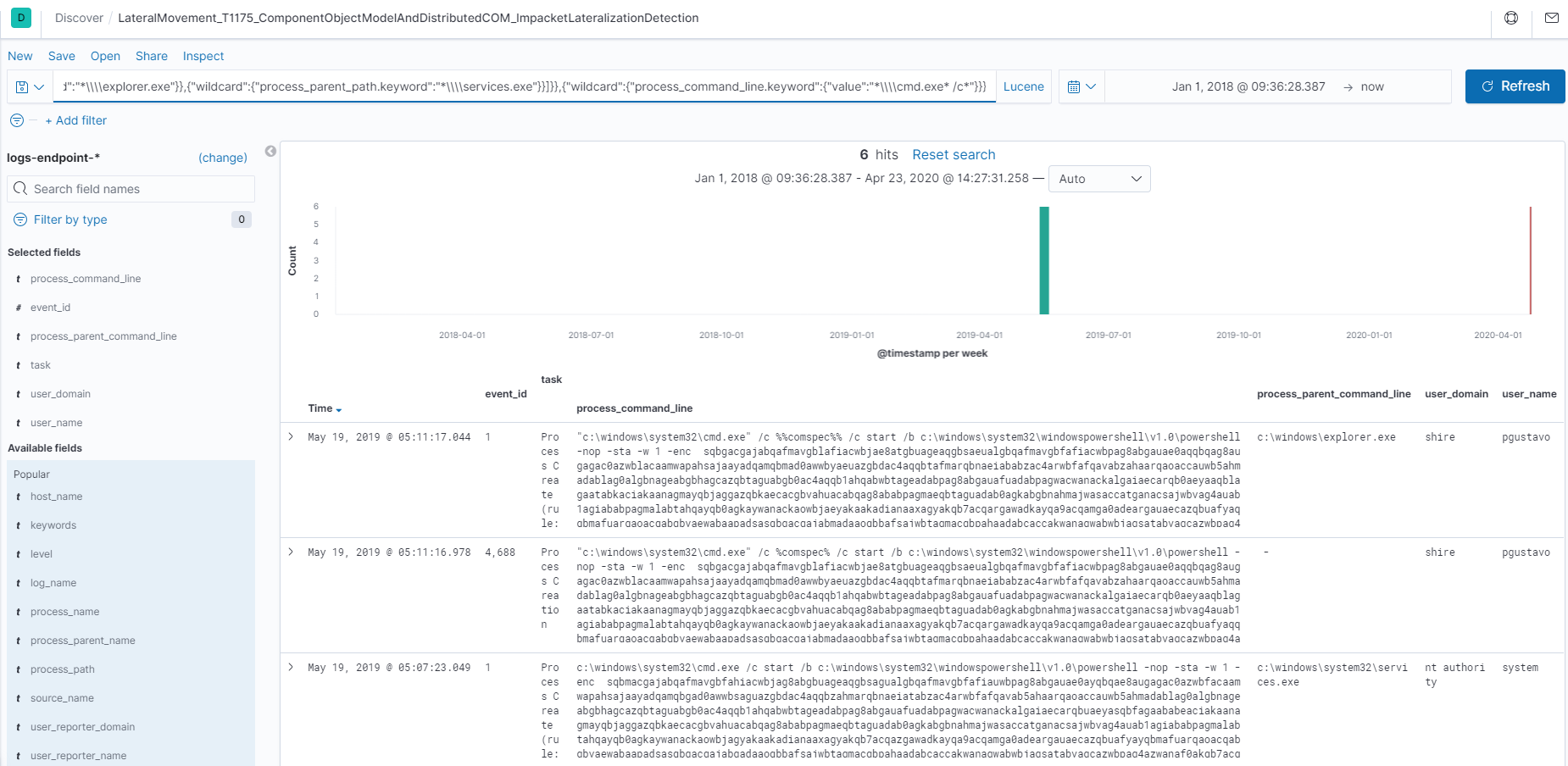
手机屏幕截图

描述已自动生成

LateralMovement\_T1175\_ComponentObjectModelAndDistributedCOM\_ImpacketLateralizationDetection

41.

