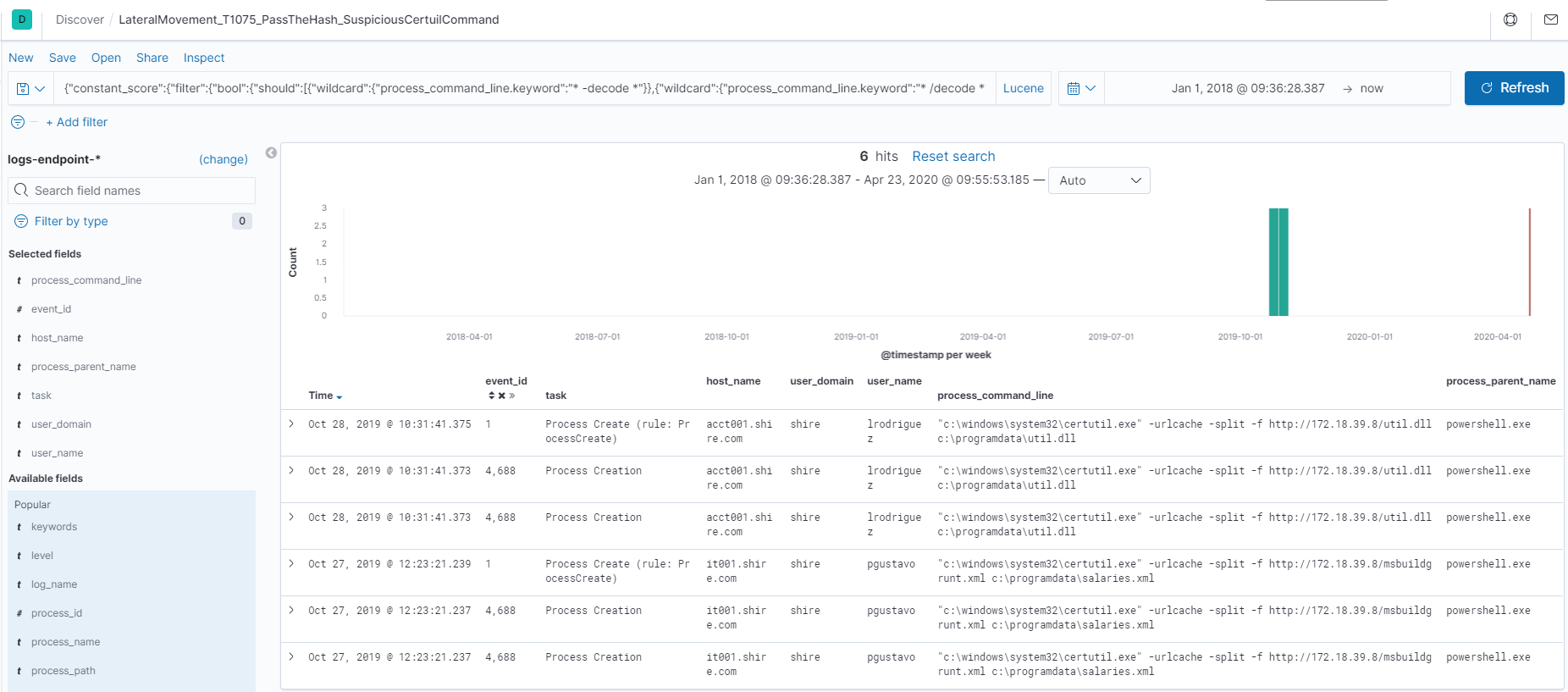
25.

