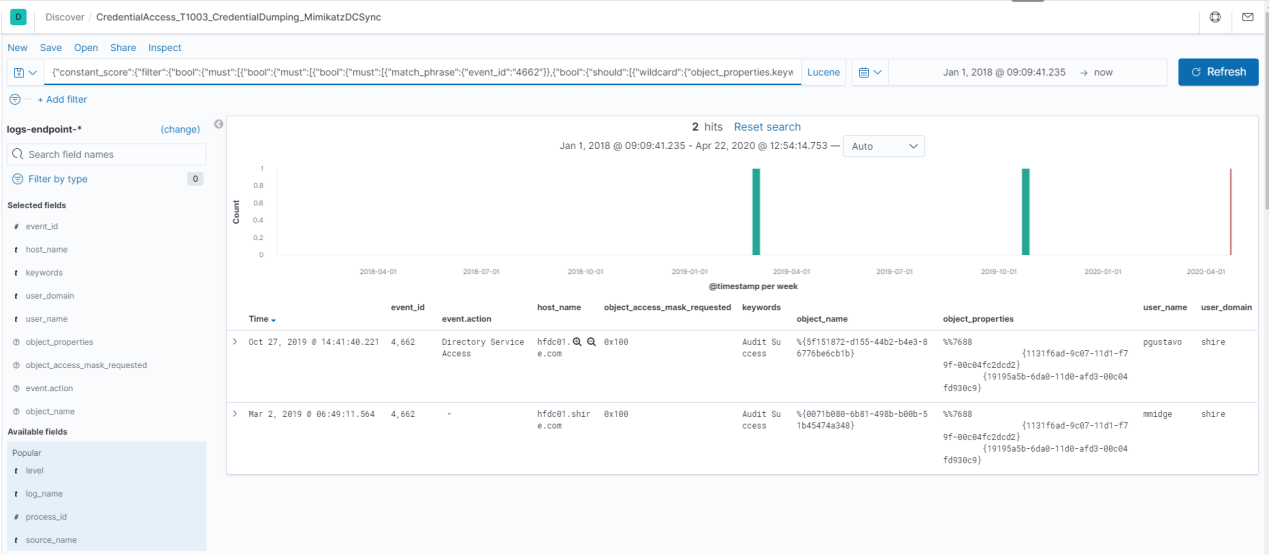
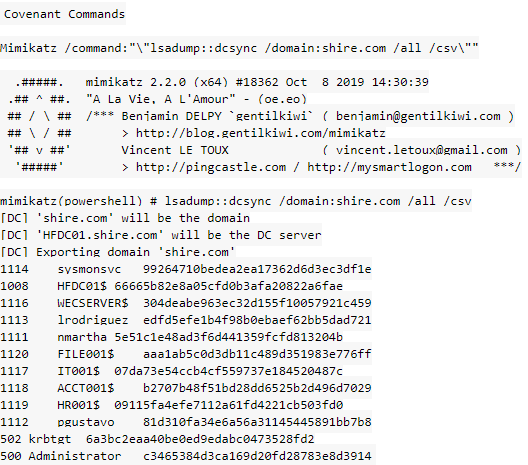
1、

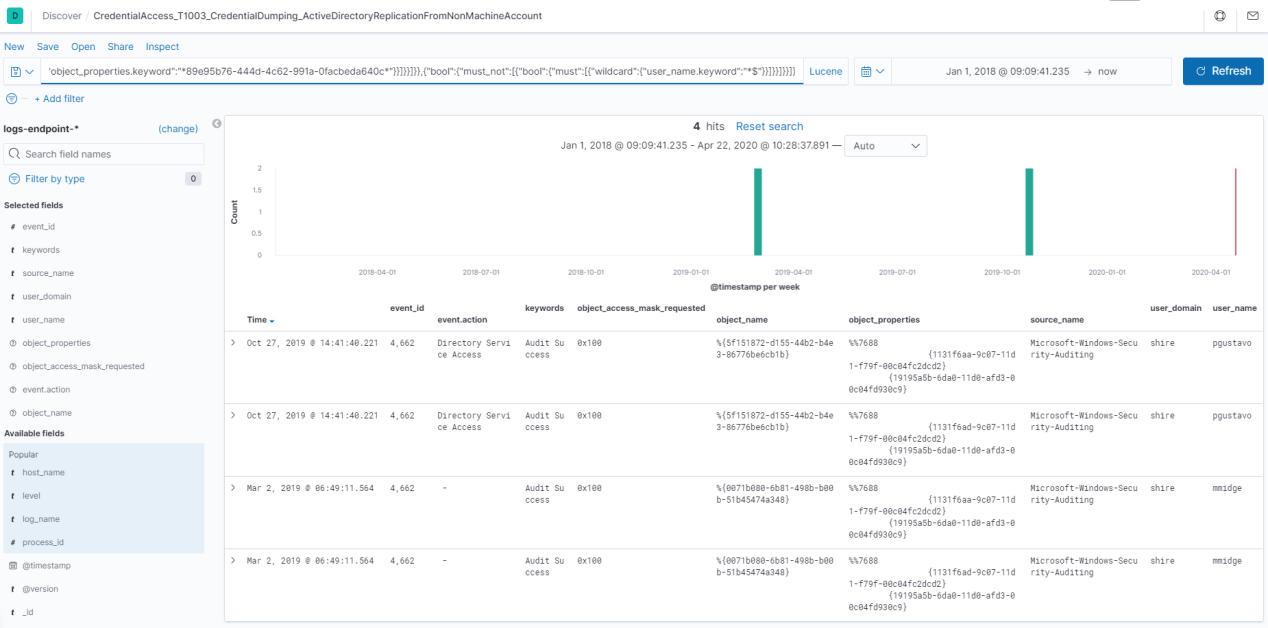
此数据集表示对手滥用Active Directory复制服务以从所有域帐户检索NTLM哈希值。

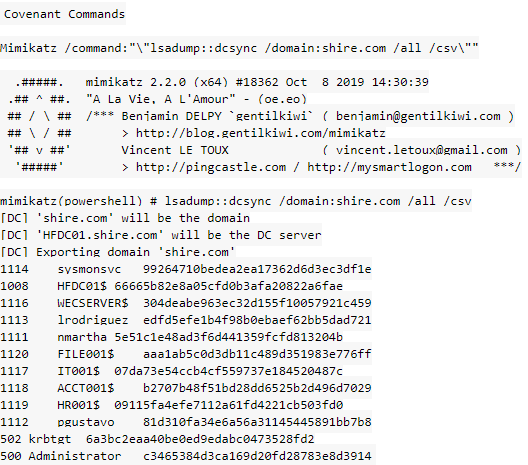




2、

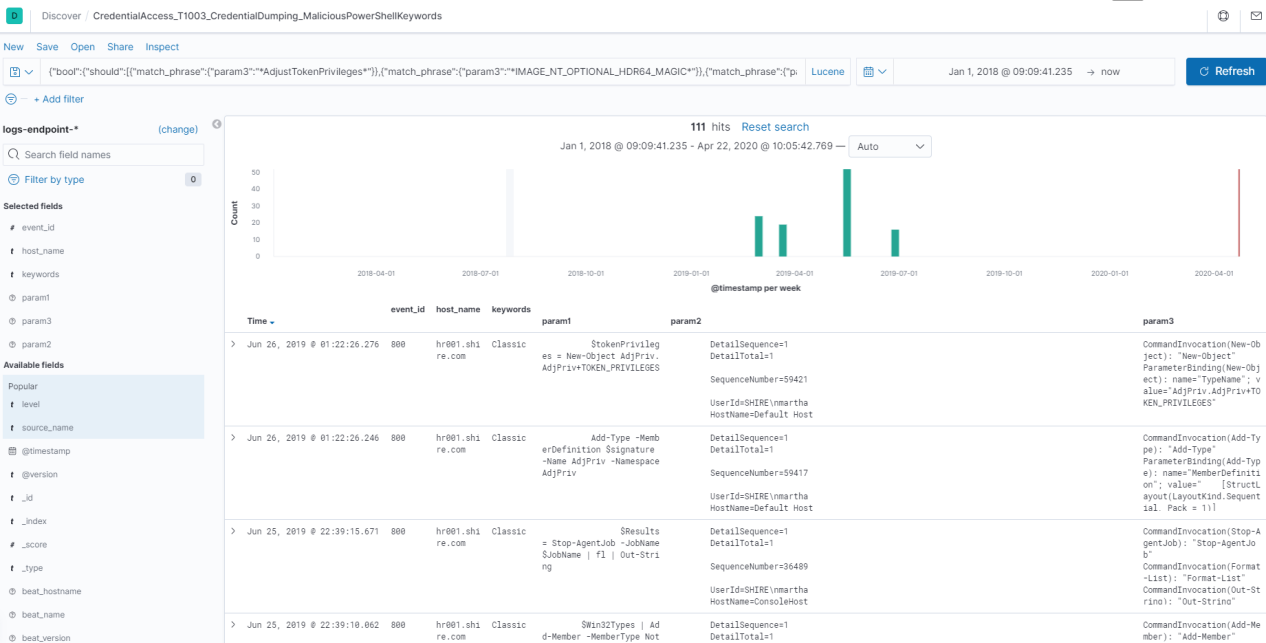
此数据集表示对手滥用Active Directory复制服务以从所有域帐户检索NTLM哈希值。