此数据集表示攻击者执行 SMBExec 类型的命令，通过NTLMv2协议完成哈希身份验证。



手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

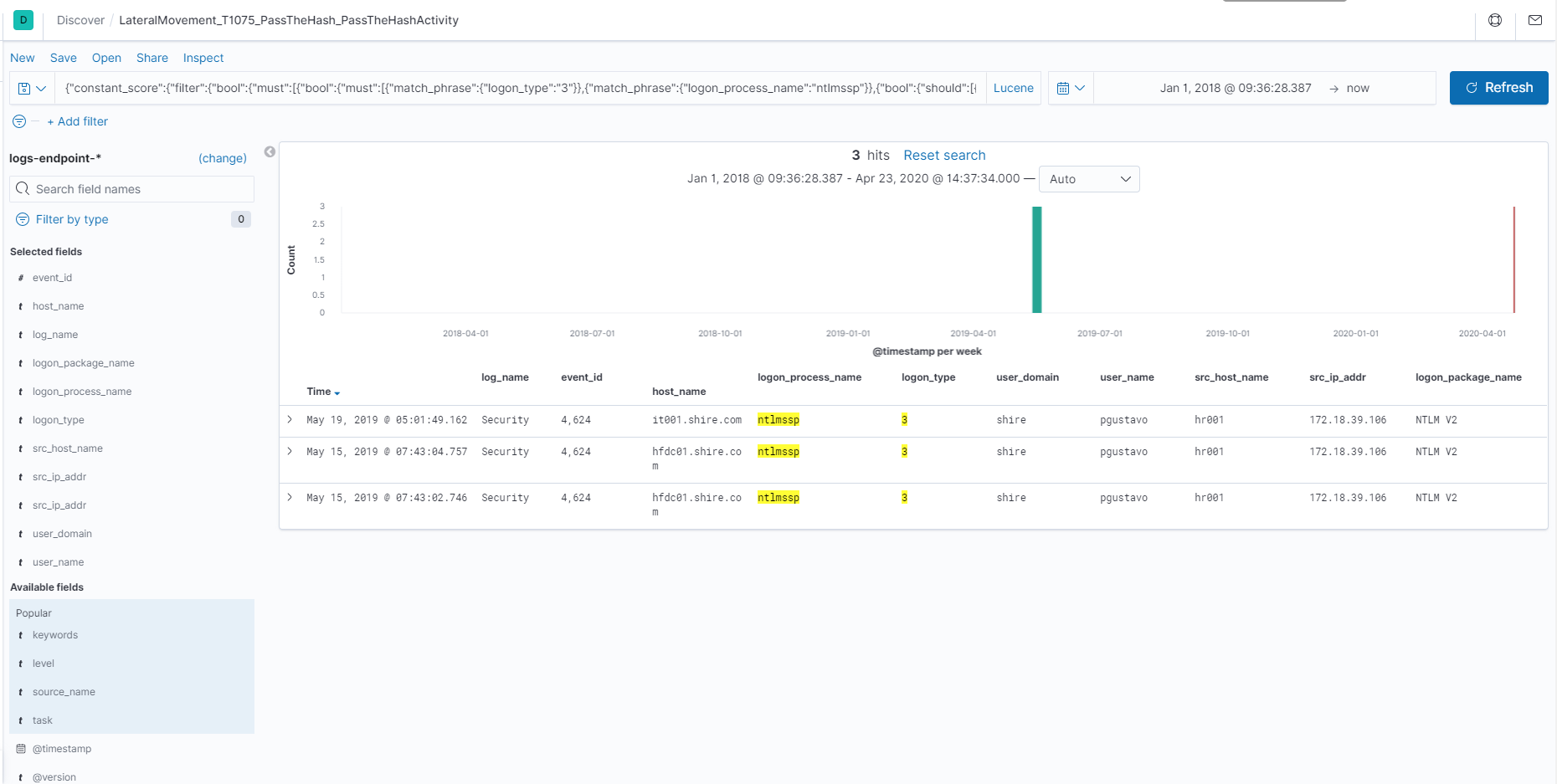
手机屏幕截图

描述已自动生成

LateralMovement\_T1175\_ComponentObjectModelAndDistributedCOM\_ImpacketLateralizationDetection

42.

此数据集表示攻击者执行 SMBExec 类型的命令，通过NTLMv2协议完成哈希身份验证。



手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

LateralMovement\_T1075\_PassTheHash\_PassTheHashActivity

43.

