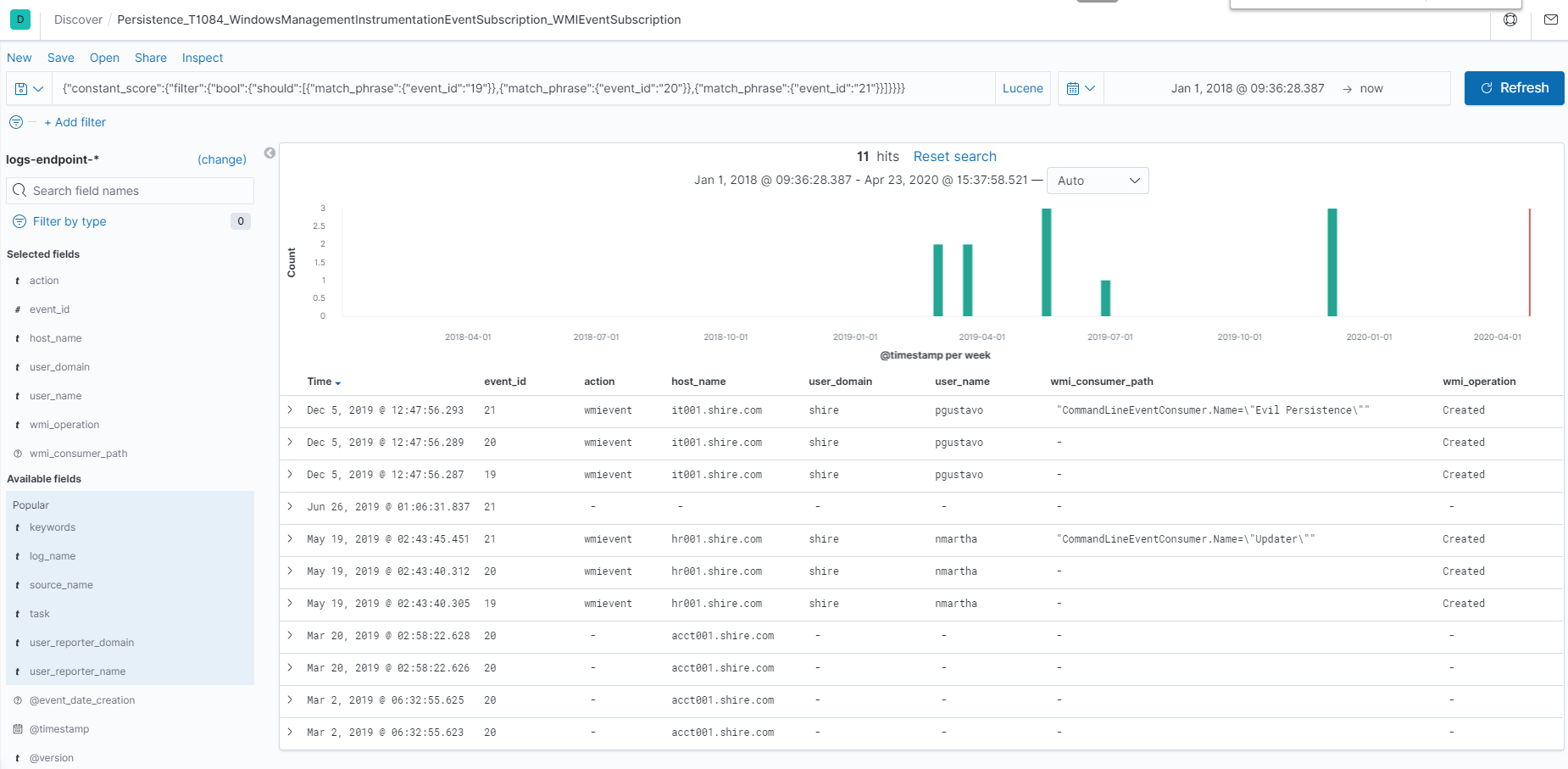
48.