此数据集表示攻击者通过受信任 Windows 实用程序 InstallUtil 代理执行代码。

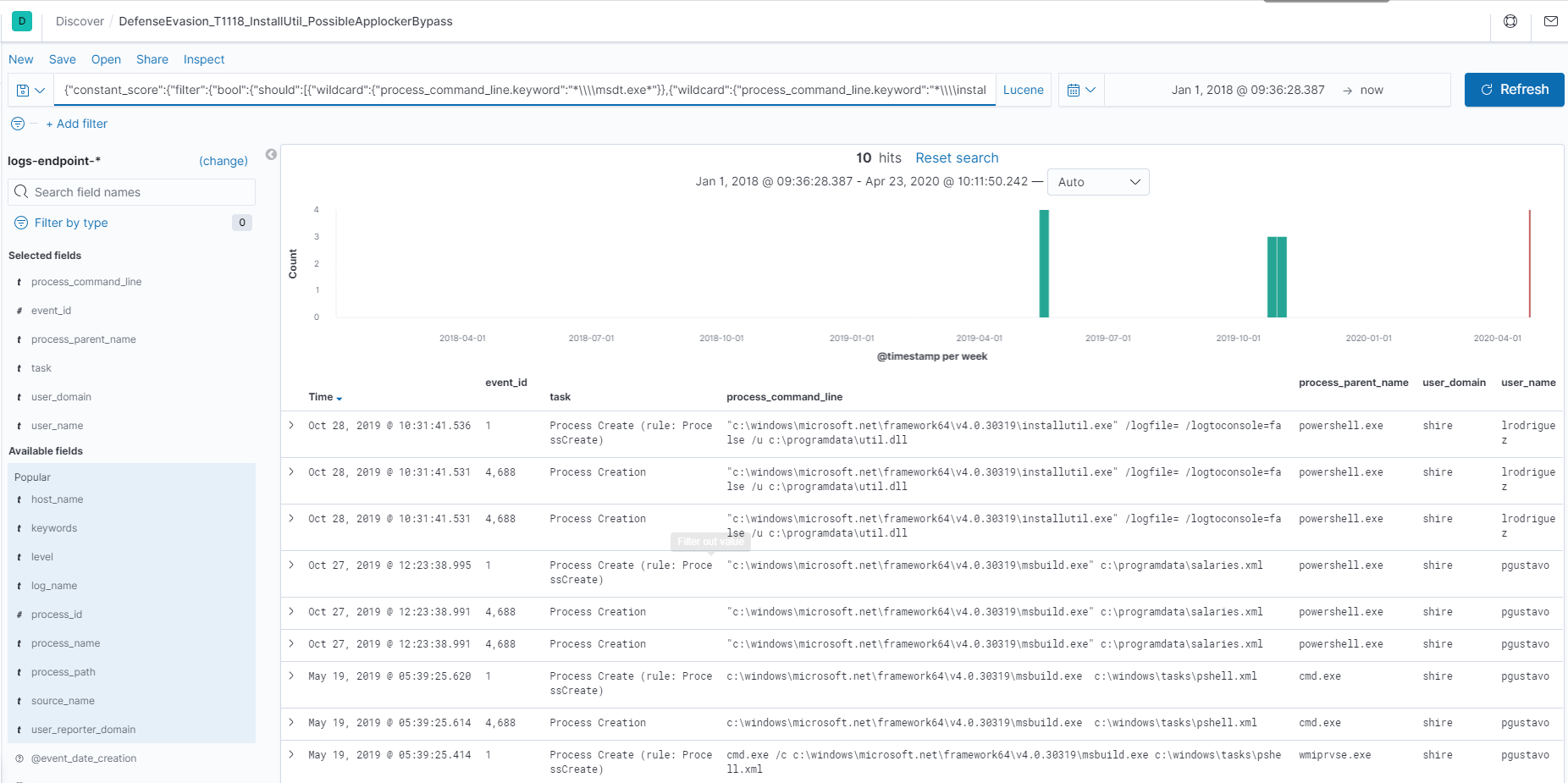




LateralMovement\_T1075\_PassTheHash\_SuspiciousCertuilCommand

26.