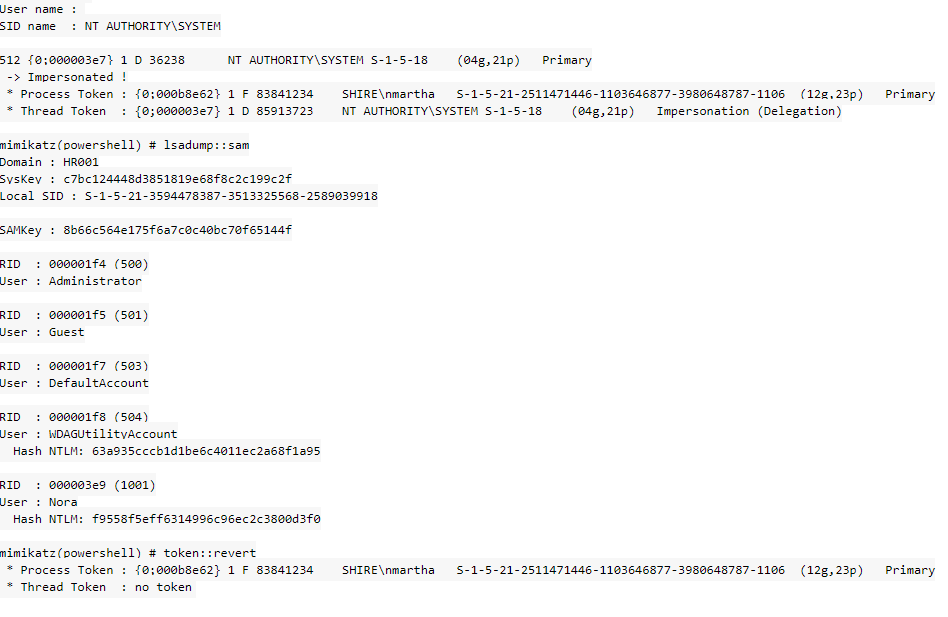


3、

该数据集表示对手使用PowerSploit的Invoke-Mimikatz函数从安全帐户管理器（SAM）数据库中提取哈希值。

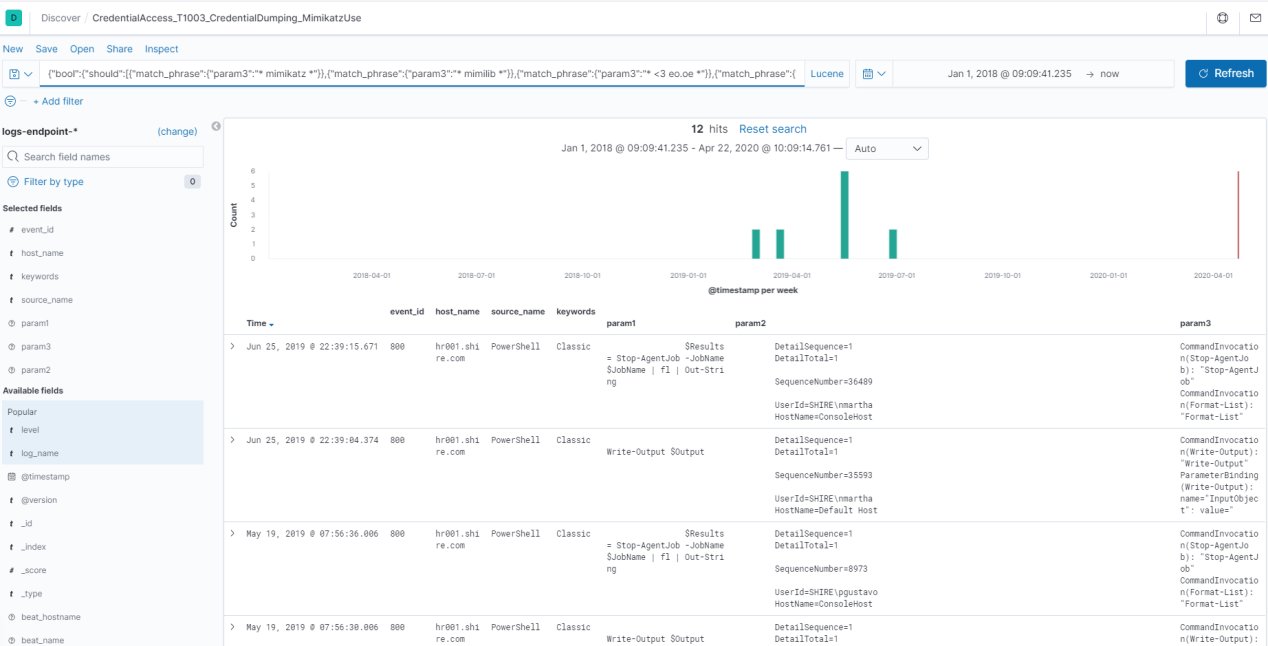




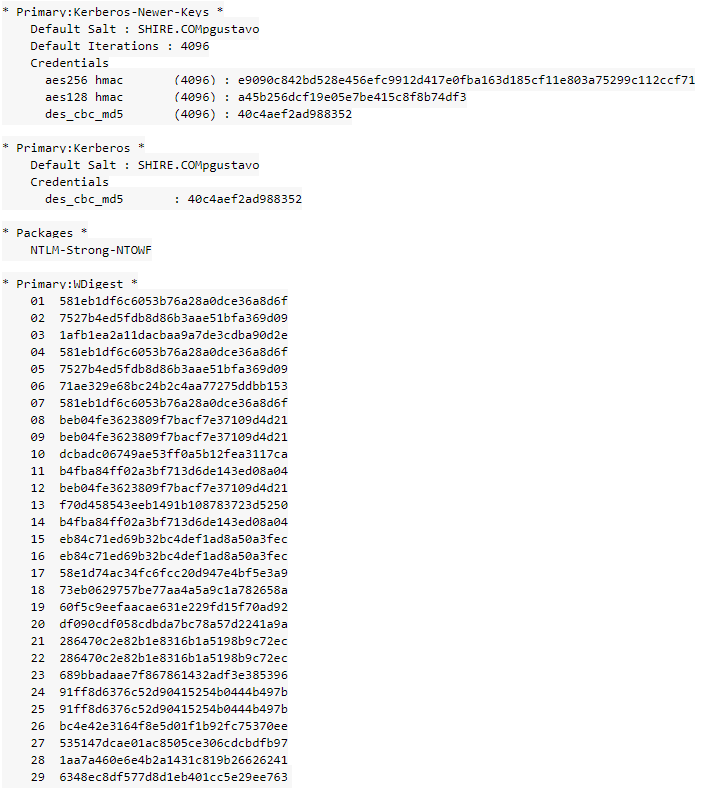


4、

该数据集表示攻击者滥用Active Directory复制服务来从域帐户中检索NTLM哈希。

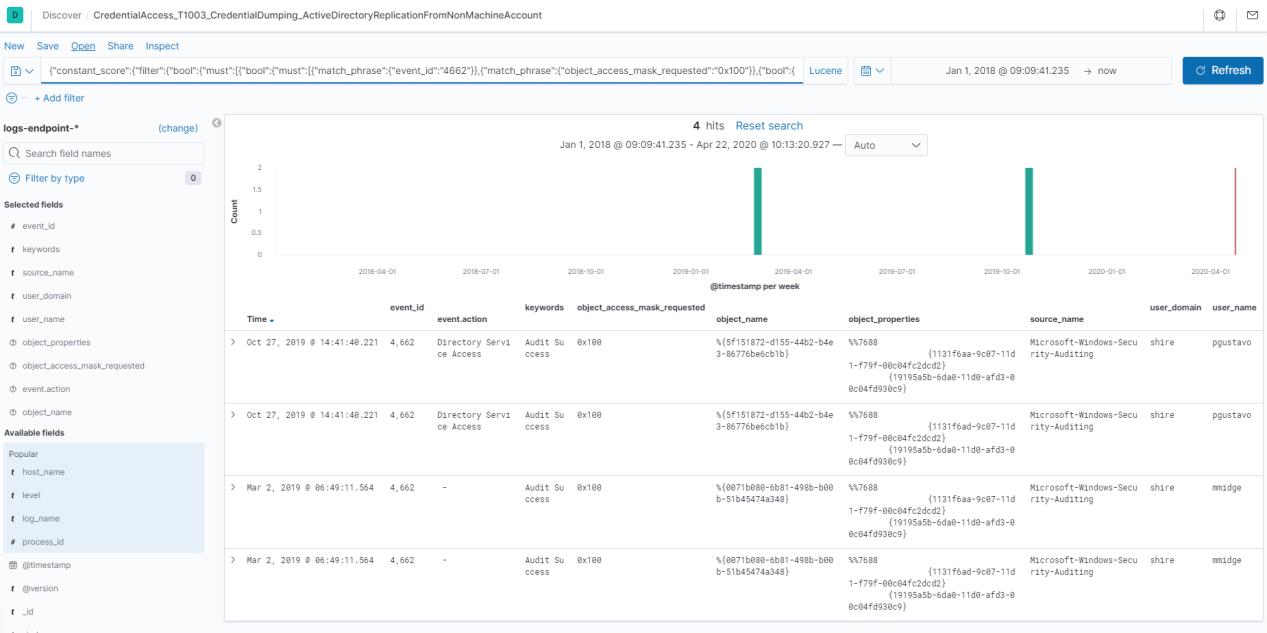




