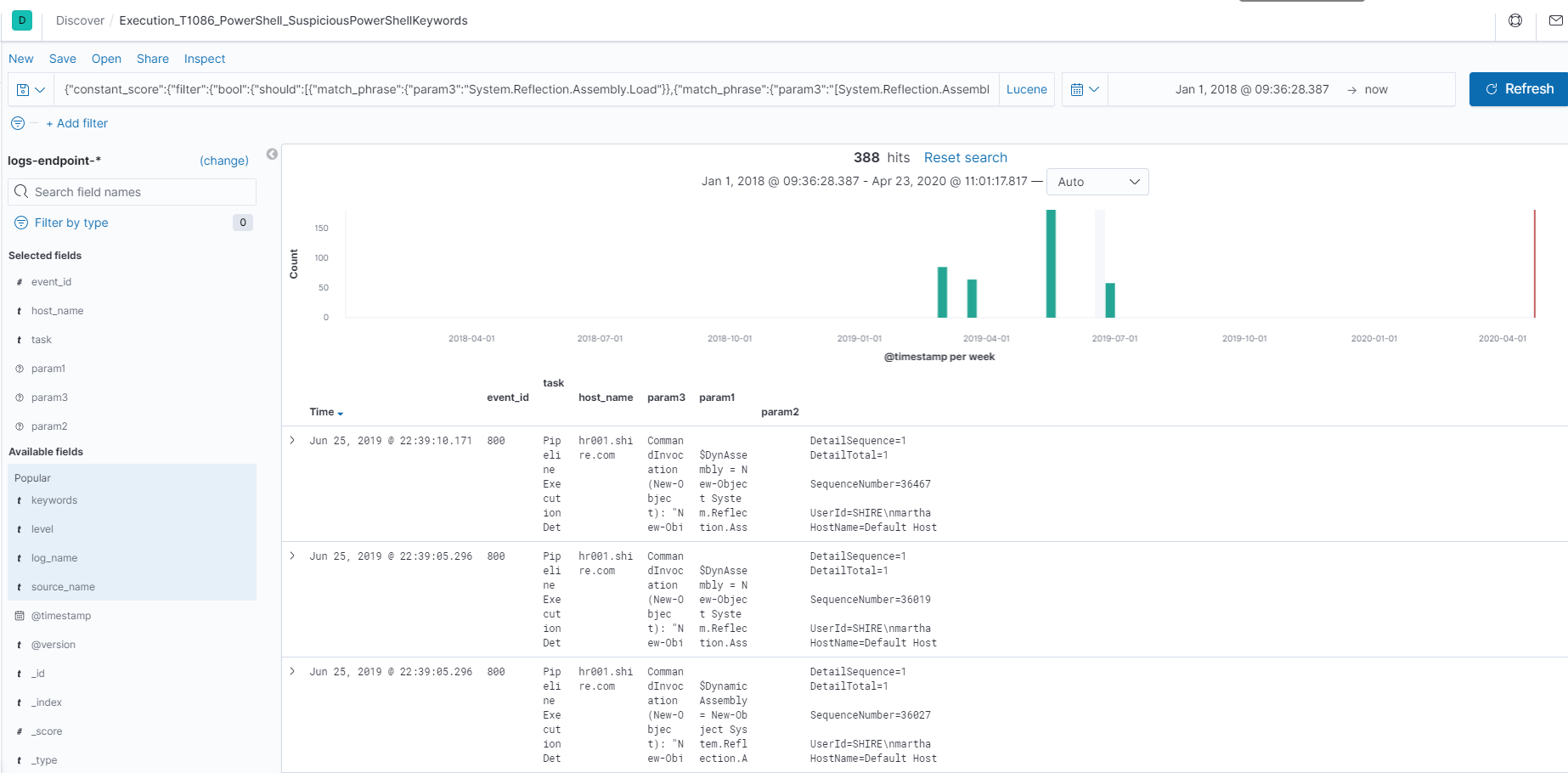
33.