此数据集表示攻击者利用 WMI 订阅特性进行持久化。



手机屏幕截图

描述已自动生成

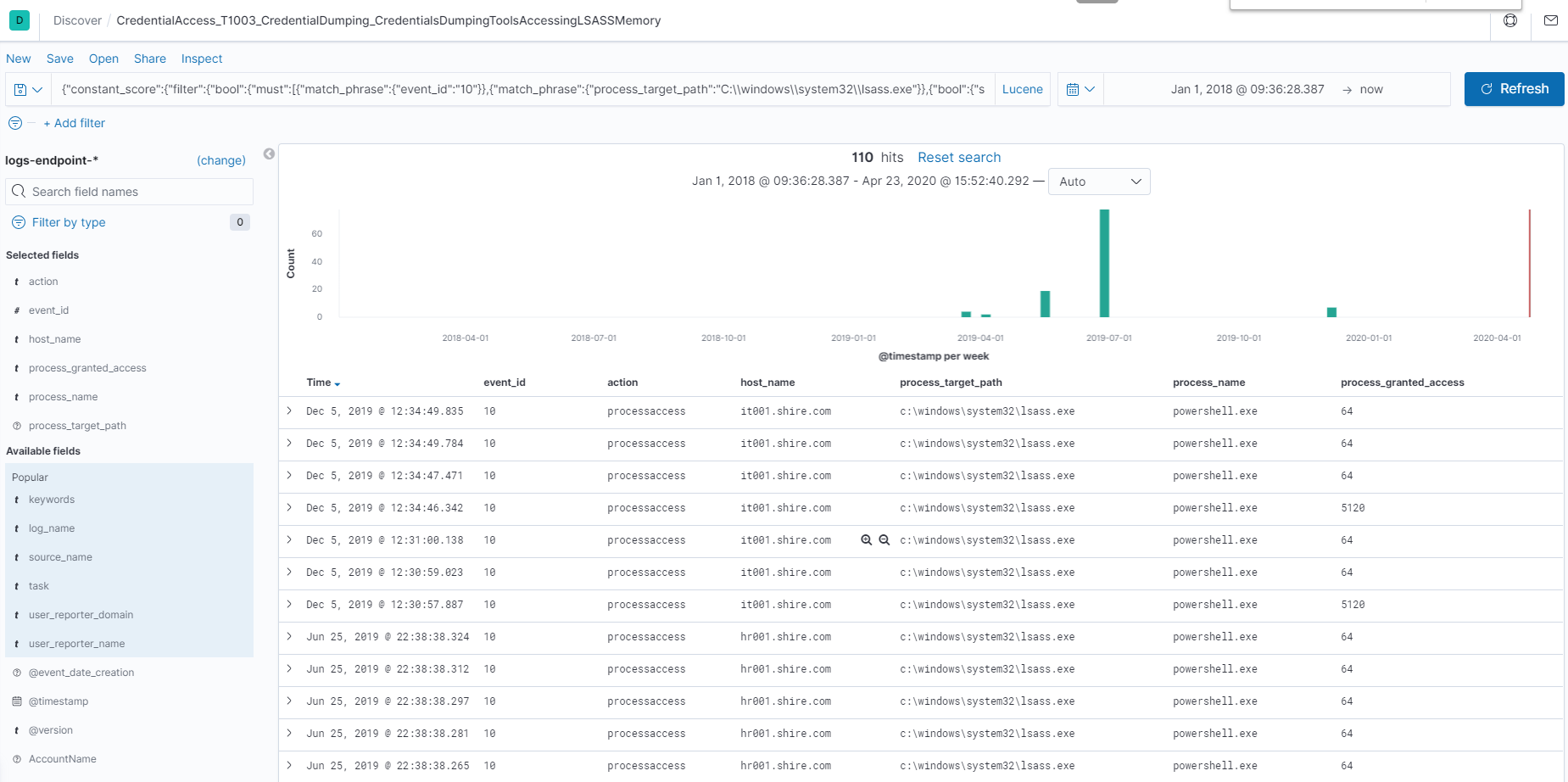


Persistence\_T1084\_WindowsManagementInstrumentationEventSubscription\_WMIEventSubscription

49.

Covenant Mimikatz LSA Cache

此数据集表示攻击者使用 Mimikatz 从 HKEY\_LOCAL\_MACHINE\SECURITY\Cache 中提取缓存的密码哈希值。



手机屏幕截图

描述已自动生成

Covenant Mimikatz LSA Secrets

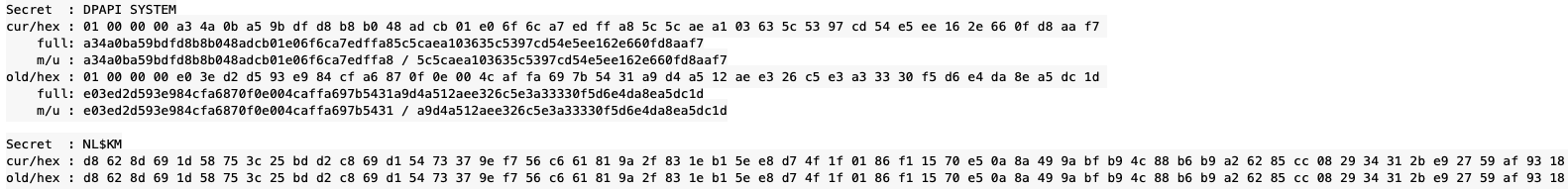
此数据集表示攻击者使用 Mimikatz 获取 SysKey 用来解密来自注册表或配置单元的机密条目。