此数据集表示攻击者执行 SMBExec 类型的命令，通过NTLMv2协议完成哈希身份验证。

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

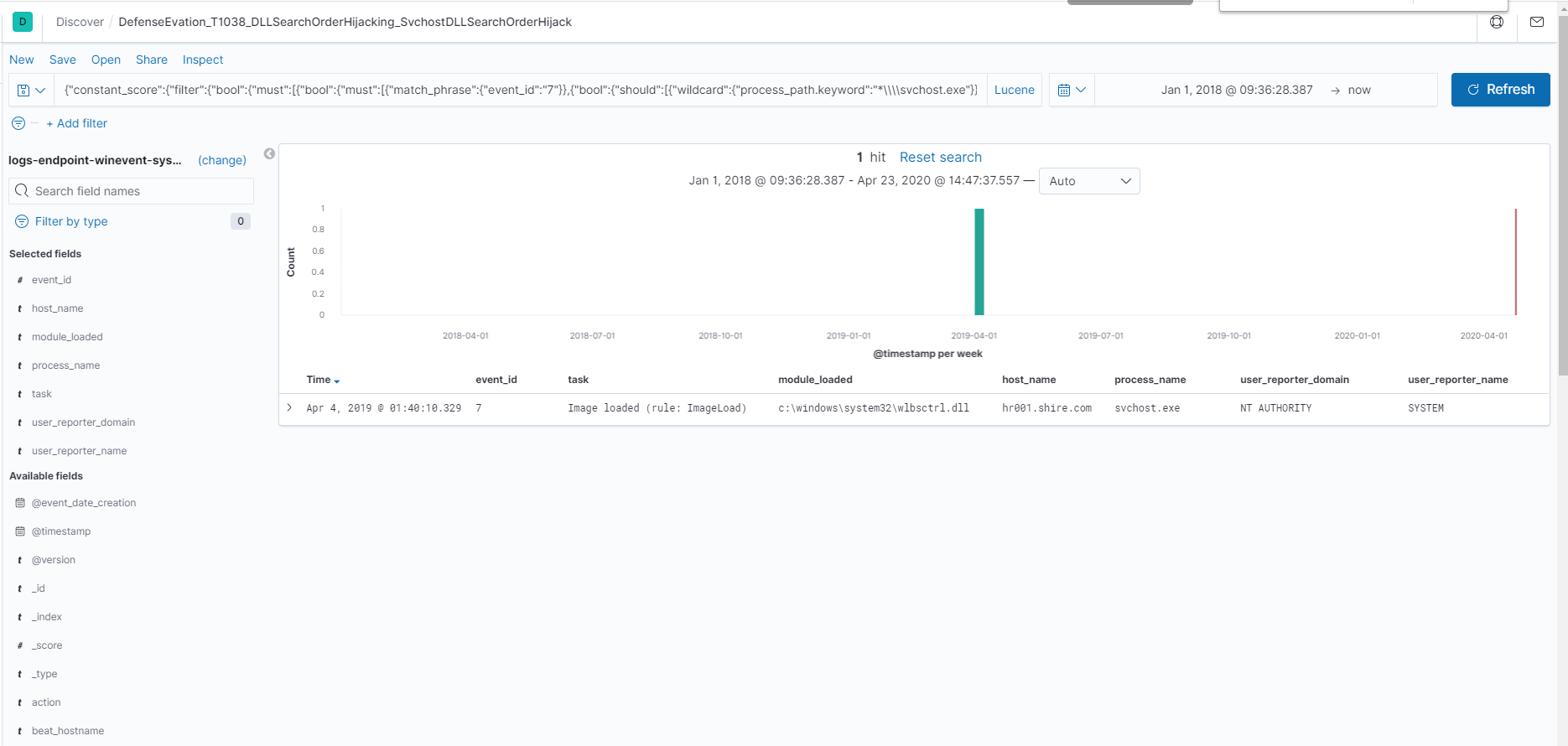
手机屏幕截图

描述已自动生成

LateralMovement\_T1075\_PassTheHash\_PassTheHashActivity2

44.