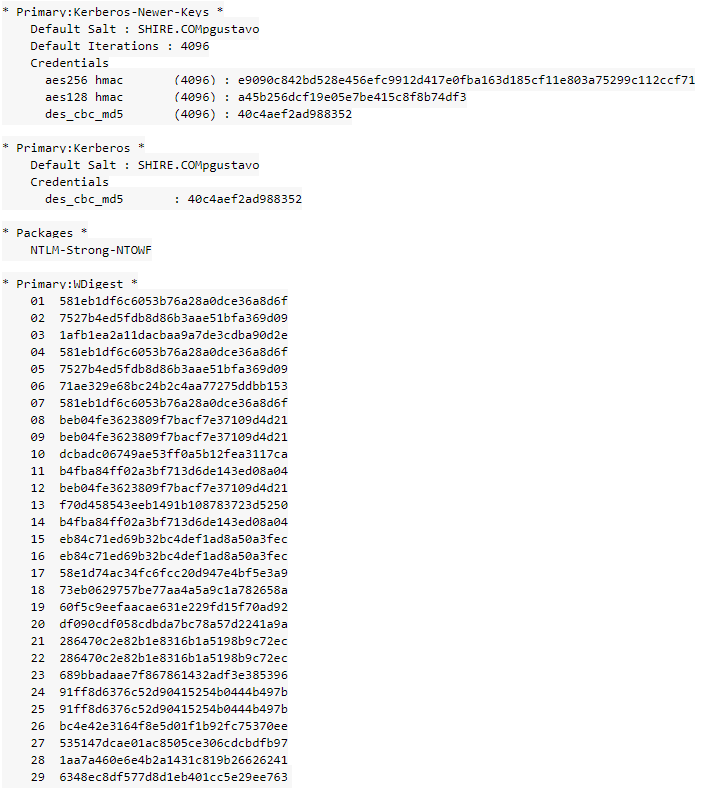


5、

该数据集表示攻击者滥用Active Directory复制服务来从域帐户中检索NTLM哈希

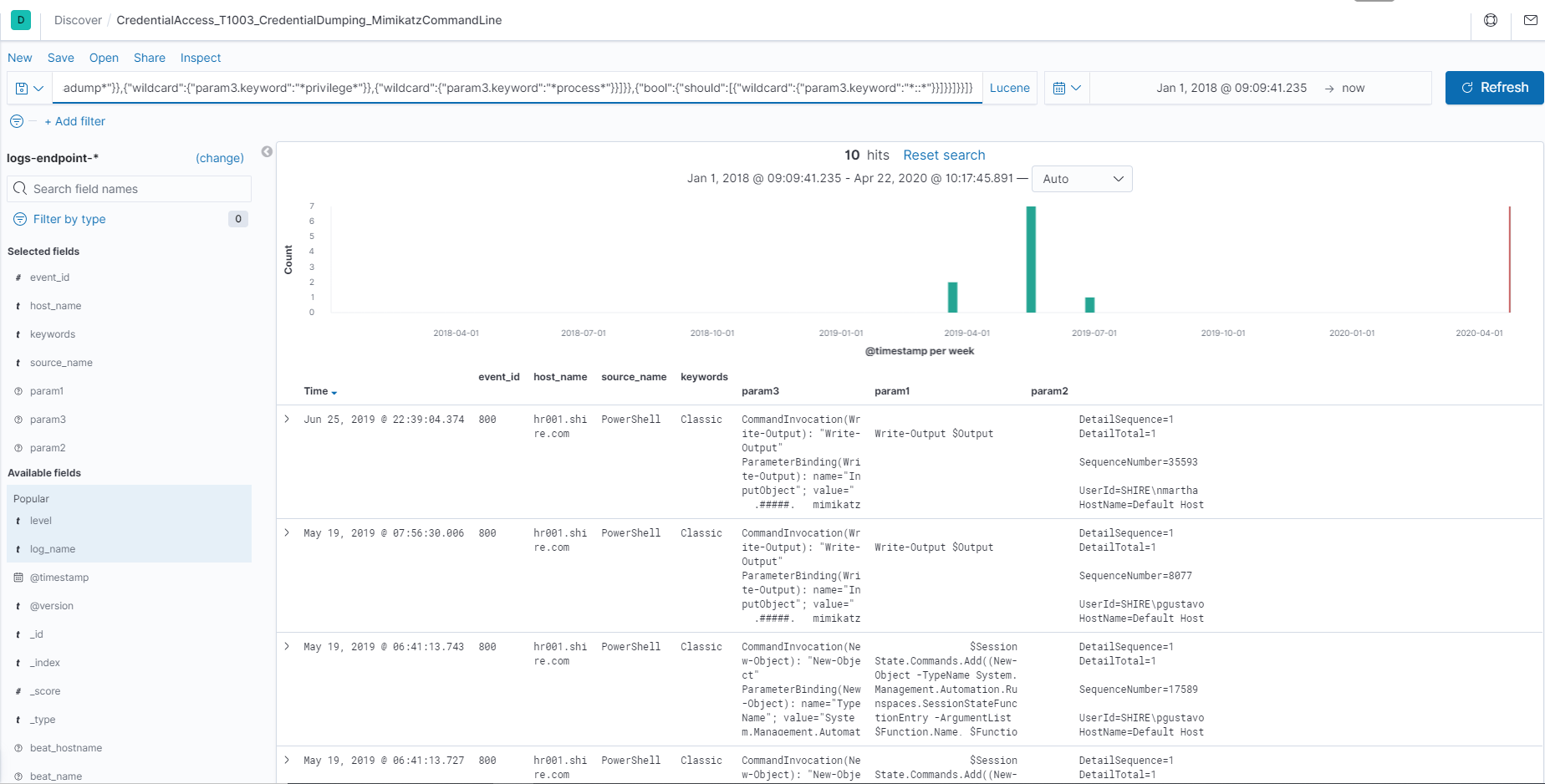






6、

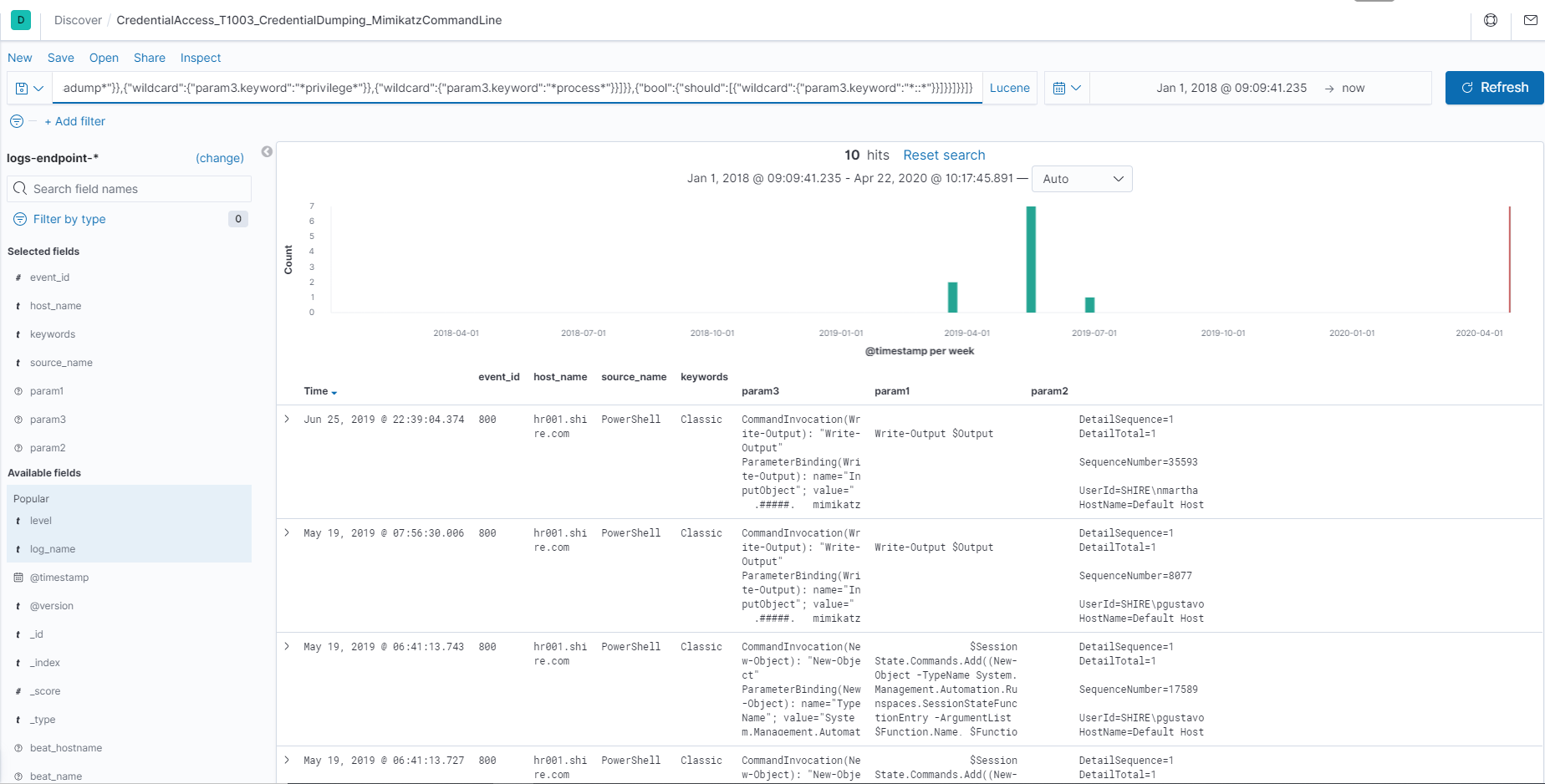
此数据集表示对手使用 Mimikatz 等工具从域控制器远程导出主密钥来。





7、

此数据集表示对手使用 PowerSploit 的 Invoke-Mimikatz 函数，以base64编码的形式从内存中提取 kerberos 票证。

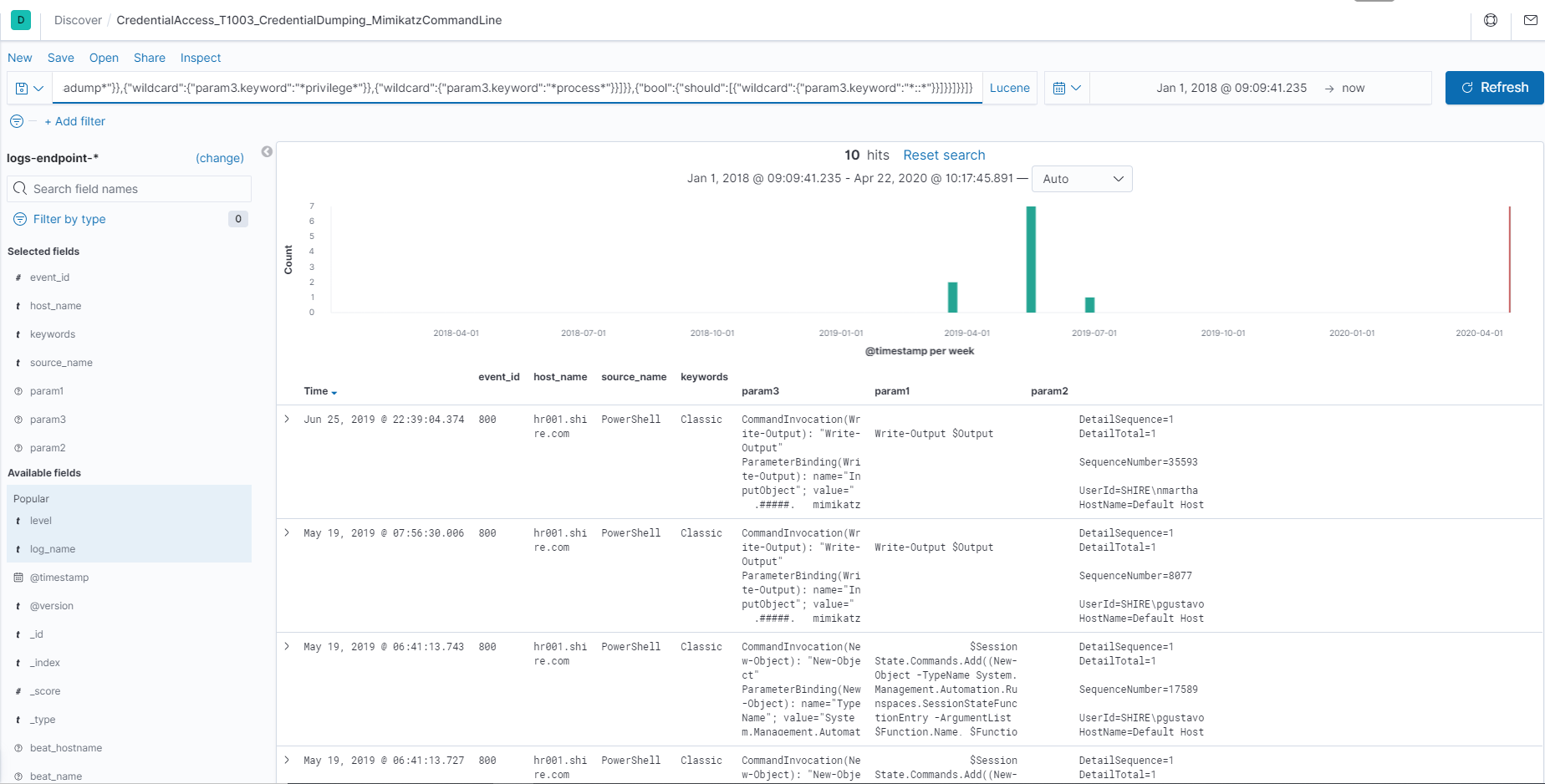