此数据集表示攻击者使用Empire项目注入脚本将不受管理的PowerShell代码 注入任何进程。



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

手机截图图社交软件的信息

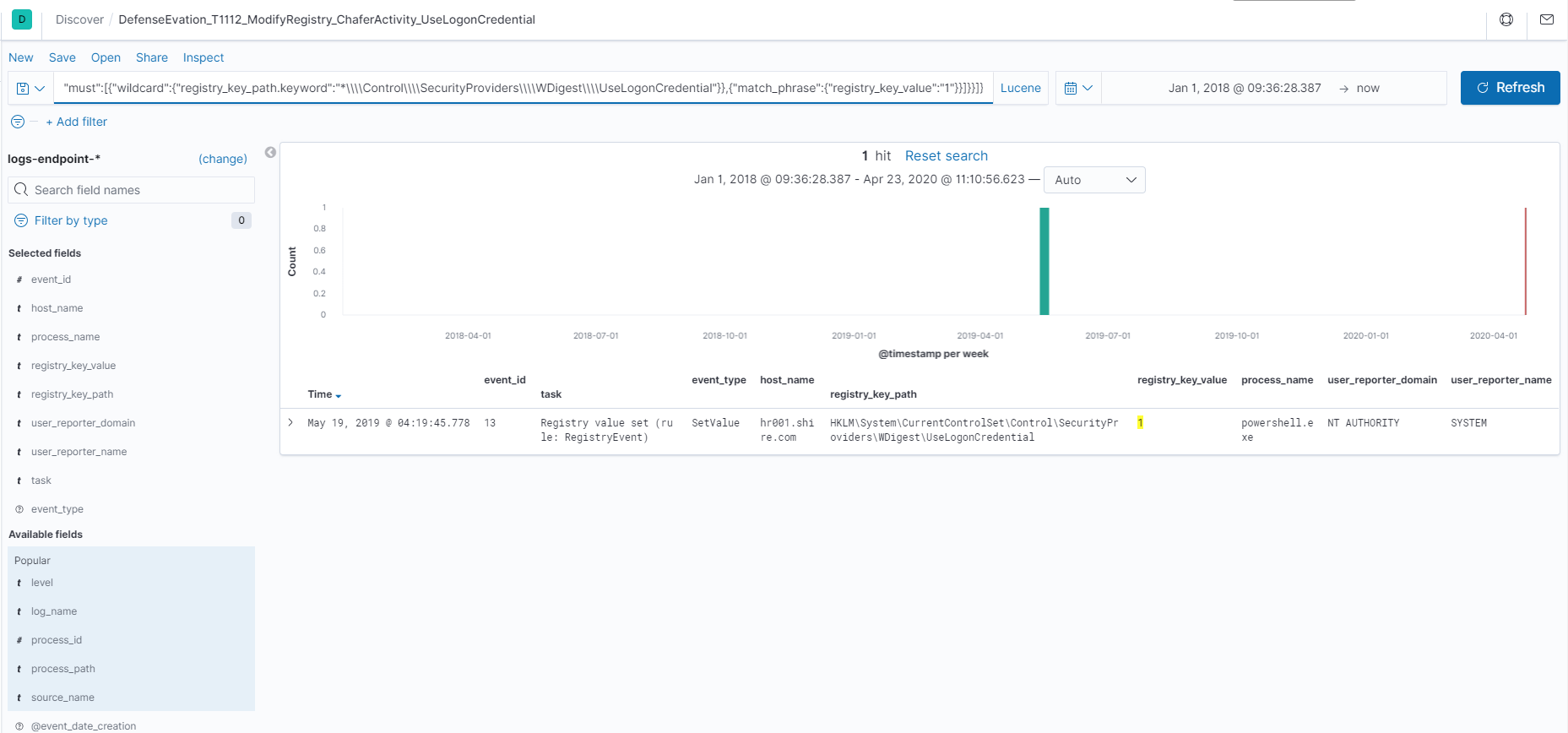
描述已自动生成

Execution\_T1086\_PowerShell\_SuspiciousPowerShellKeywords

34.