手机屏幕截图

描述已自动生成

手机屏幕截图

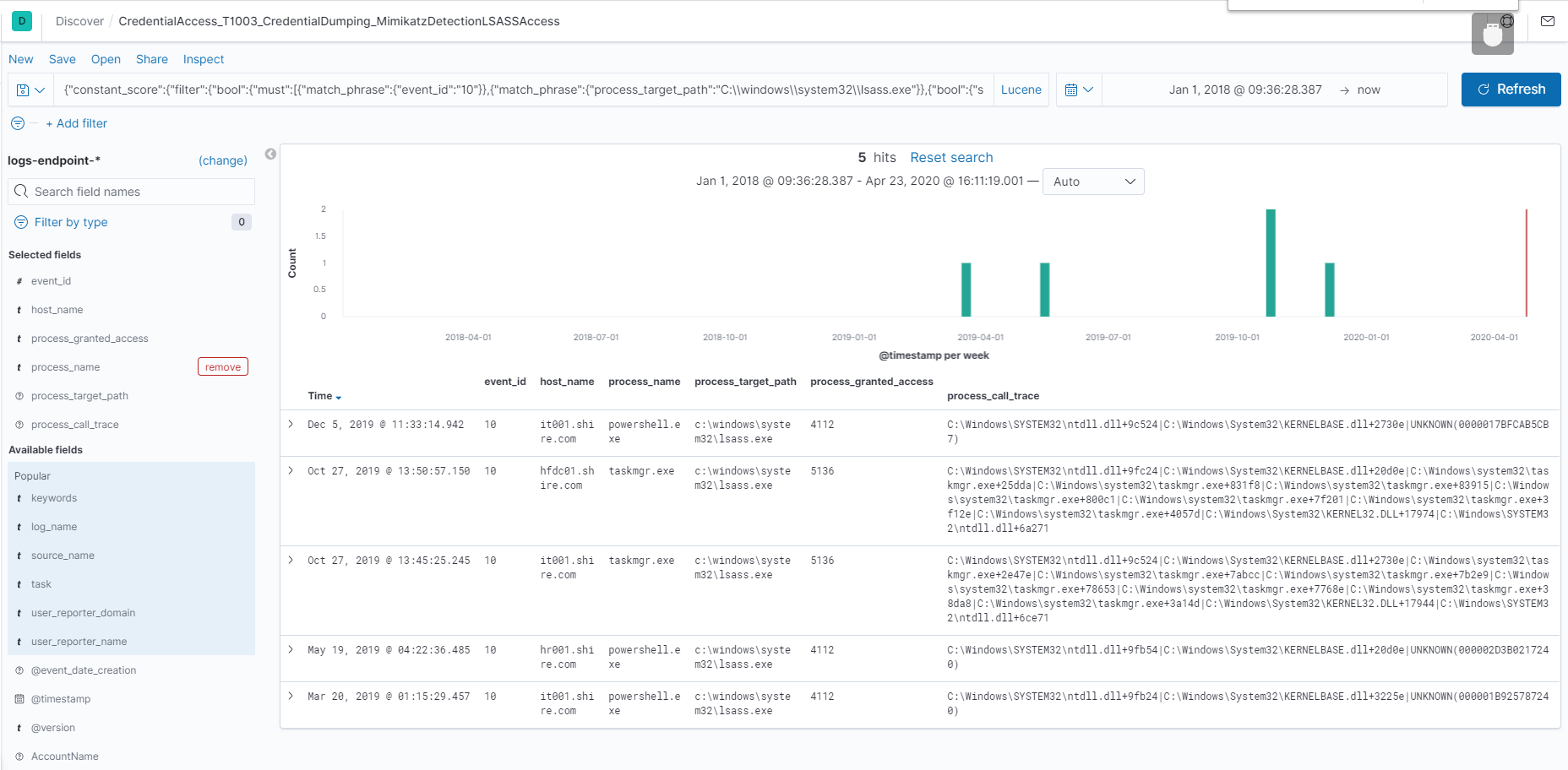
描述已自动生成



CredentialAccess\_T1003\_CredentialDumping\_CredentialsDumpingToolsAccessingLSASSMemory

50.