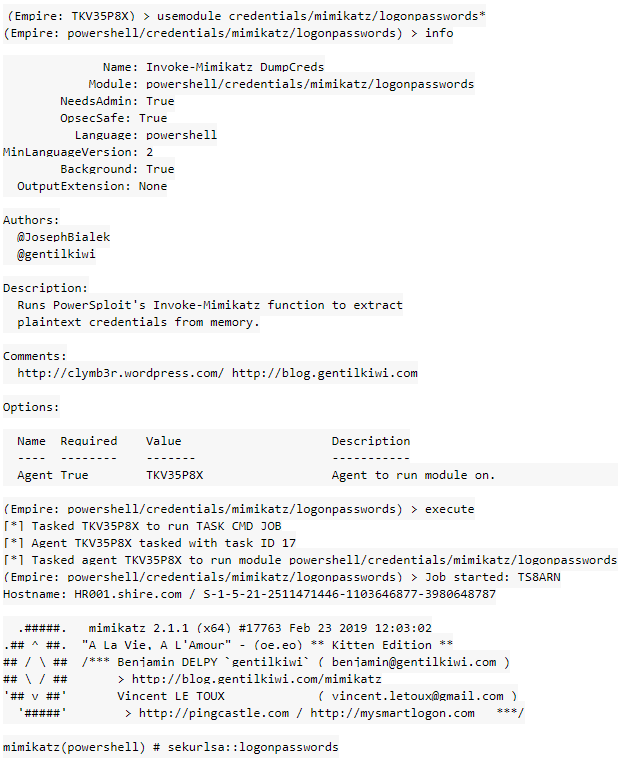




8、

此数据集表示攻击者使用 mimikatz 和模块logonpasswords 从 lsass.exe 的内存内容转储凭据。

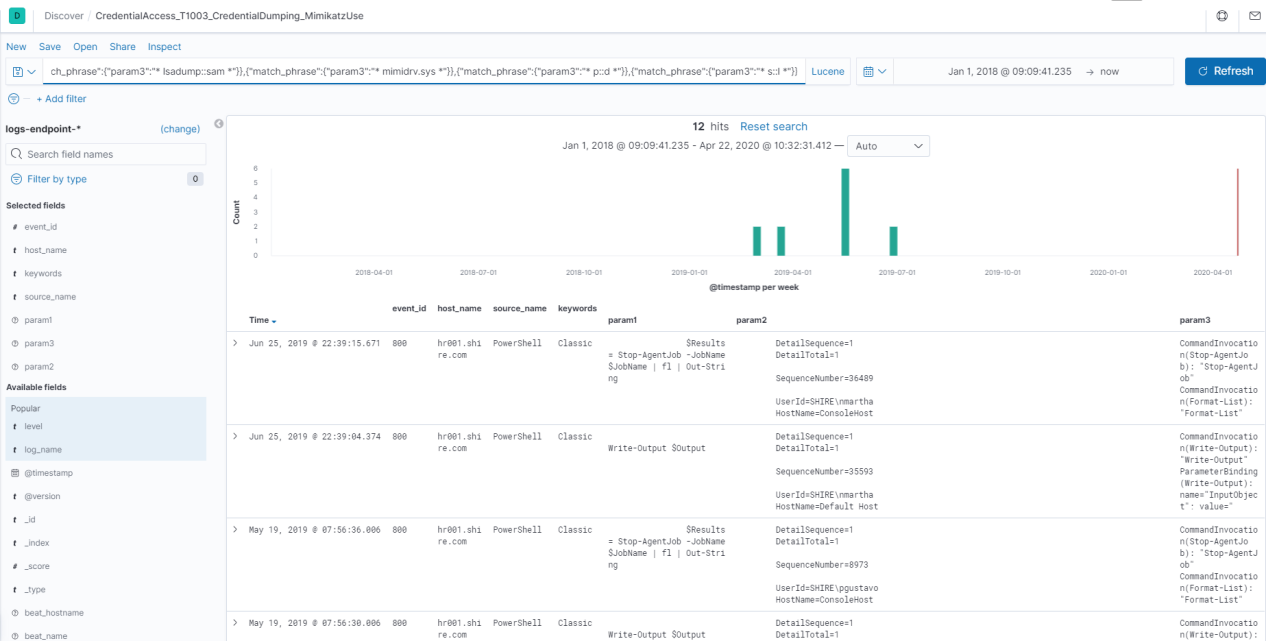


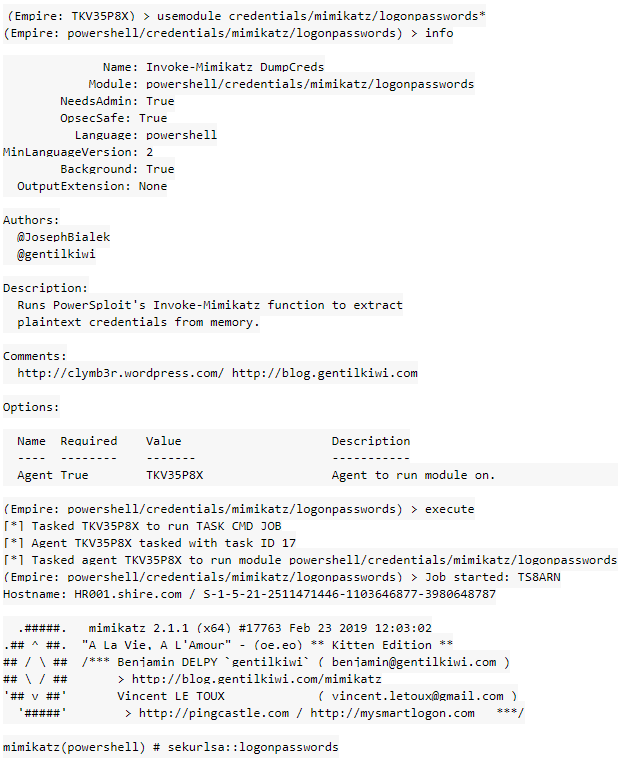




9、

此数据集表示攻击者使用 mimikatz 和模块logonpasswords 从 lsass.exe 的内存内容转储凭据。

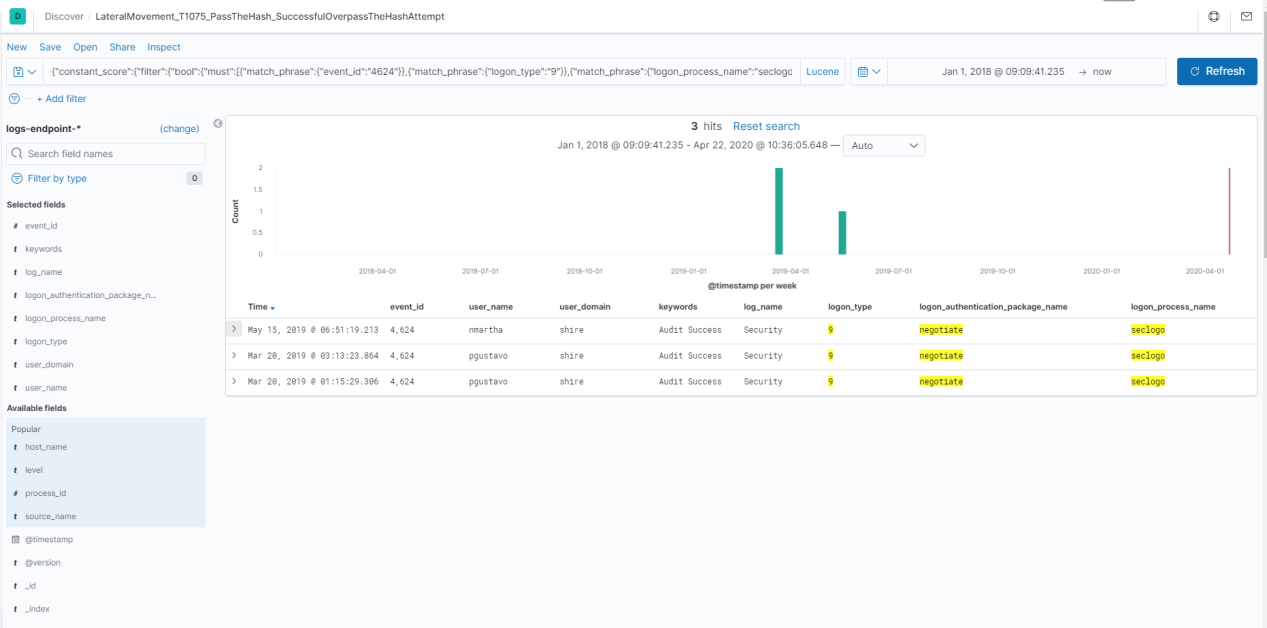