此数据集表示对手将HKLM：\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest

中UseLogonCredential键对应的属性值设置为 1 ，从而启用纯文本密码。

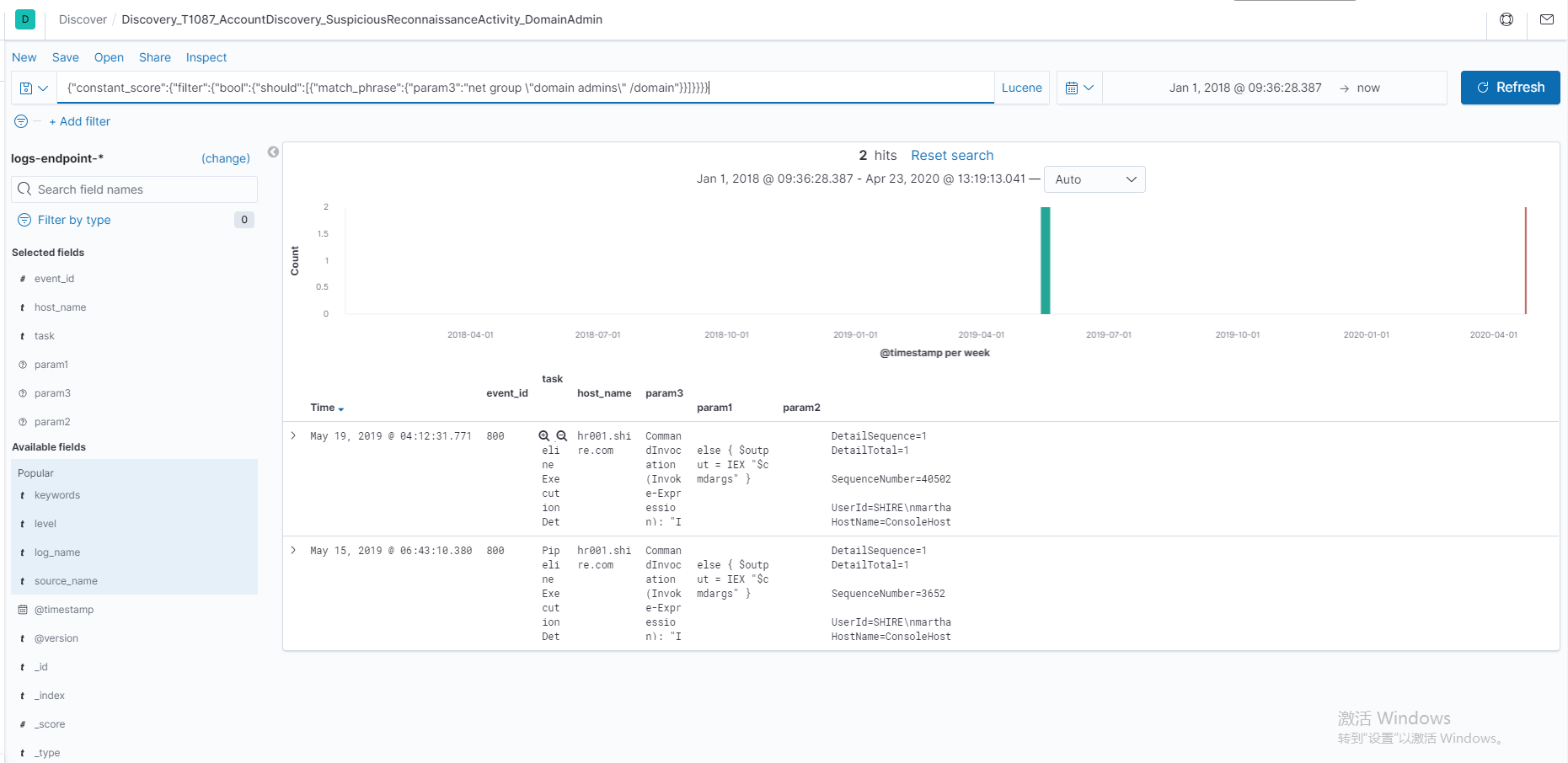


没有攻击者视图

DefenseEvation\_T1112\_ModifyRegistry\_ChaferActivity\_UseLogonCredential

35.