此数据集表示攻击者使用 mimikatz 和模块登录密码从 lsass.exe 的内存内容转储凭据。



手机屏幕截图

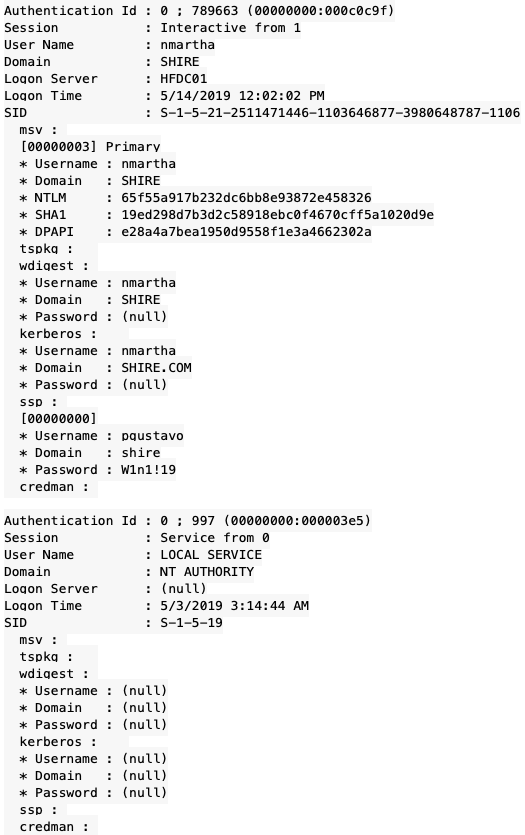
描述已自动生成

报纸上的文字

描述已自动生成

一些文字和图片的手机截图

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

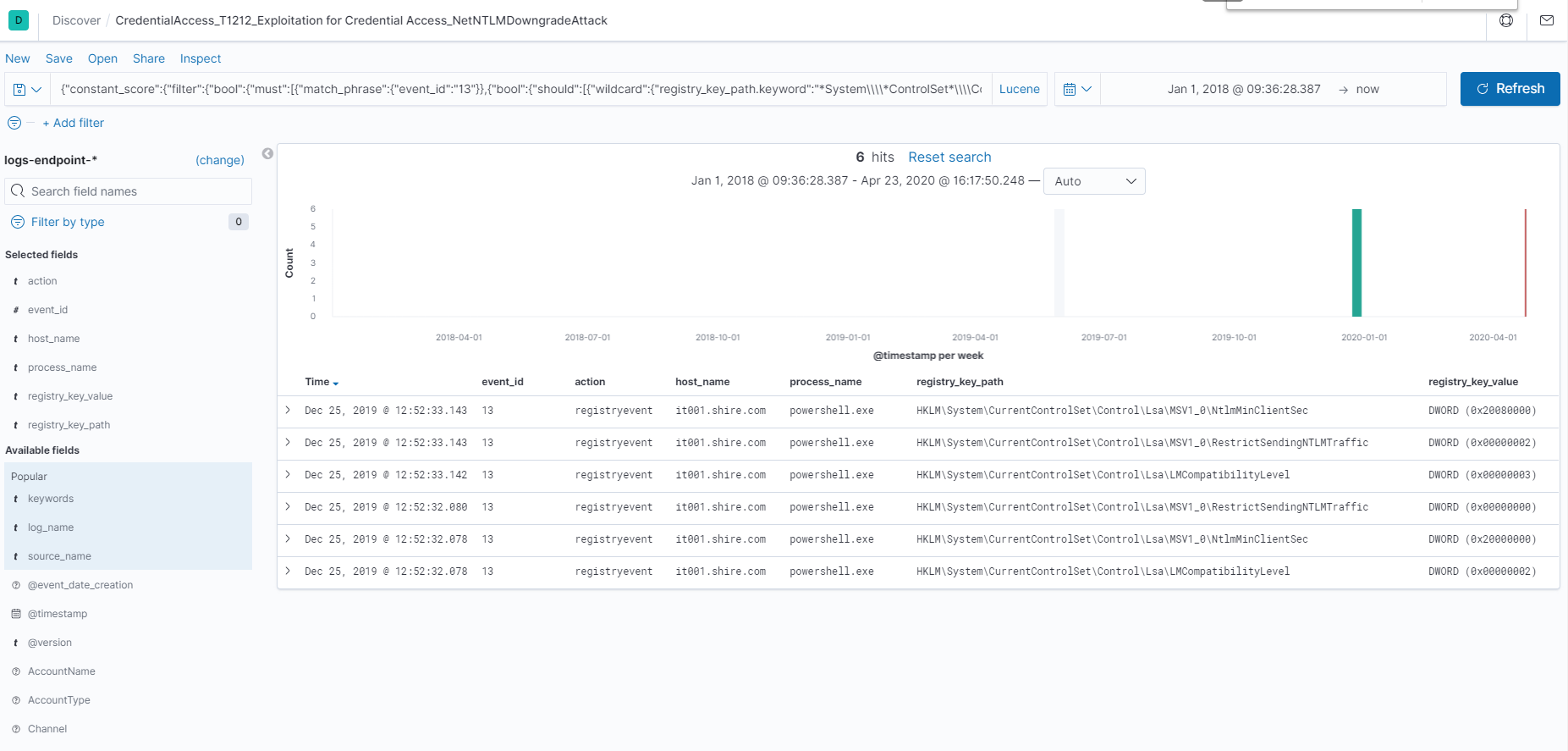
描述已自动生成

CredentialAccess\_T1003\_CredentialDumping\_MimikatzDetectionLSASSAccess

51.

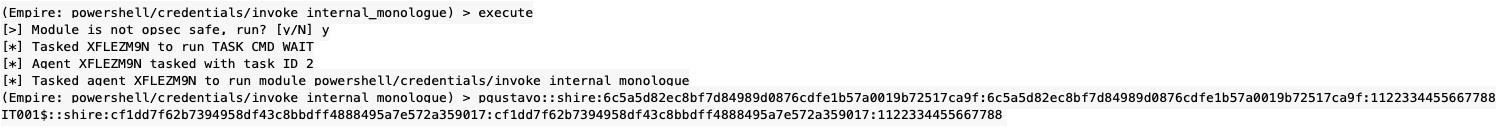
此数据集表示攻击者将对用在以下3方面的协议进行降级：

1. 网络登录的挑战/响应身份验证；
2. 使用NTLMSP进行最低限度安全协商；
3. 环境中限制NTLM流量到远端服务器的安全设置。



手机屏幕截图

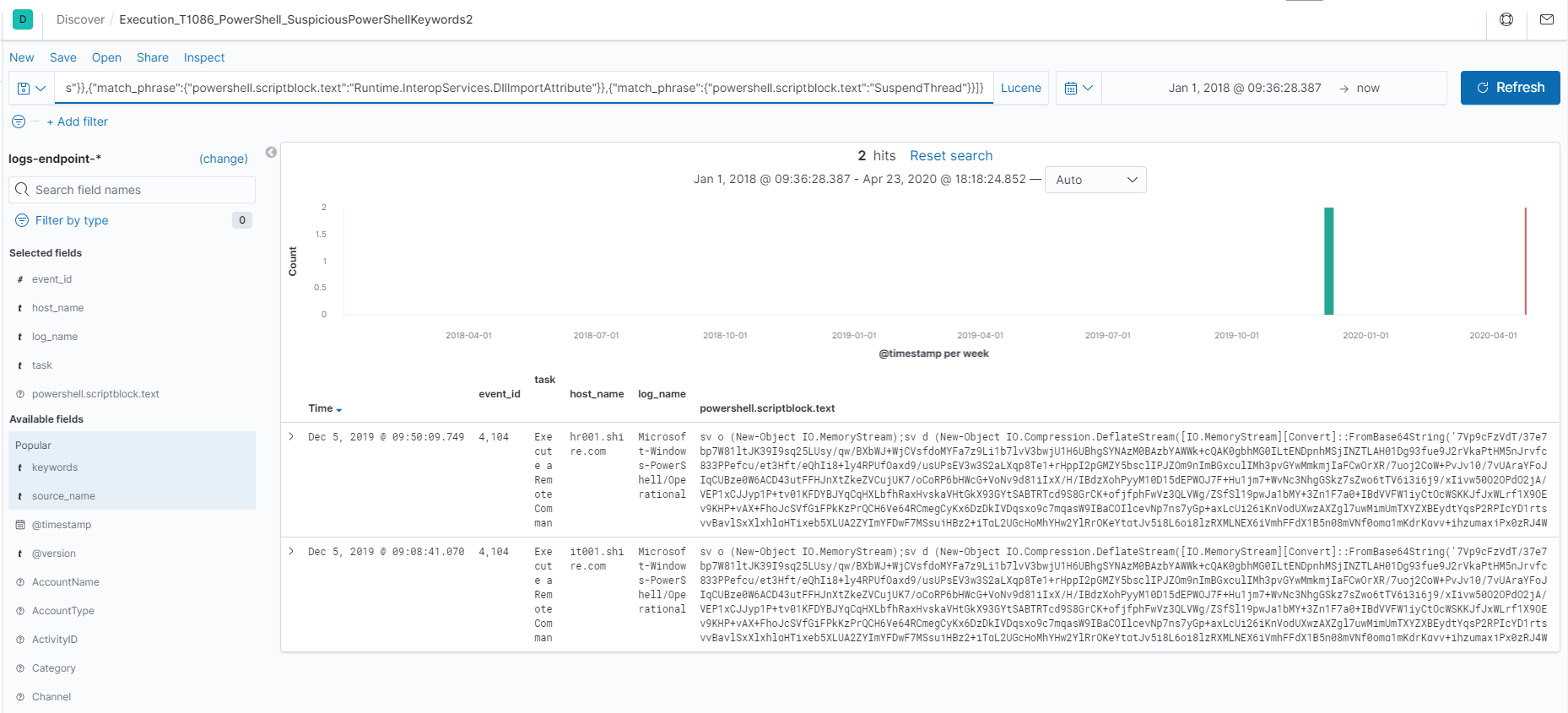
描述已自动生成



CredentialAccess\_T1212\_Exploitation for Credential Access\_NetNTLMDowngradeAttack