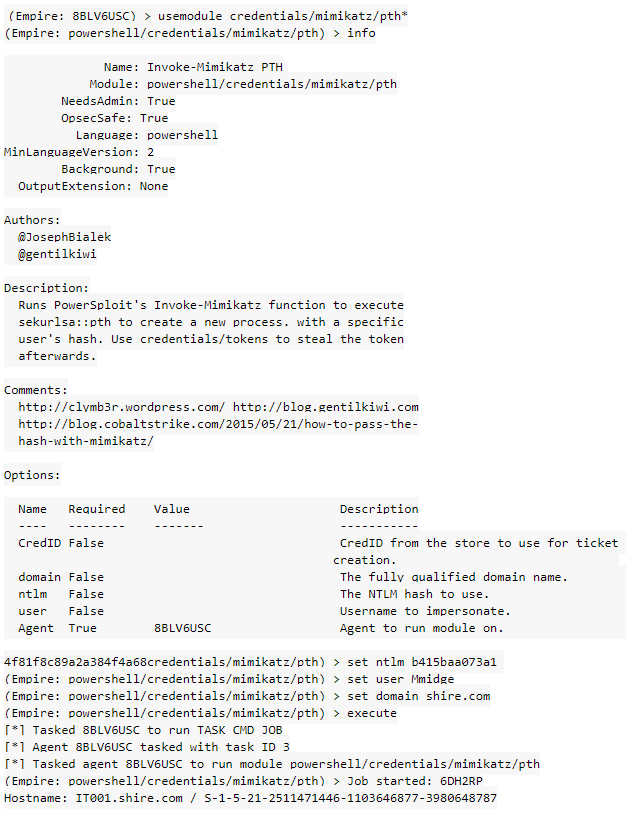


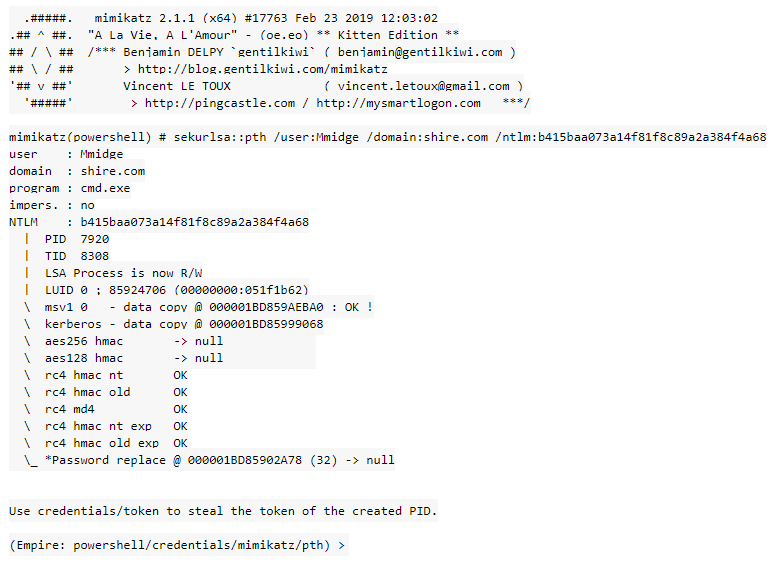


10、

该数据集表示对手将哈希放入充分鉴权后的Kerberos TGT

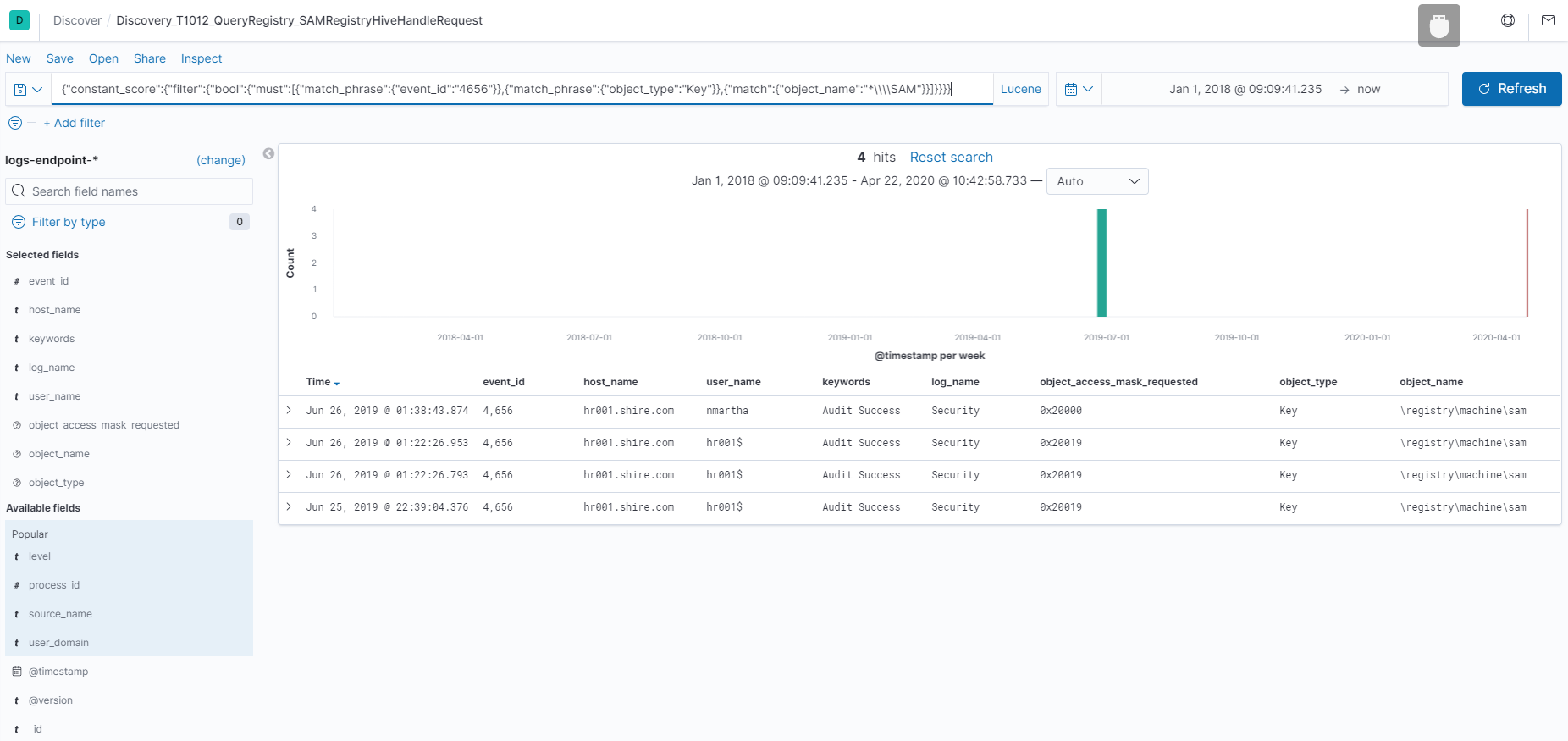


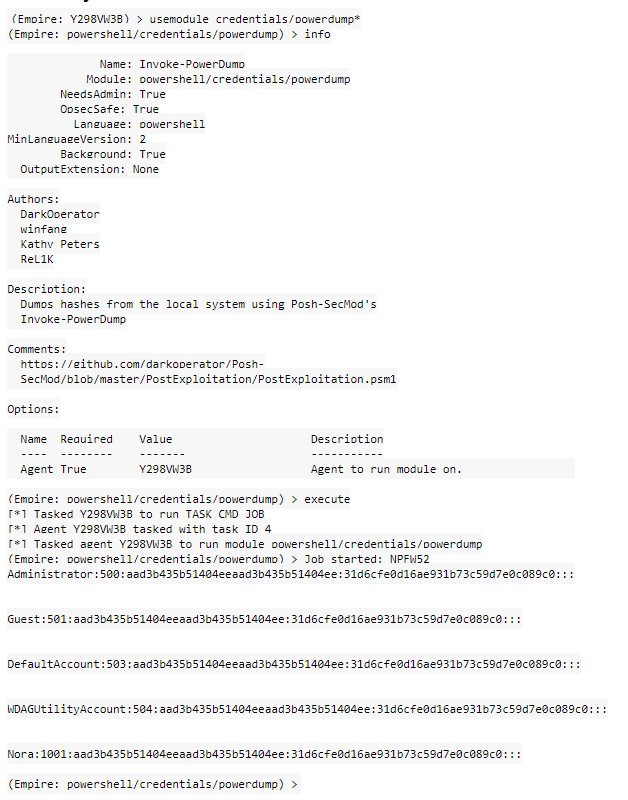




11、

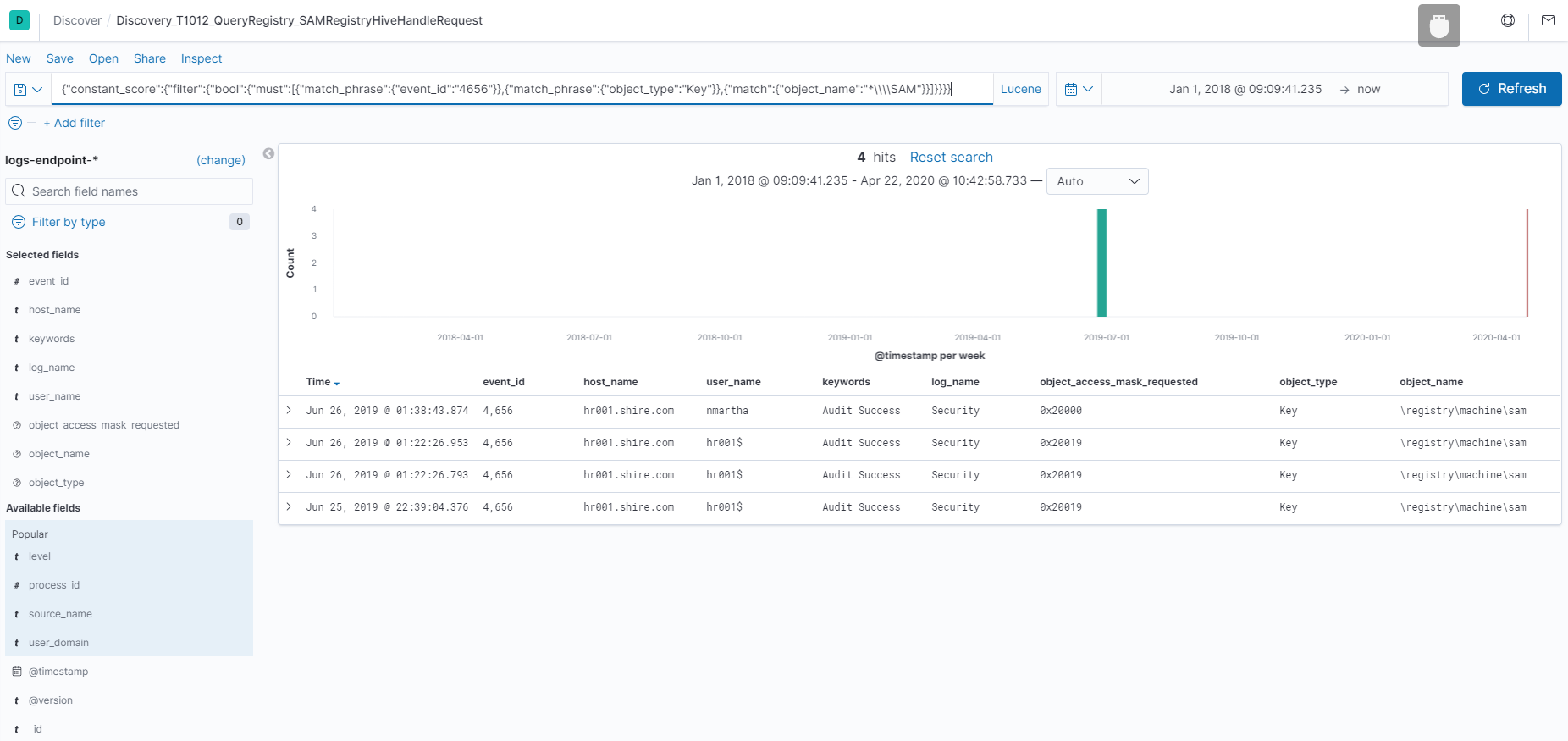
此数据集表示攻击者从注册表项 HKLM:\SAM\SAM\Domains\ 的键中取值。