此数据集表示攻击者通过 net.exe 枚举"域管理员"活动目录组成员。



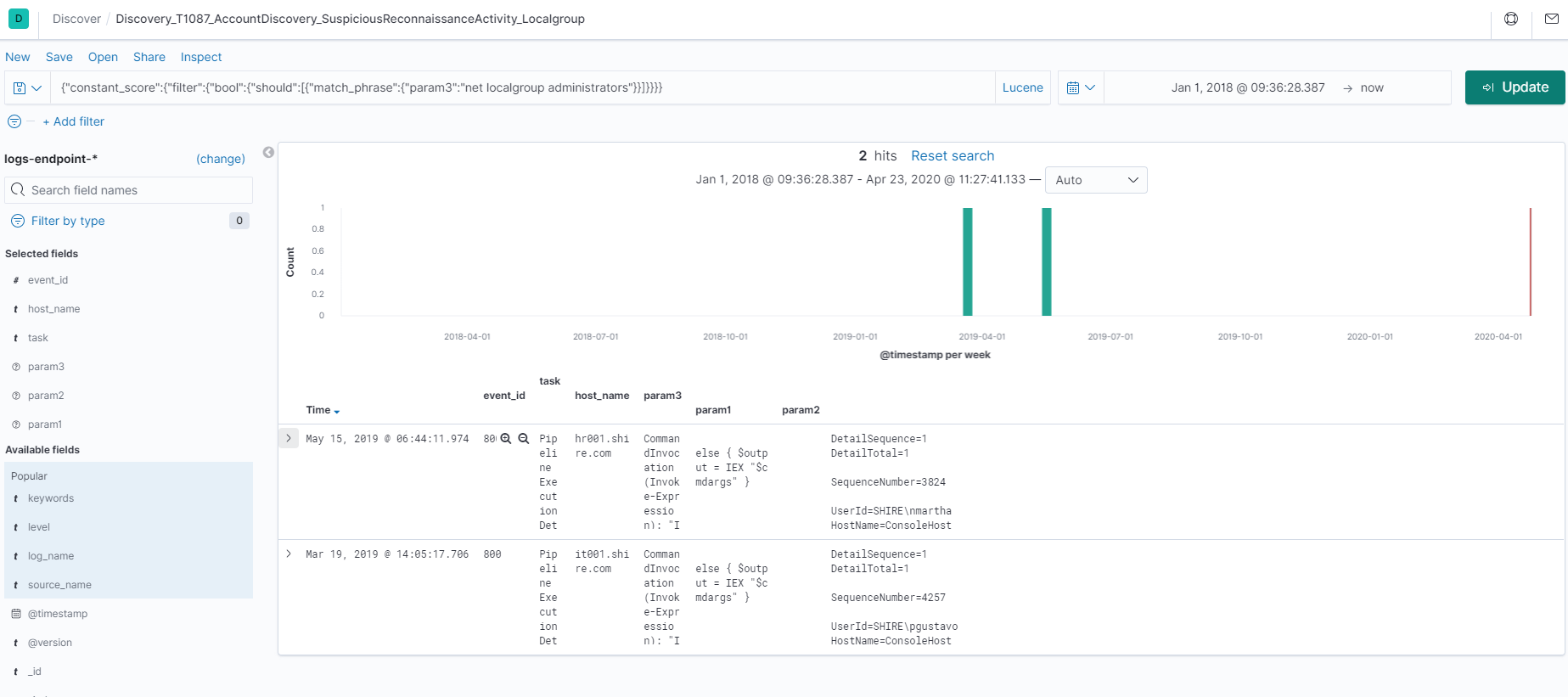
手机屏幕截图

描述已自动生成

Discovery\_T1087\_AccountDiscovery\_SuspiciousReconnaissanceActivity\_DomainAdmin

36.