此数据集表示攻击者通过受信任 Windows 实用程序 InstallUtil 代理执行代码。

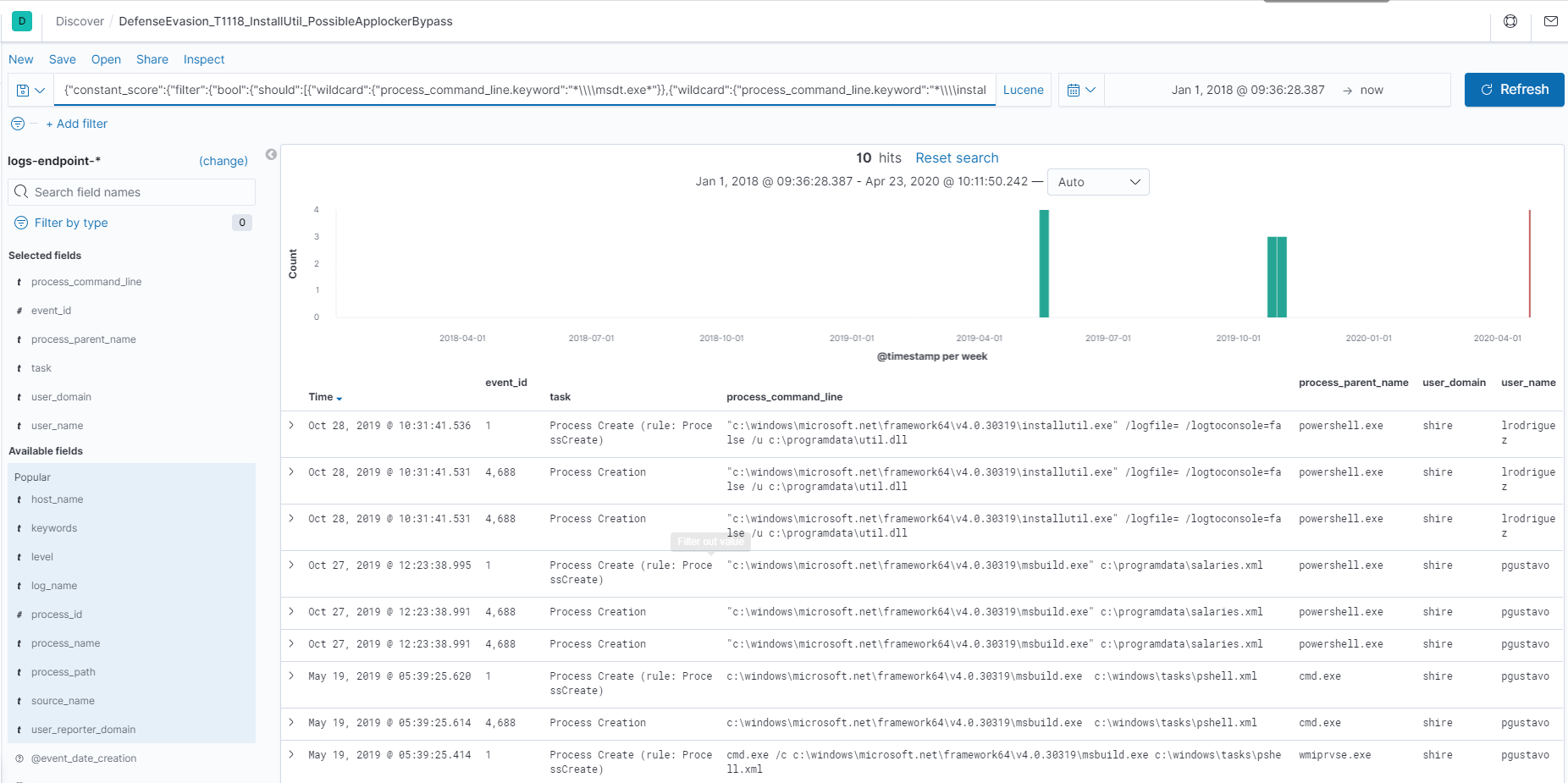




DefenseEvasion\_T1118\_InstallUtil\_PossibleApplockerBypass

27.