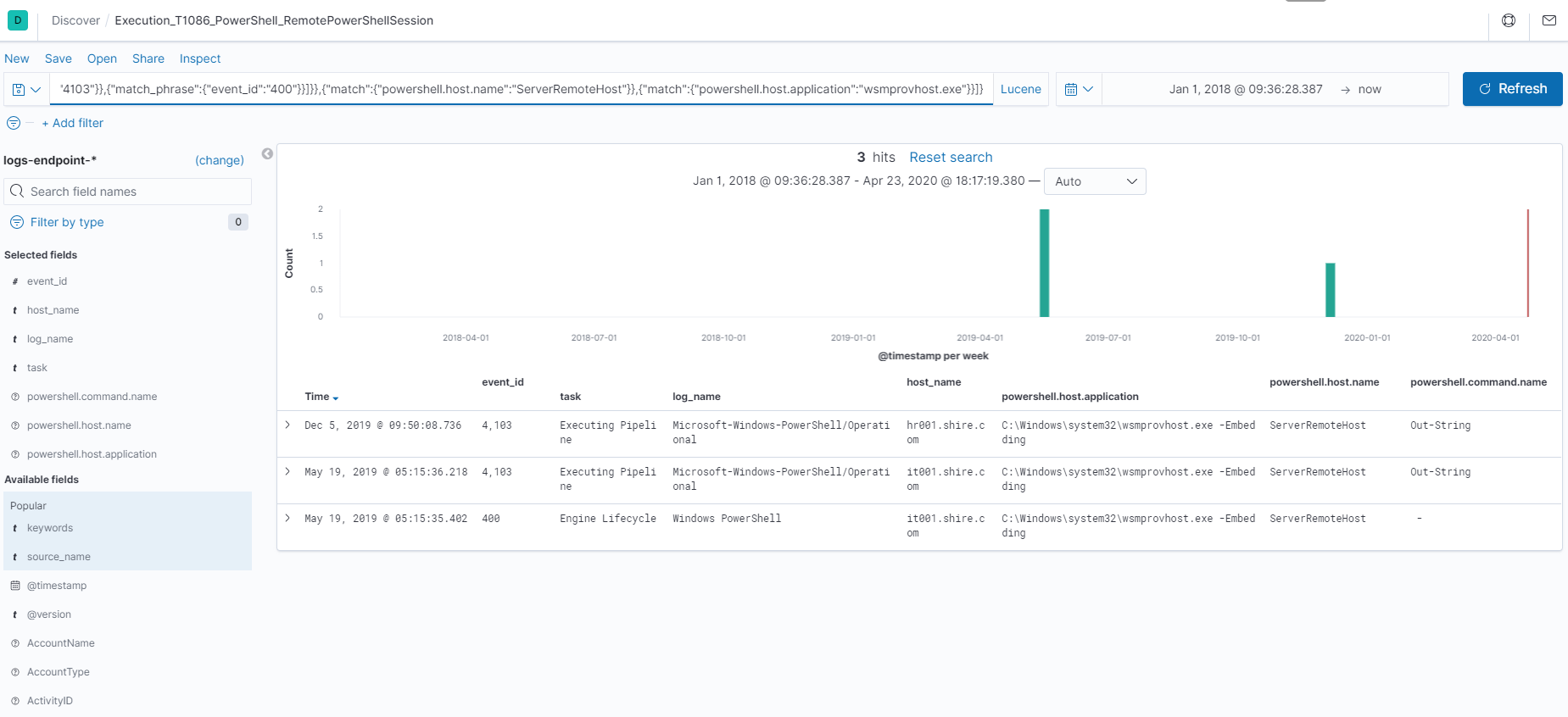
52.

Execution\_T1086\_PowerShell\_SuspiciousPowerShellKeywords2



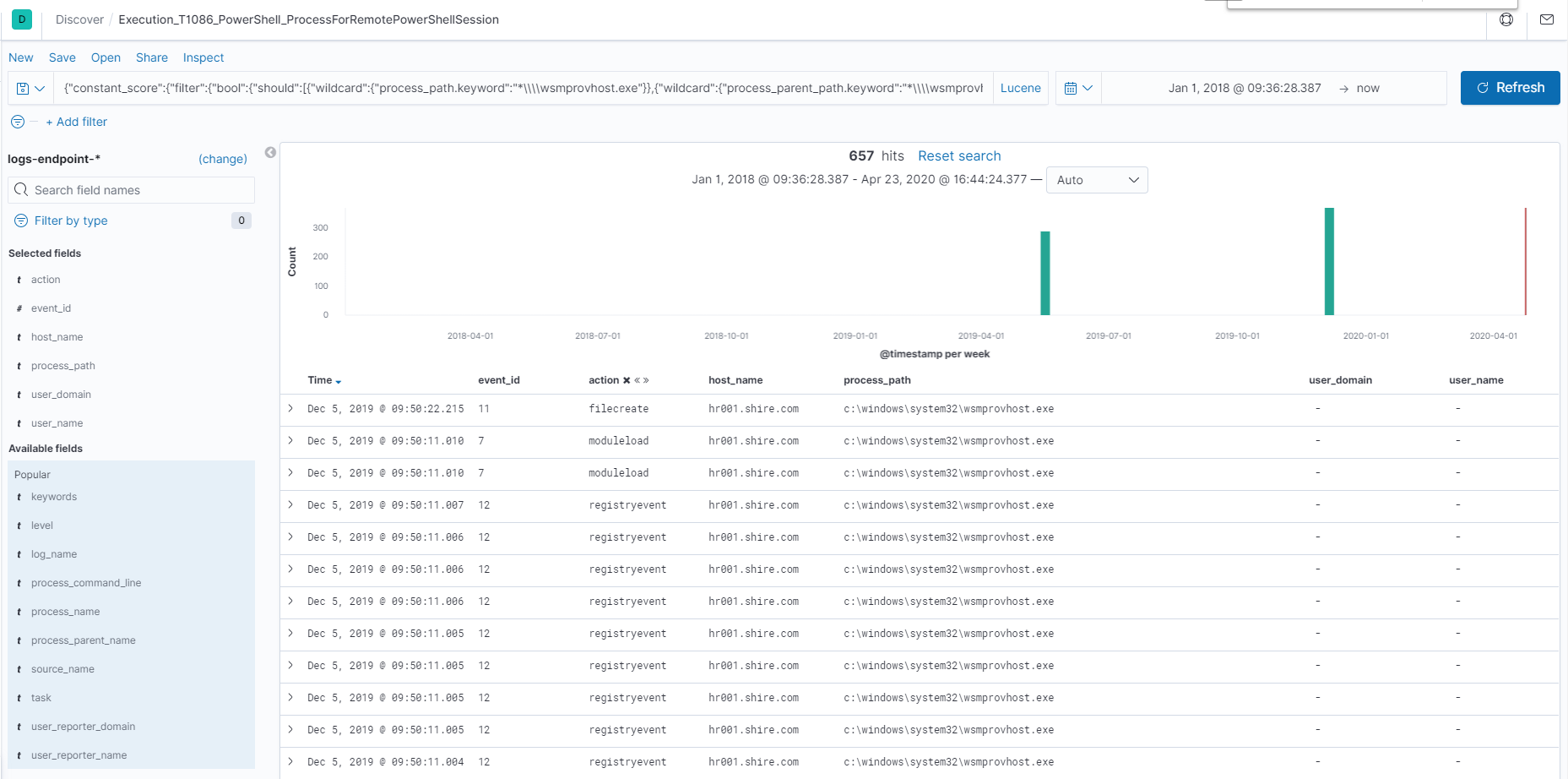
53.