此数据集表示攻击者远程复制文件以替换由 IKEEXT 执行的 wlbsctrl.dll 文件（易受 DLL 劫持攻击）。



手机屏幕截图

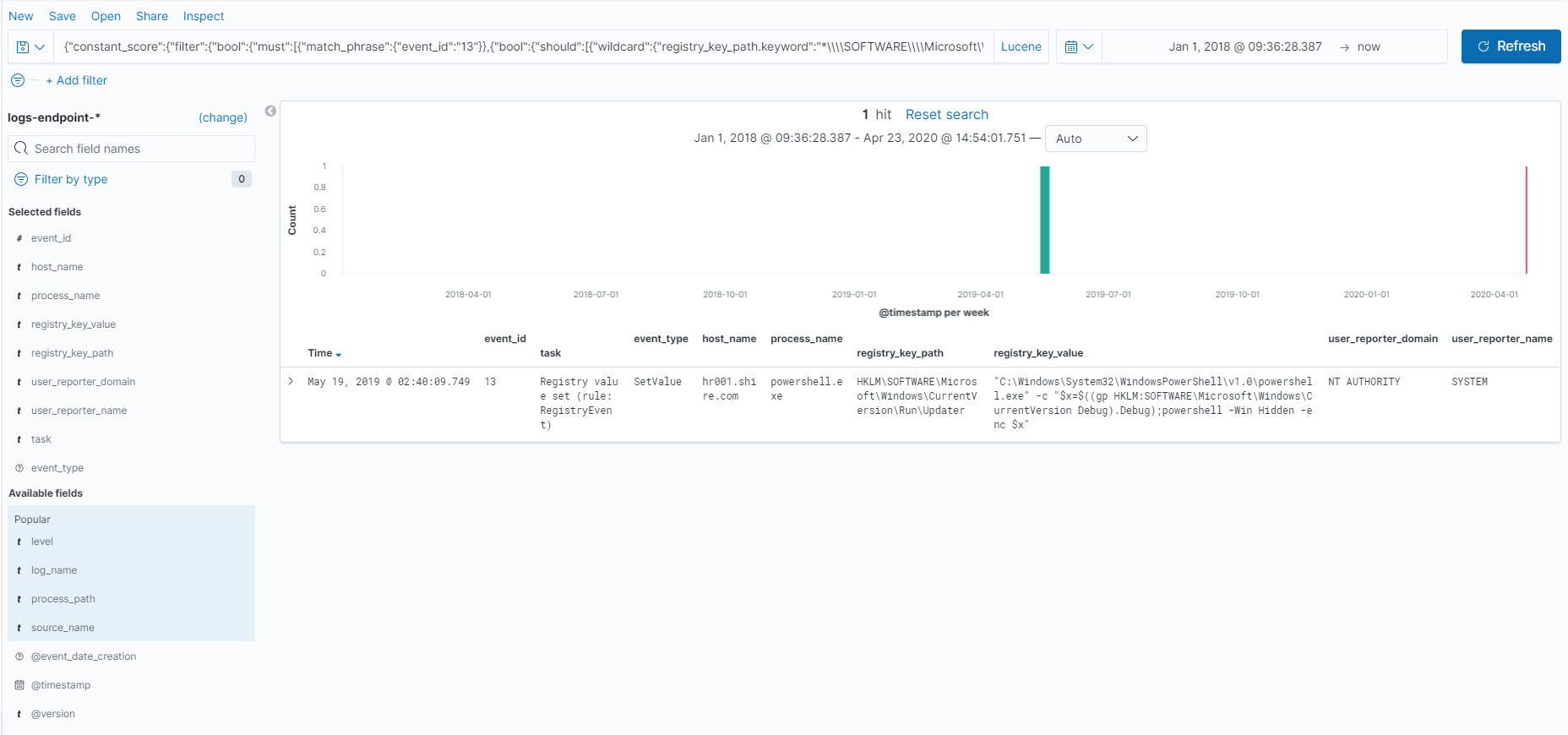
描述已自动生成

DefenseEvation\_T1038\_DLLSearchOrderHijacking\_SvchostDLLSearchOrderHijack

45.

Empire Elevated Registry

此数据集表示攻击者修改 HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Run注册表项以进行持久化。



手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成



Empire Userland Registry

此数据集表示攻击者修改 HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Run注册表项以进行持久化。

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成



Persistence\_T1060\_RegistryRunKeys/StartupFolder\_AutorunKeysModification

46.