此数据集表示对手使用受信任的窗口实用程序（如 msbuild）对恶意代码的代理执行。

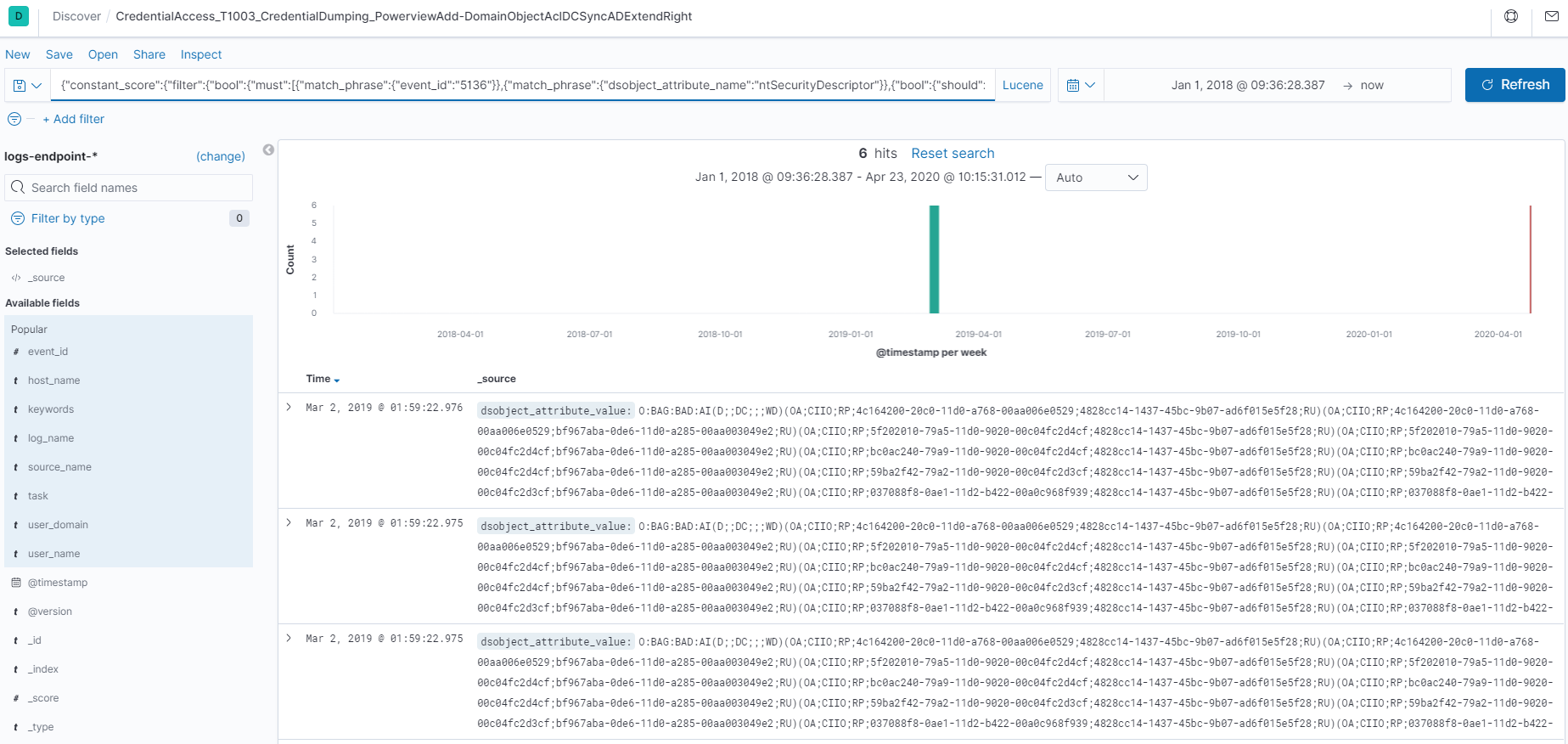




DefenseEvasion\_T1118\_InstallUtil\_PossibleApplockerBypass

28.