Execution\_T1086\_PowerShell\_RemotePowerShellSession



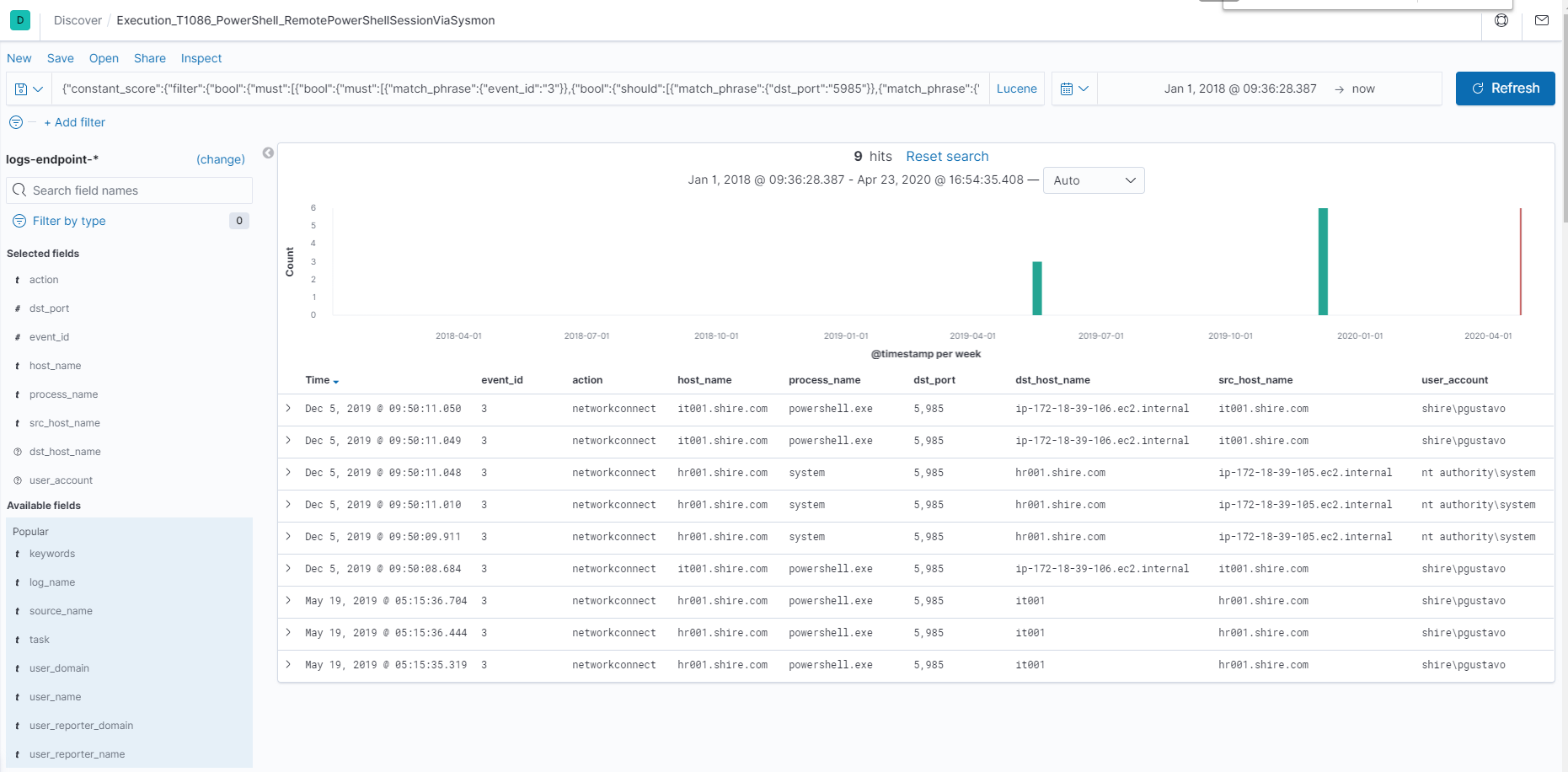
54.