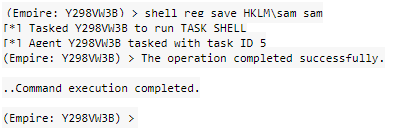




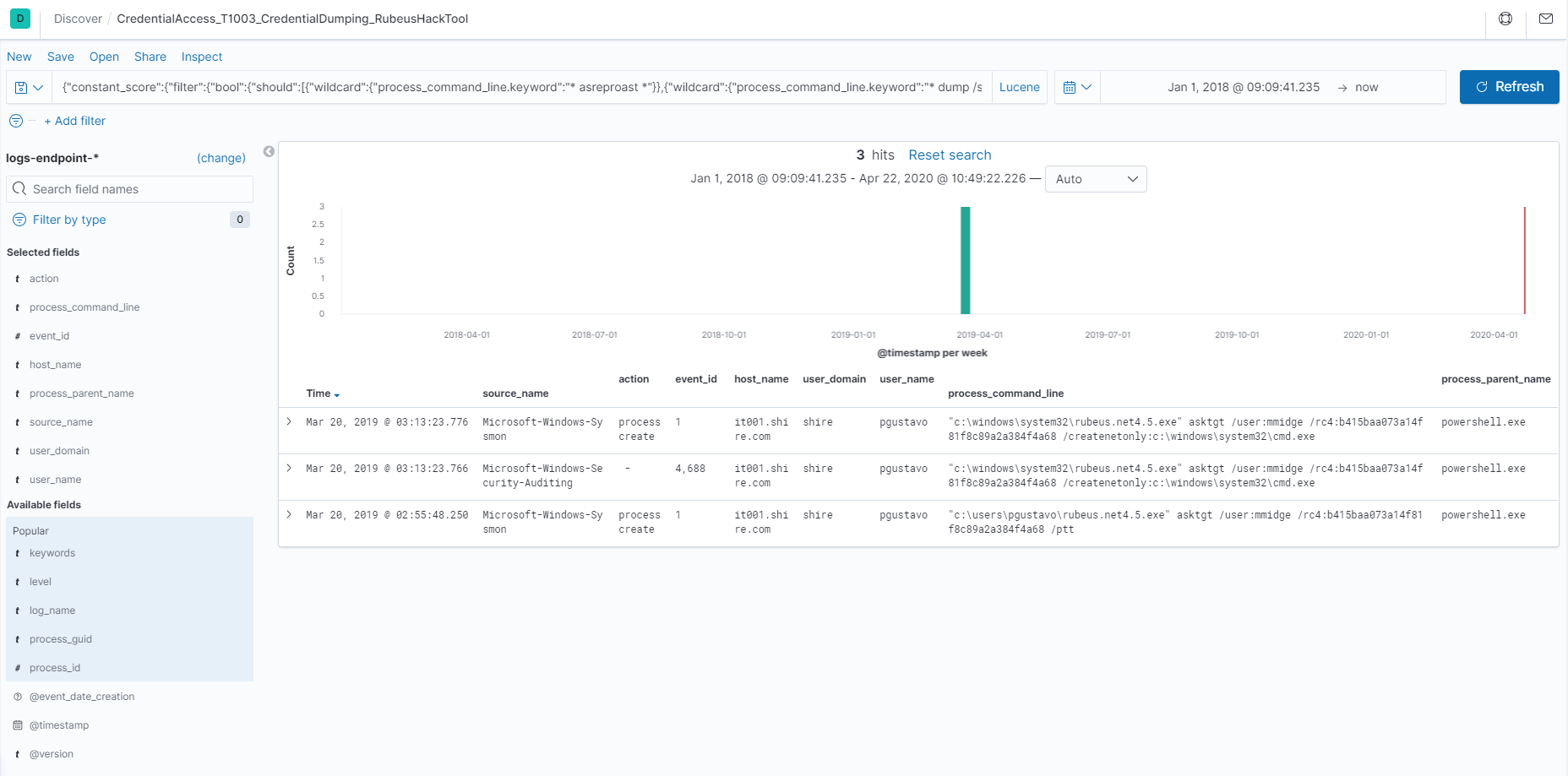
12、

此数据集表示具有管理员权限的攻击者，使用 windows reg 实用程序转储 SAM 注册表配置项。

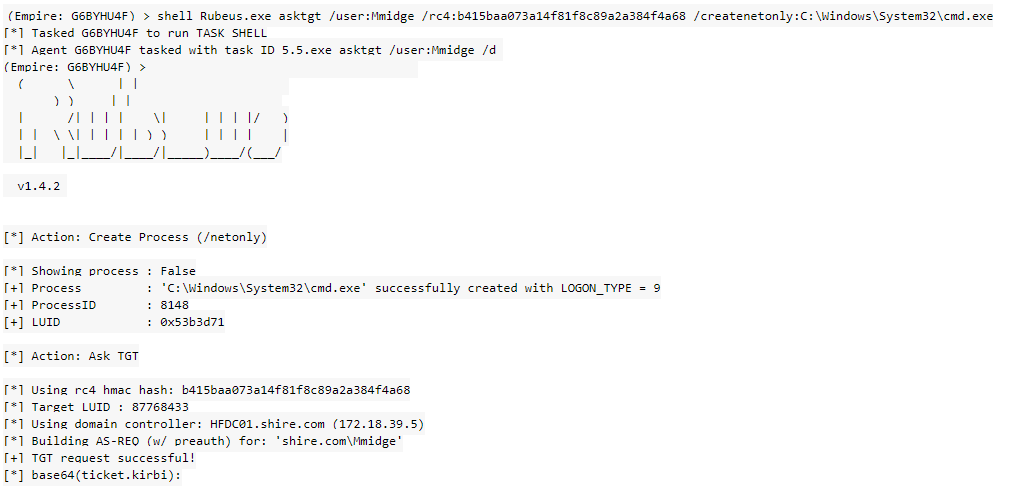




13、

该数据集表示攻击者为特定用户制作原始AS-REQ（TGT请求）流量和加密密钥（/ rc4，/ aes128，/ aes256或/ des）以请求TGT。

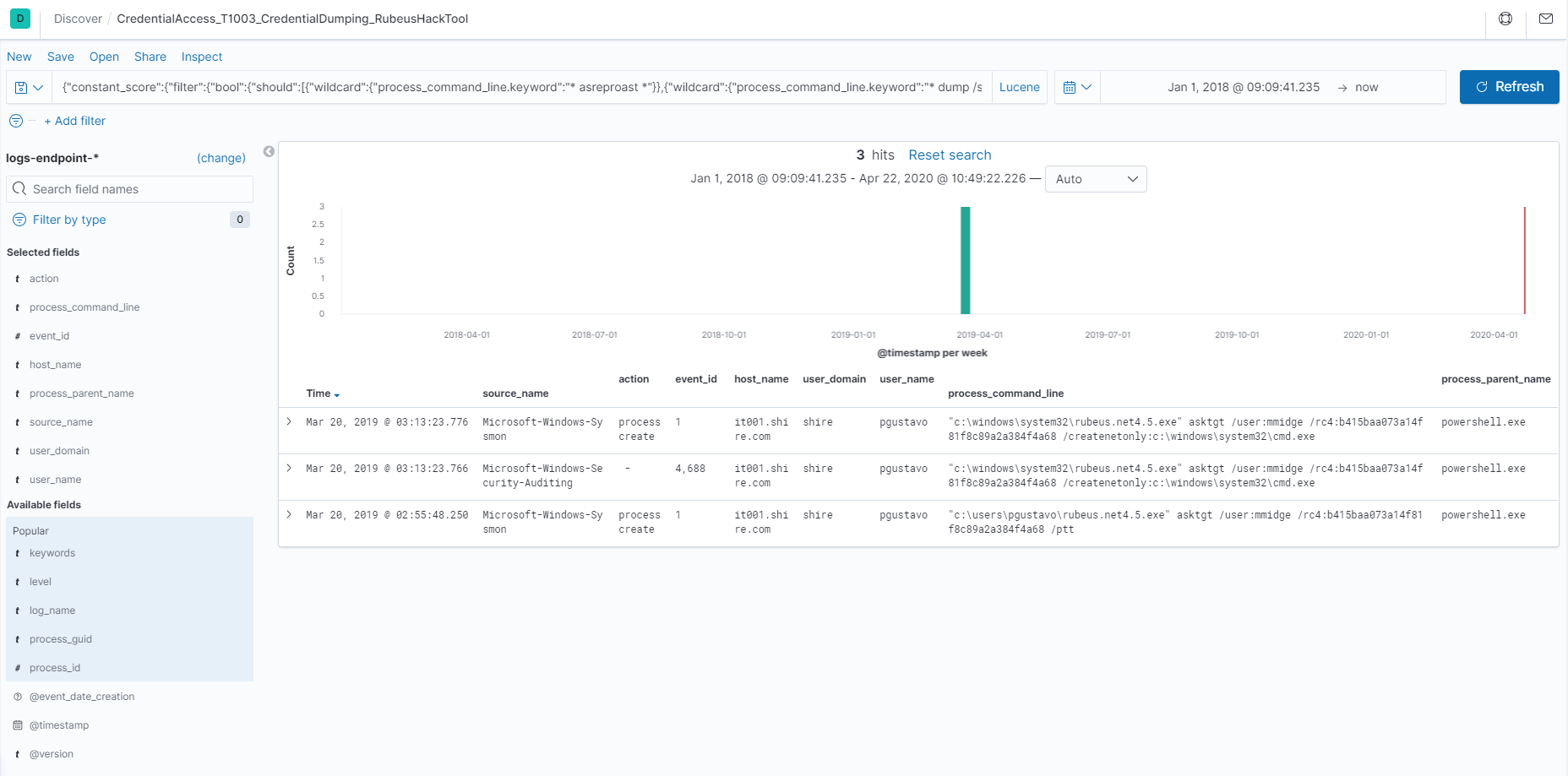


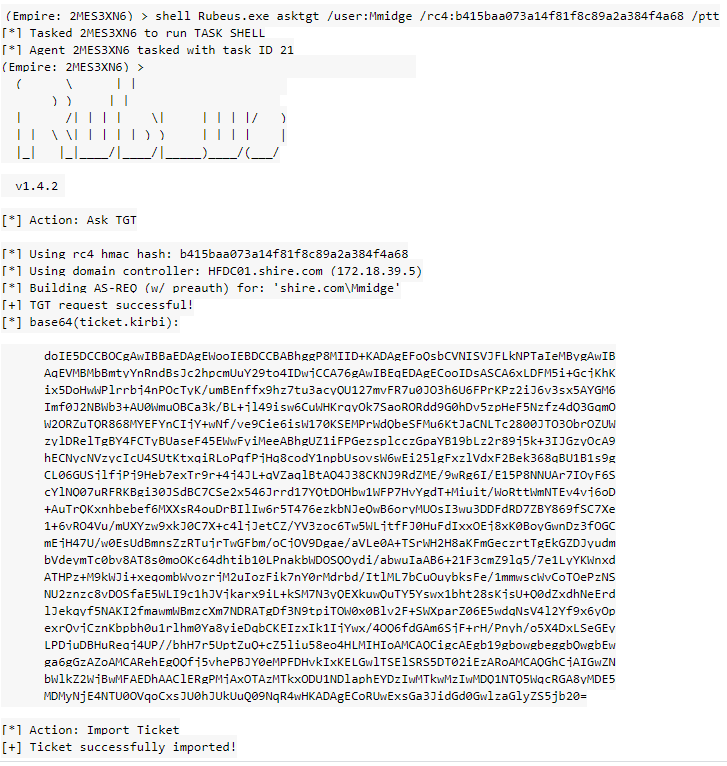


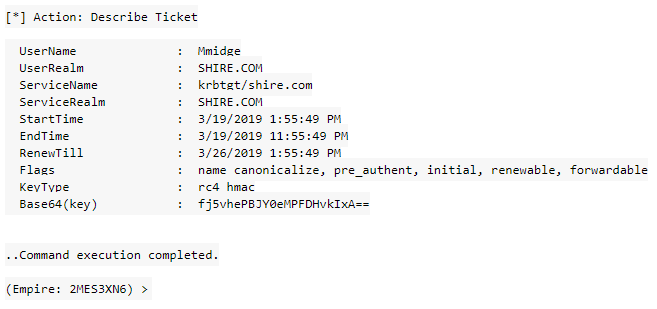


14、

该数据集表示攻击者为特定用户制作原始AS-REQ（TGT请求）流量和加密密钥（/ rc4，/ aes128，/ aes256或/ des）以请求TGT。