此数据集表示攻击者具有有限权限（例如域管理员）但可以为任何用户向根域添加 ACL，尽管该用户没有特权组，没有恶意 sidHistory，并且域控制器本身没有本地管理员权限。





scriptcmd $nmarthaSid = Get-DomainUser nmartha | Select-Object -ExpandProperty objectsid; Get-DomainObjectACL "dc=shire,dc=com" -Domain shire.com -ResolveGUIDs | Where-Object {$\_.securityidentifier -eq $nmarthaSid}

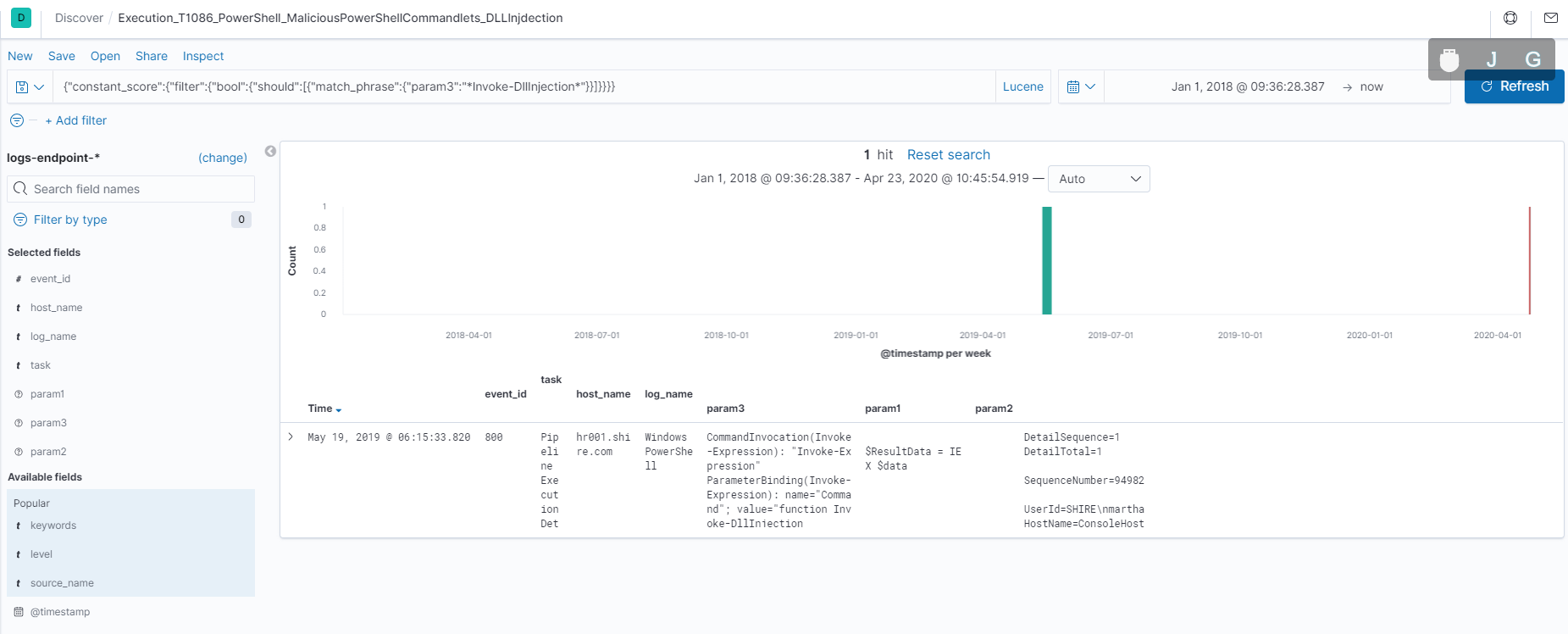
图片包含 文字, 游戏机

描述已自动生成

CredentialAccess\_T1003\_CredentialDumping\_PowerviewAdd-DomainObjectAclDCSyncADExtendRight

29.