Execution\_T1086\_PowerShell\_ProcessForRemotePowerShellSession



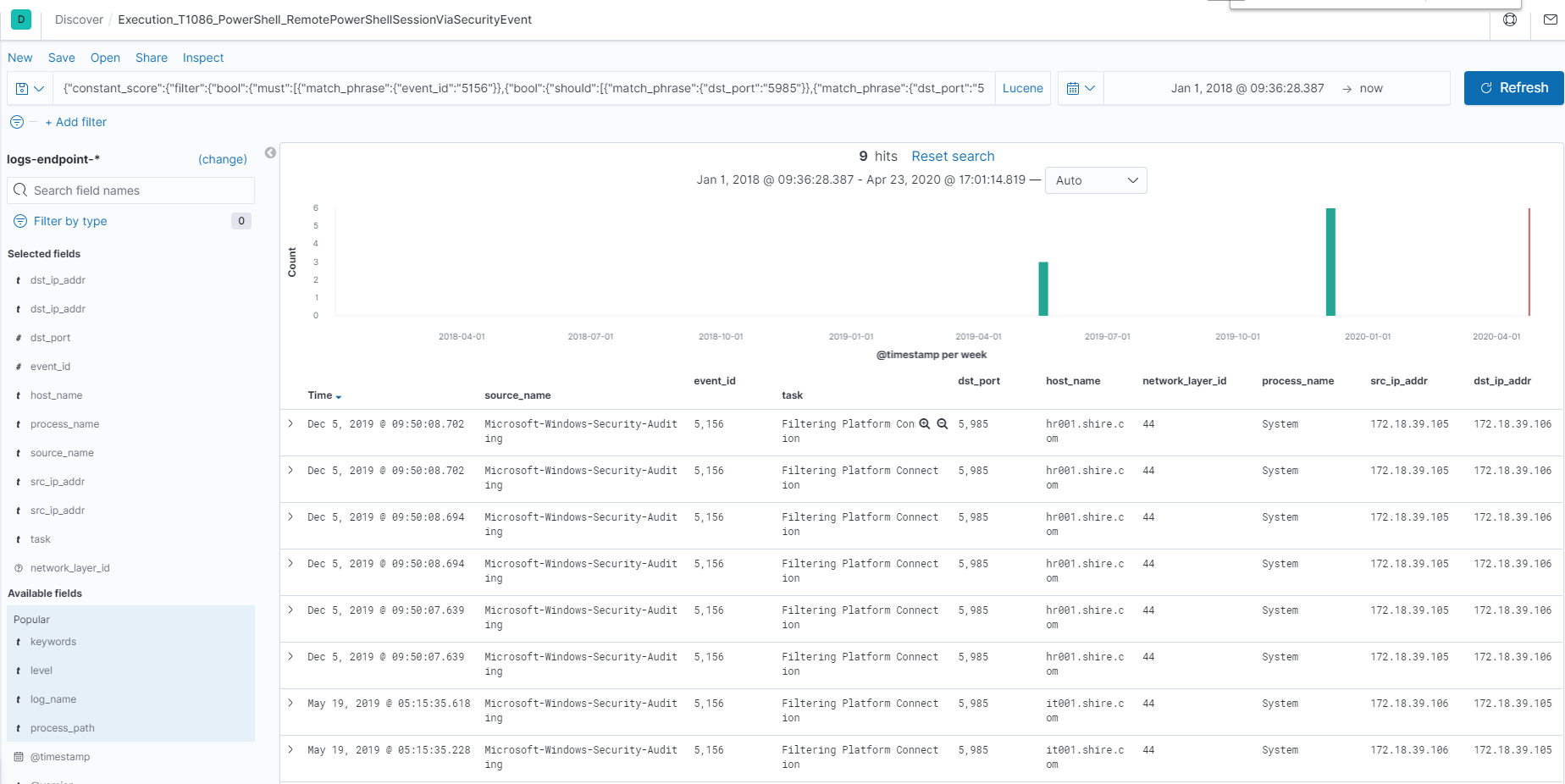
55.

Execution\_T1086\_PowerShell\_RemotePowerShellSessionViaSysmon



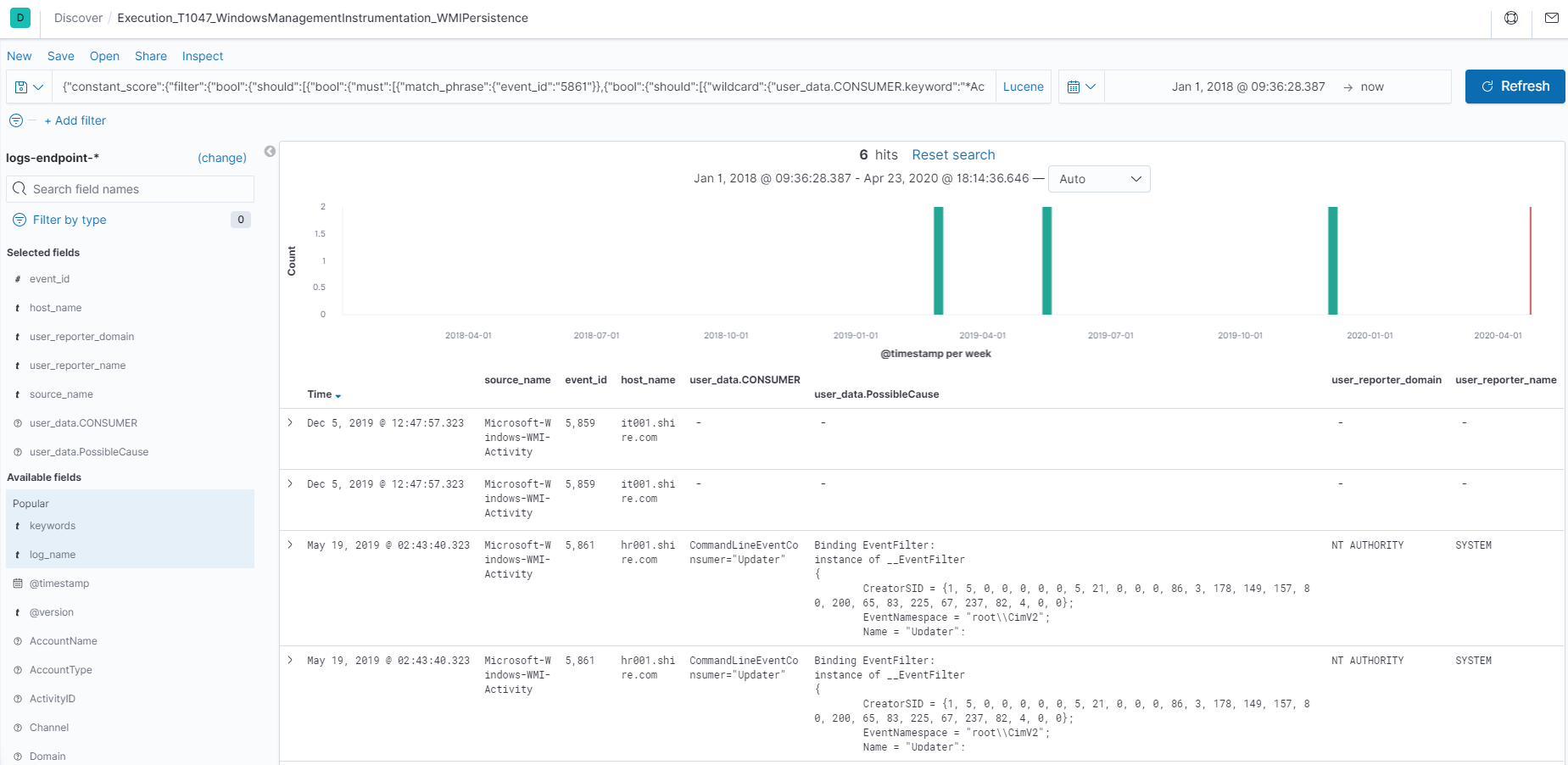
56.