此数据集表示攻击者创建计划任务从而在环境中进行持久化。

手机屏幕截图

描述已自动生成

手机屏幕截图

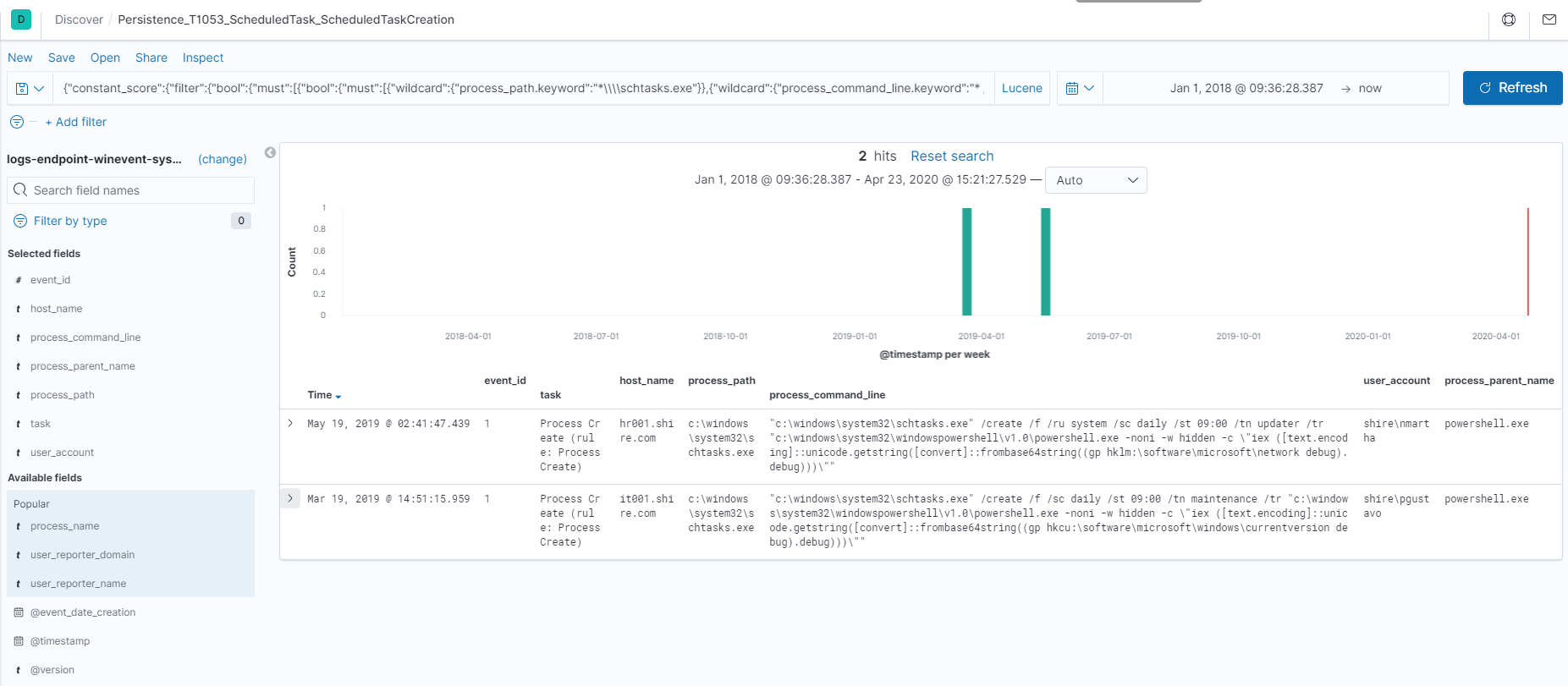
描述已自动生成

Persistence\_T1053\_ScheduledTask\_DefaultPowerSploitAndEmpireSchtasksPersistence

47.

Empire Elevated Scheduled Tasks

此数据集表示攻击者创建计划任务从而在环境中进行持久化。



手机屏幕截图

描述已自动生成

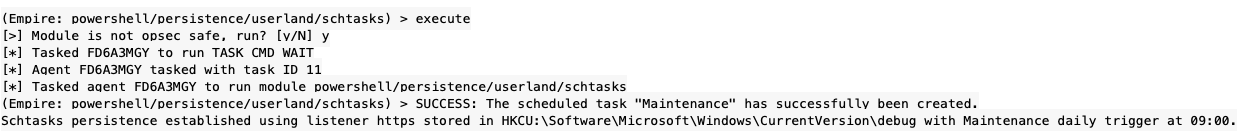
手机屏幕截图

描述已自动生成

Empire Userland Scheduled Tasks

手机屏幕截图

描述已自动生成



Persistence\_T1053\_ScheduledTask\_ScheduledTaskCreation