此数据集表示攻击者将 Dll 注入任意进程。



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

图片包含 游戏机, 文字

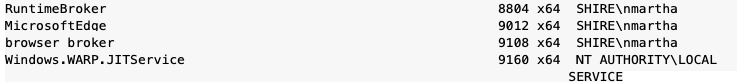
描述已自动生成

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



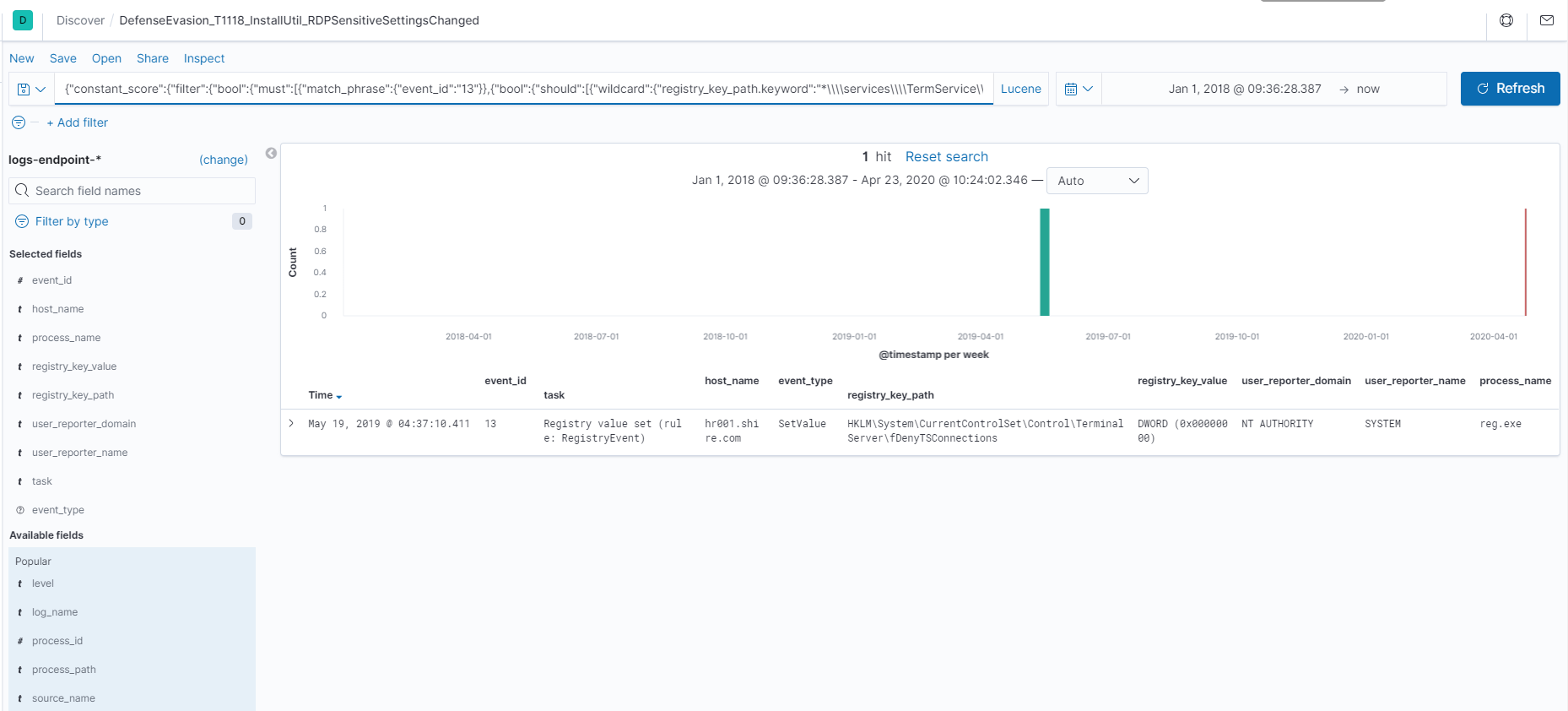
手机屏幕截图

描述已自动生成

Execution\_T1086\_PowerShell\_MaliciousPowerShellCommandlets\_DLLInjdection

30.