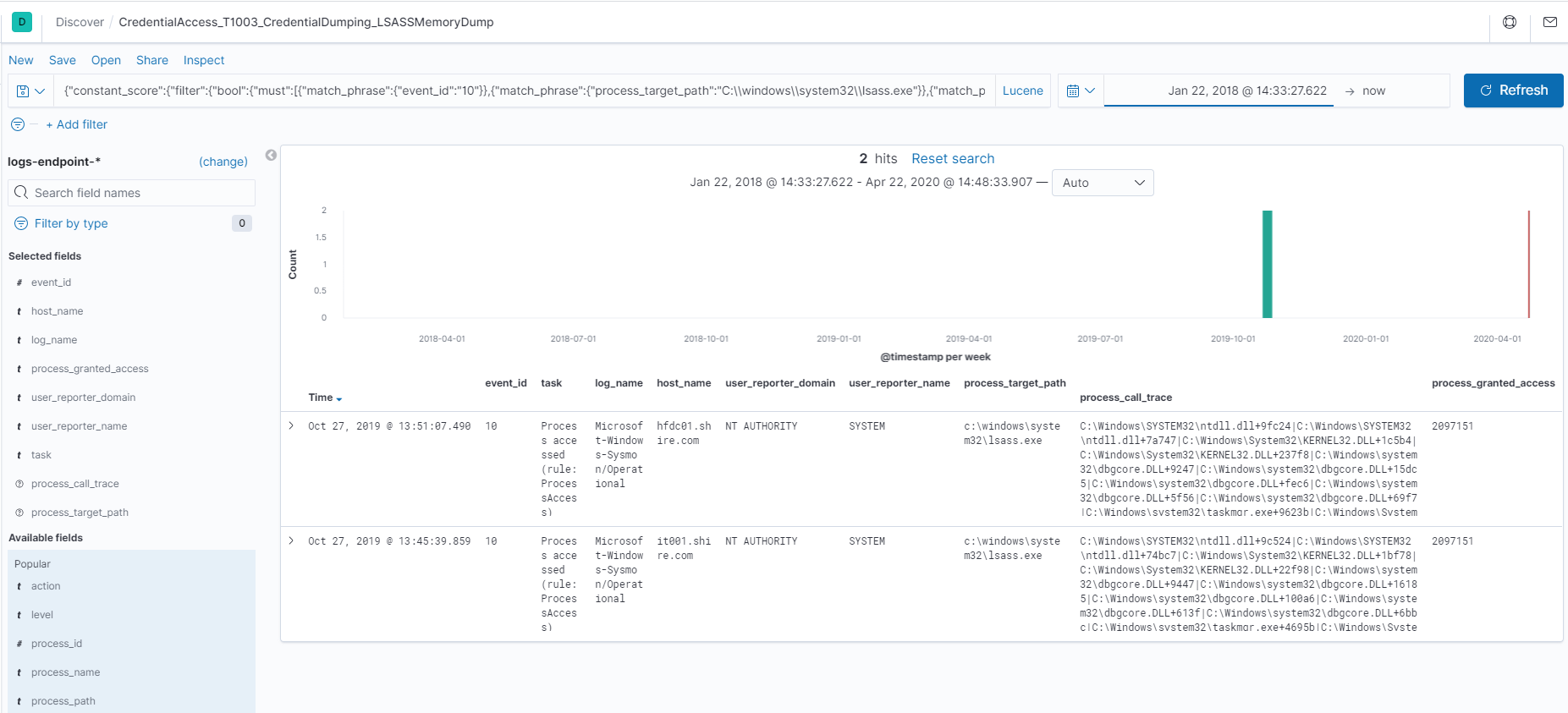


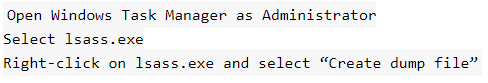




15、

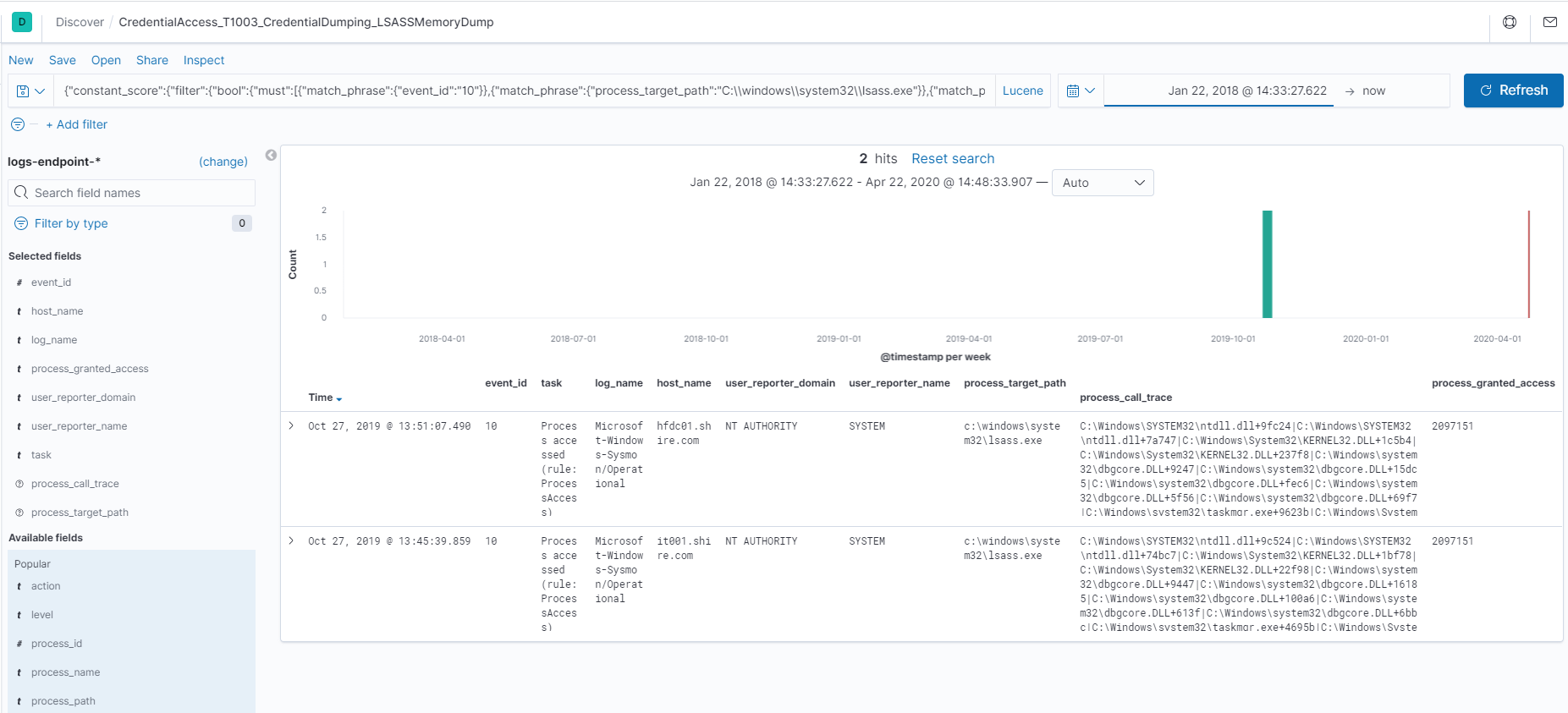
此数据集表示对手以交互方式使用任务管理器，从而转储 lsass 的内存空间。

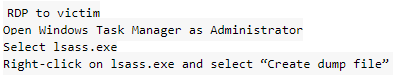




16、

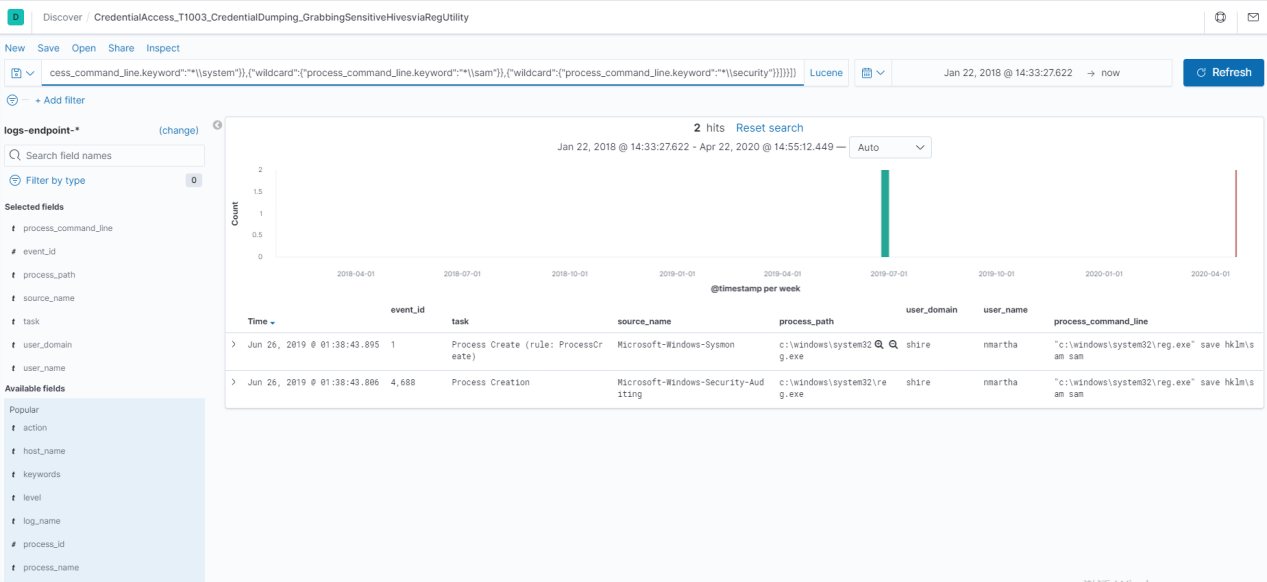
此数据集表示对手以交互方式使用RDP和任务管理器，从而转储 lsass 的内存空间。

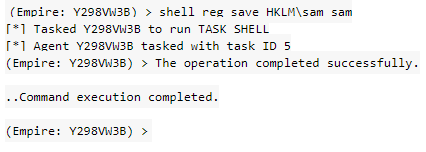




17、

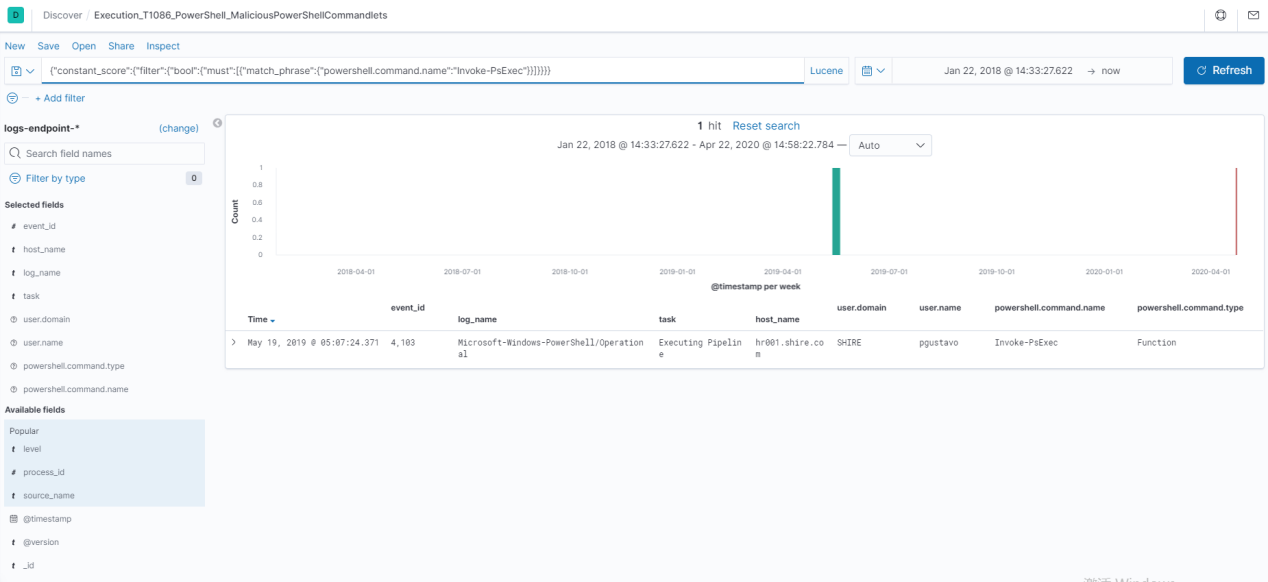
此数据集表示具有管理员权限的攻击者，使用 windows reg 实用程序转储 SAM 注册表配置单元。