此数据集表示攻击者通过 net.exe 实用程序枚举本地管理员组成员。



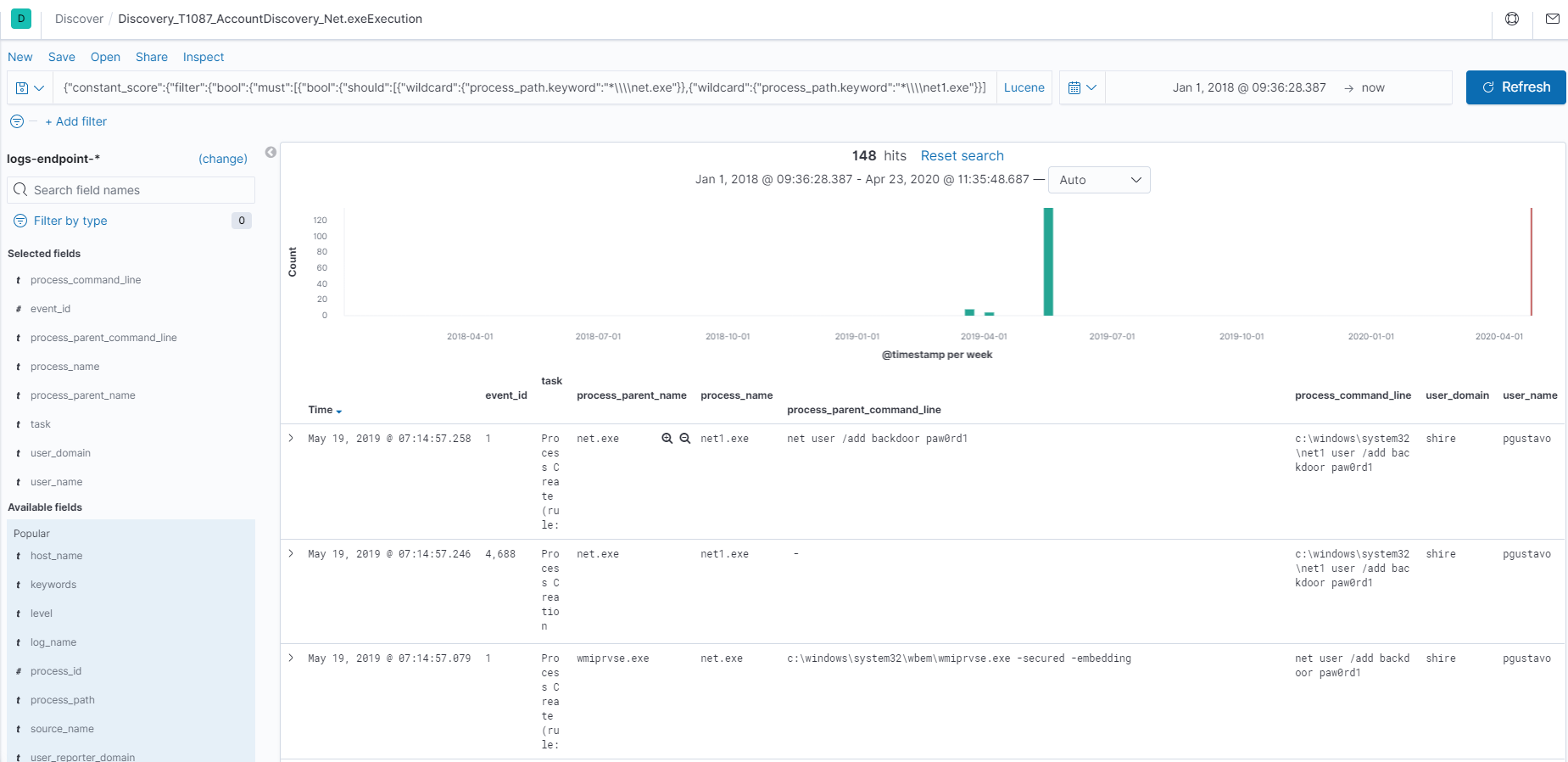
手机屏幕截图

描述已自动生成

Discovery\_T1087\_AccountDiscovery\_SuspiciousReconnaissanceActivity\_Localgroup

37.