此数据集表示攻击者开启RDP并且打开一条被入侵主机上的防火墙放行策略。



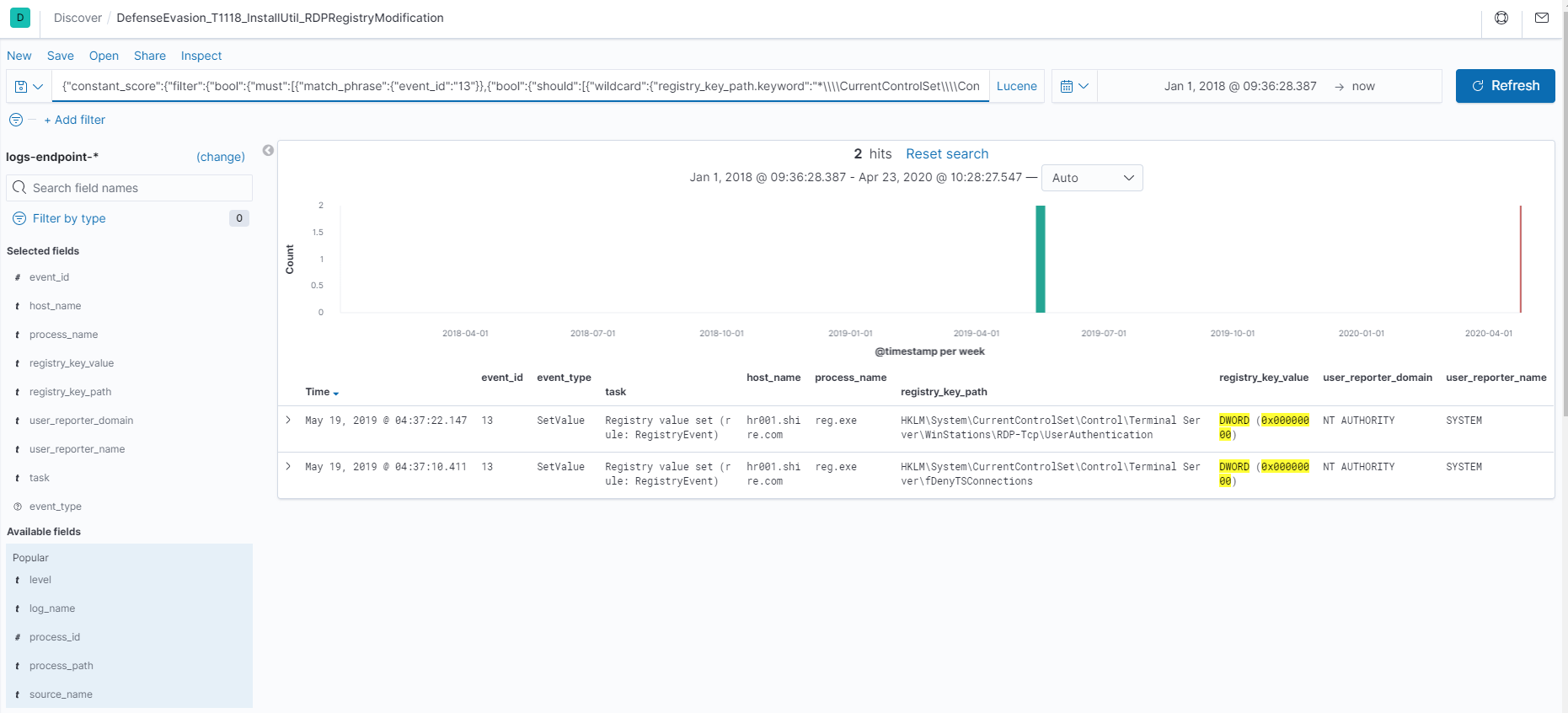
手机屏幕截图

描述已自动生成

DefenseEvasion\_T1118\_InstallUtil\_RDPSensitiveSettingsChanged

31.