Execution\_T1086\_PowerShell\_RemotePowerShellSessionViaSecurityEvent



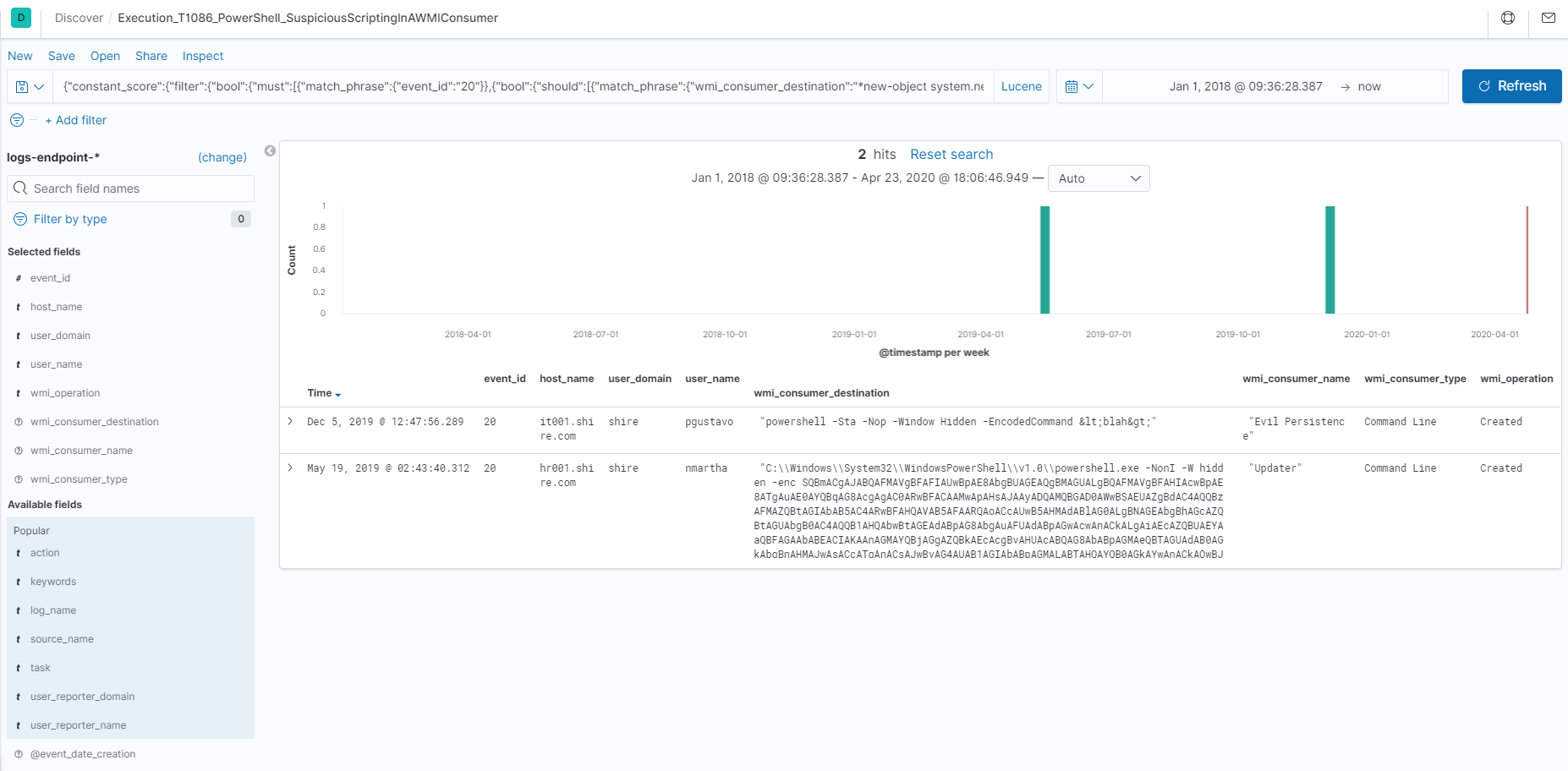
57.

Execution\_T1047\_WindowsManagementInstrumentation\_WMIPersistence



58.

Execution\_T1086\_PowerShell\_SuspiciousScriptingInAWMIConsumer



59.

Execution\_T1086\_PowerShell\_DetectsSuspiciousPowershellCommandLineParametersUsedInEmpire