此数据集表示攻击者通过 net.exe 实用程序枚举所有本地用户。



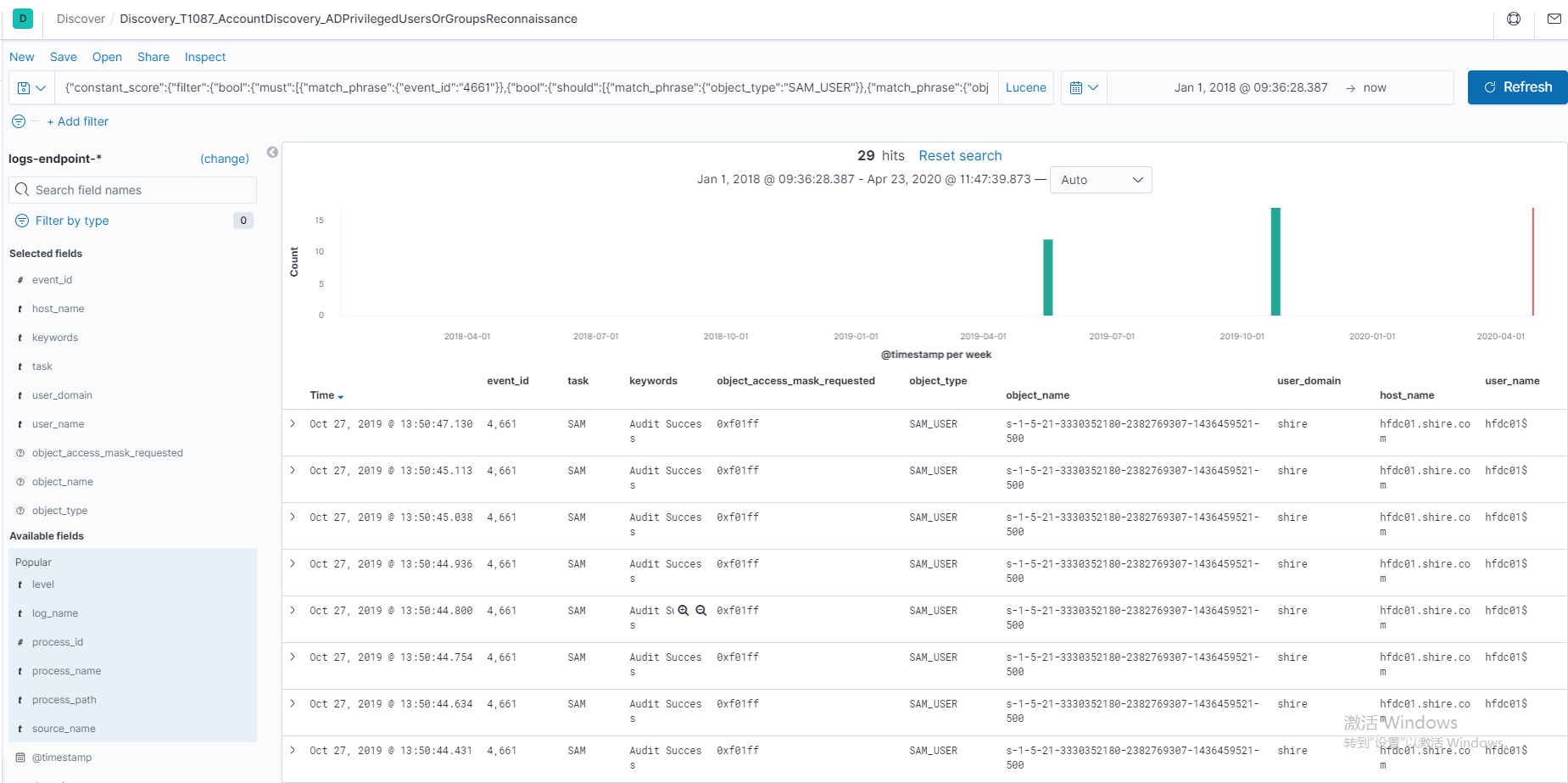
手机屏幕截图

描述已自动生成

Discovery\_T1087\_AccountDiscovery\_Net.exeExecution

38.