此数据集表示攻击者开启RDP并且打开一条被入侵主机上的防火墙放行策略。



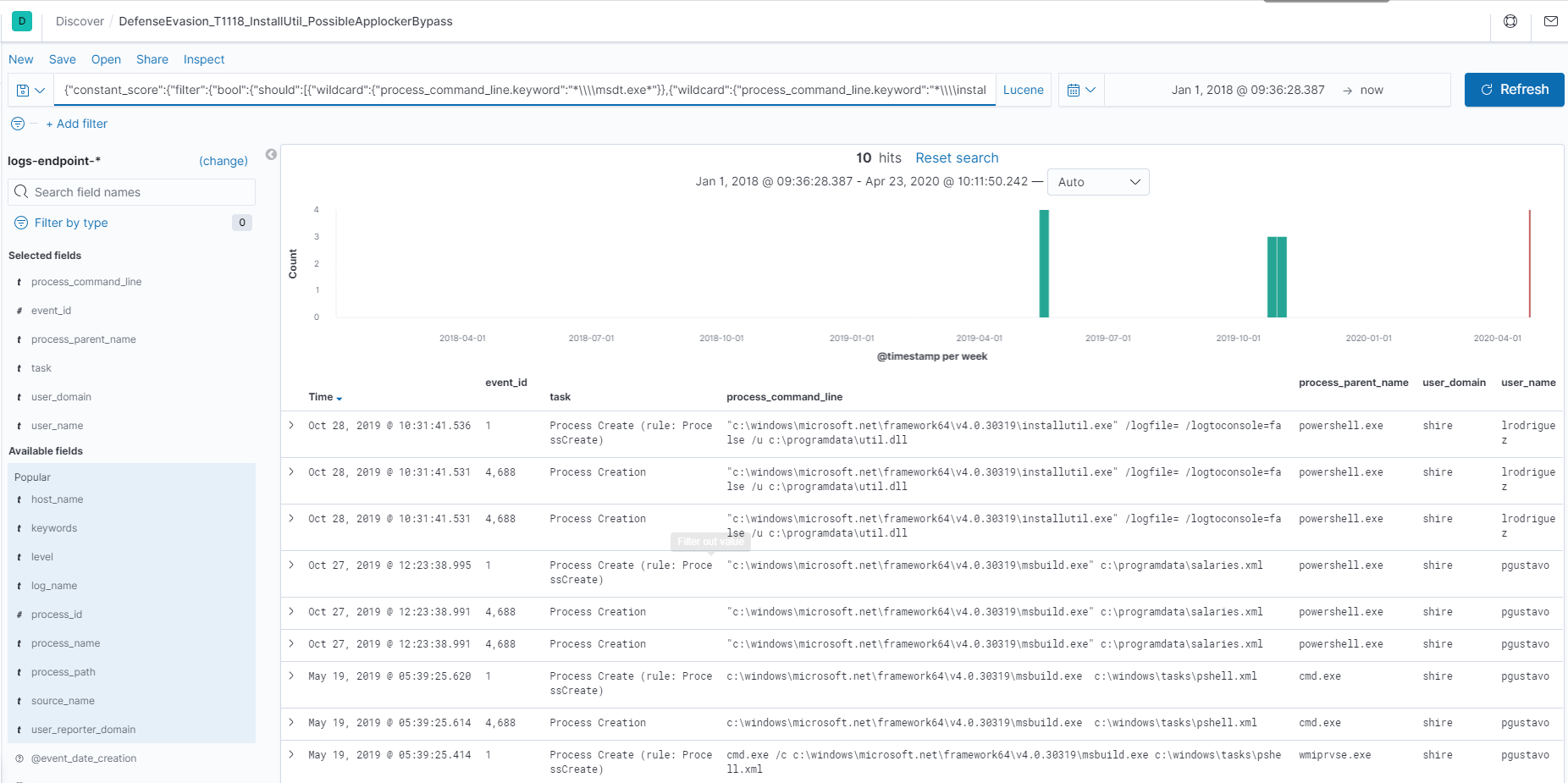
手机屏幕截图

描述已自动生成

DefenseEvasion\_T1118\_InstallUtil\_RDPRegistryModification

32.

此数据集表示对手使用受信任的窗口实用程序（如 msbuild）对恶意代码的代理执行。



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

DefenseEvasion\_T1118\_InstallUtil\_PossibleApplockerBypass