此数据集表示攻击者通过 net.exe 枚举"域管理员"活动目录组成员。



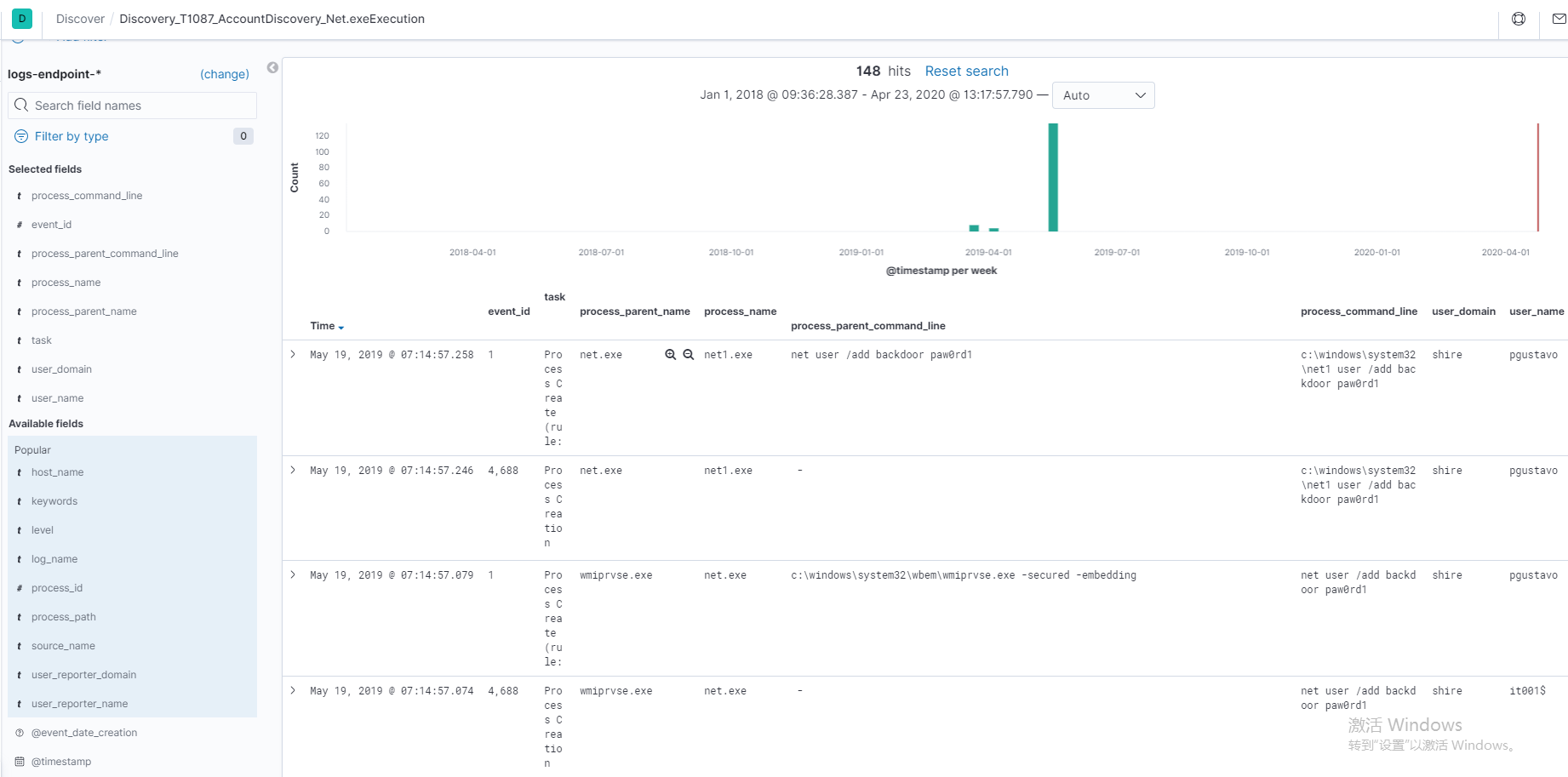
手机屏幕截图

描述已自动生成

Discovery\_T1087\_AccountDiscovery\_ADPrivilegedUsersOrGroupsReconnaissance

39.

此数据集表示攻击者通过 net.exe 实用程序枚举特定域用户。



手机屏幕截图

描述已自动生成

Discovery\_T1087\_AccountDiscovery\_Net.exeExecution