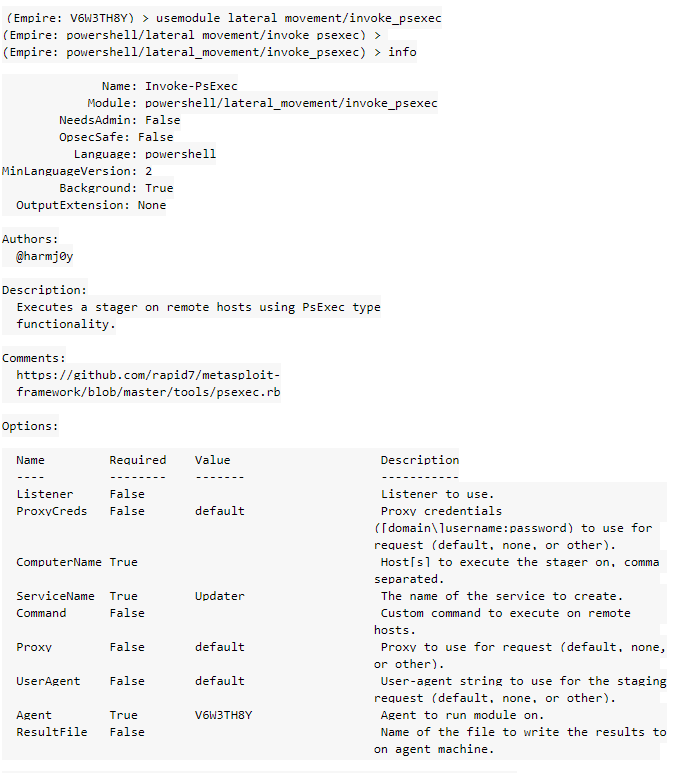


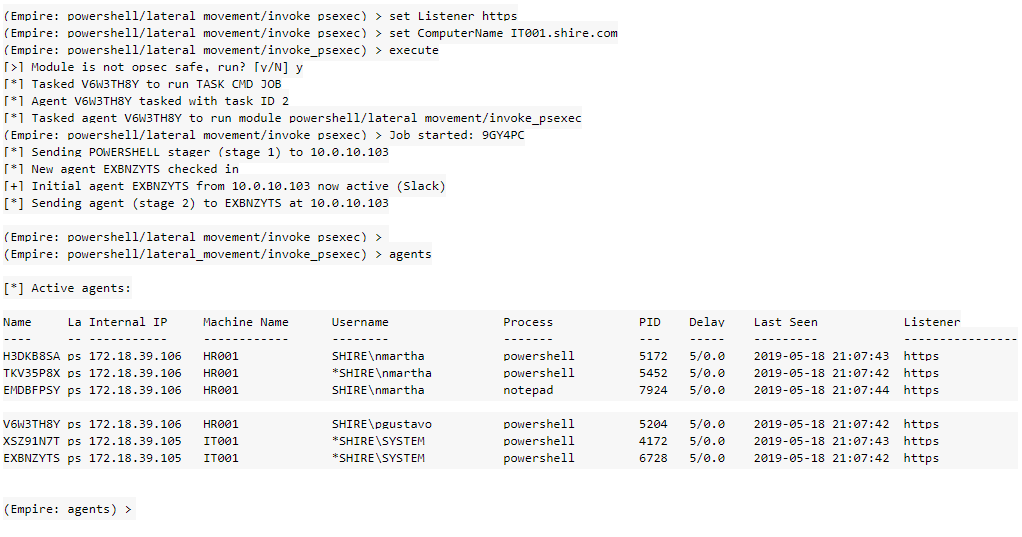


18、

此数据集表示对手通过psexec的方式远程执行恶意代码。

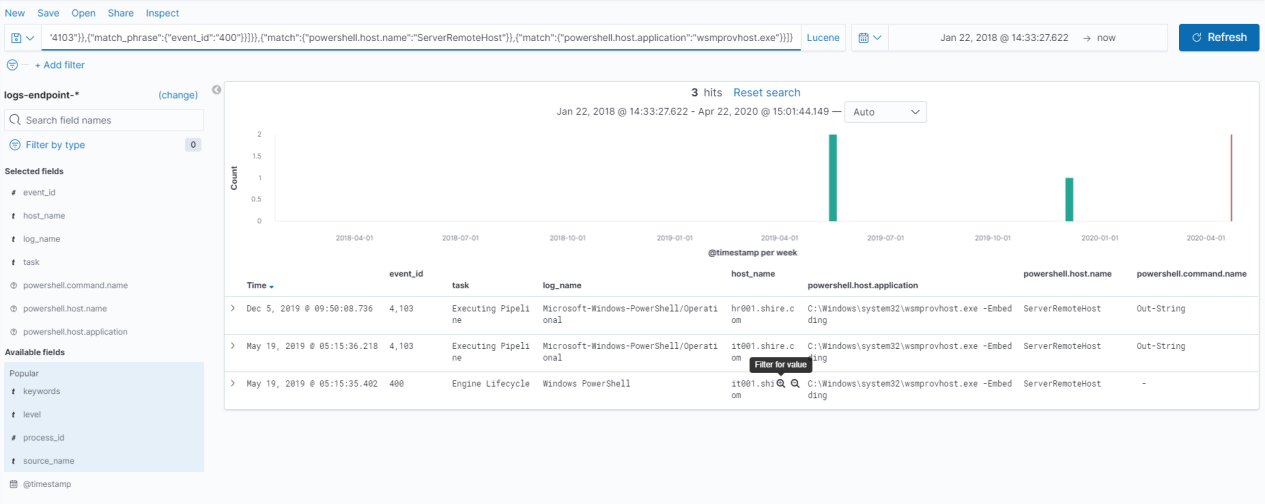


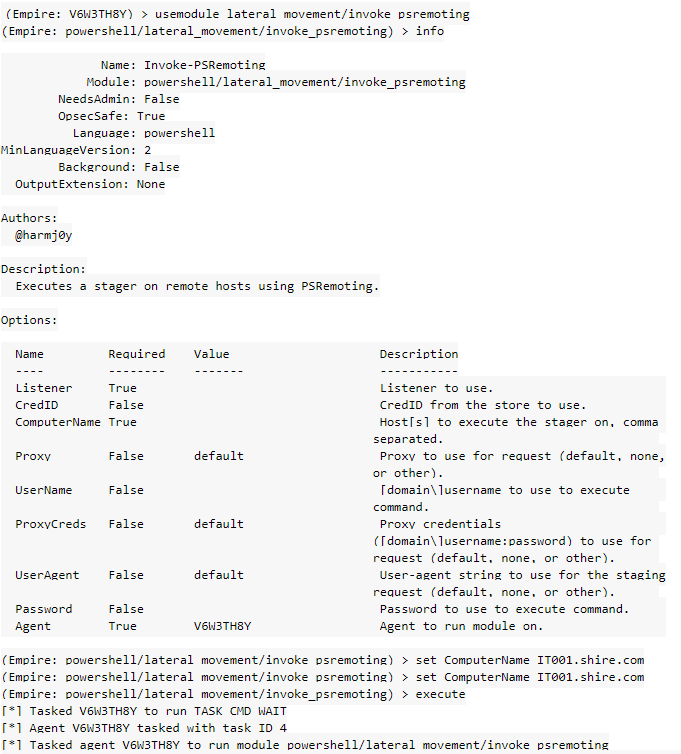


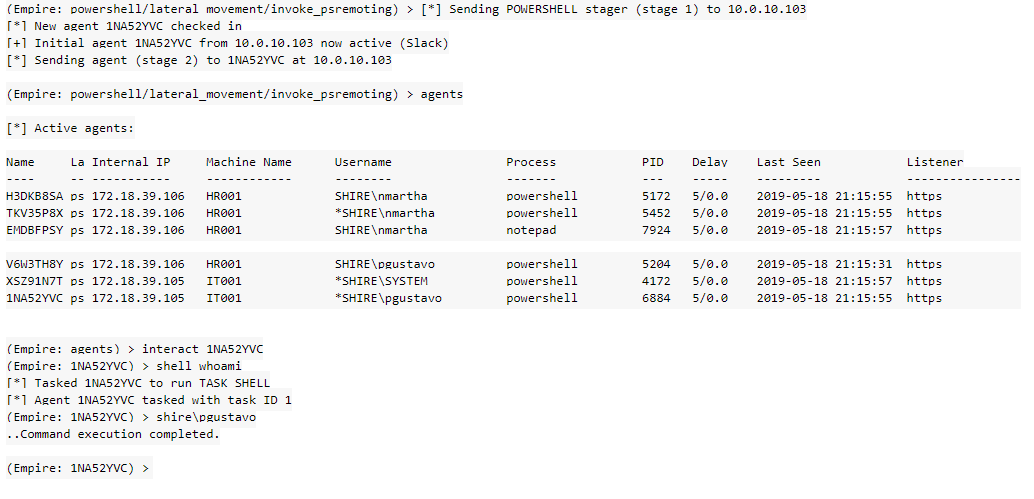


19、

此数据集表示对手在远程主机上使用 PowerShell 远程执行恶意代码。

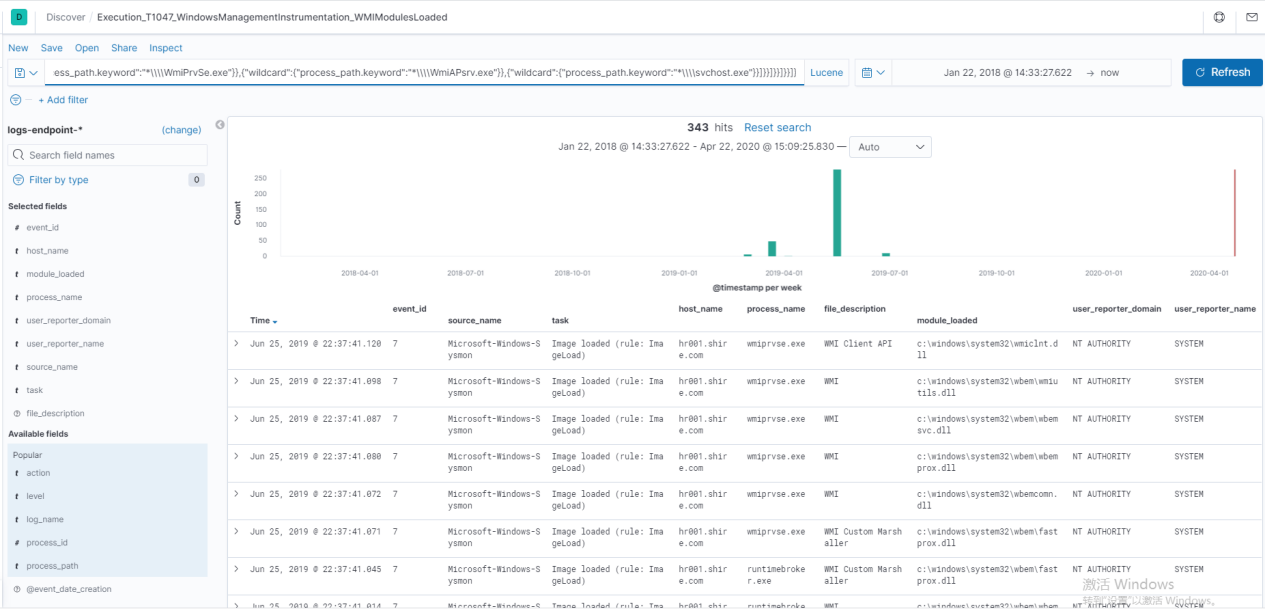


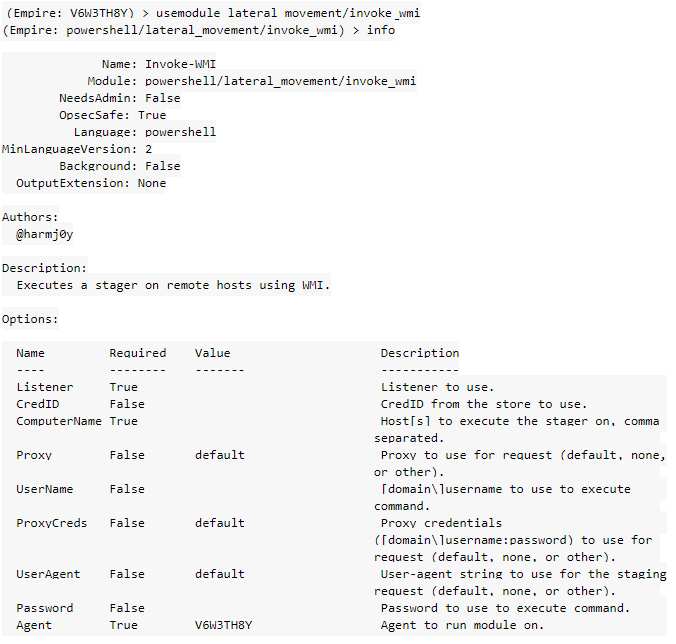


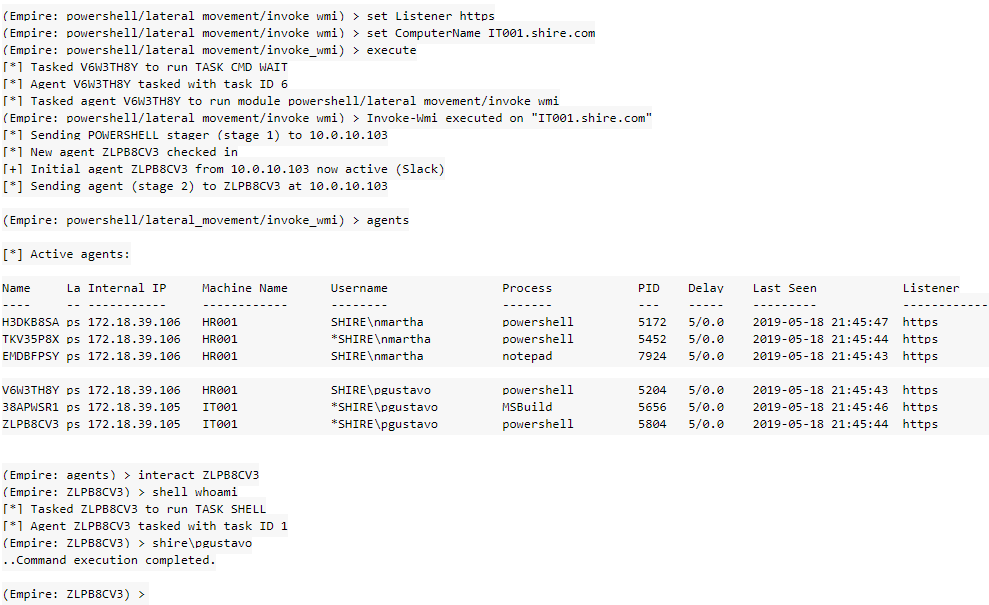


20、

此数据集表示对手使用 WMI 方式远程地在主机上执行恶意代码。

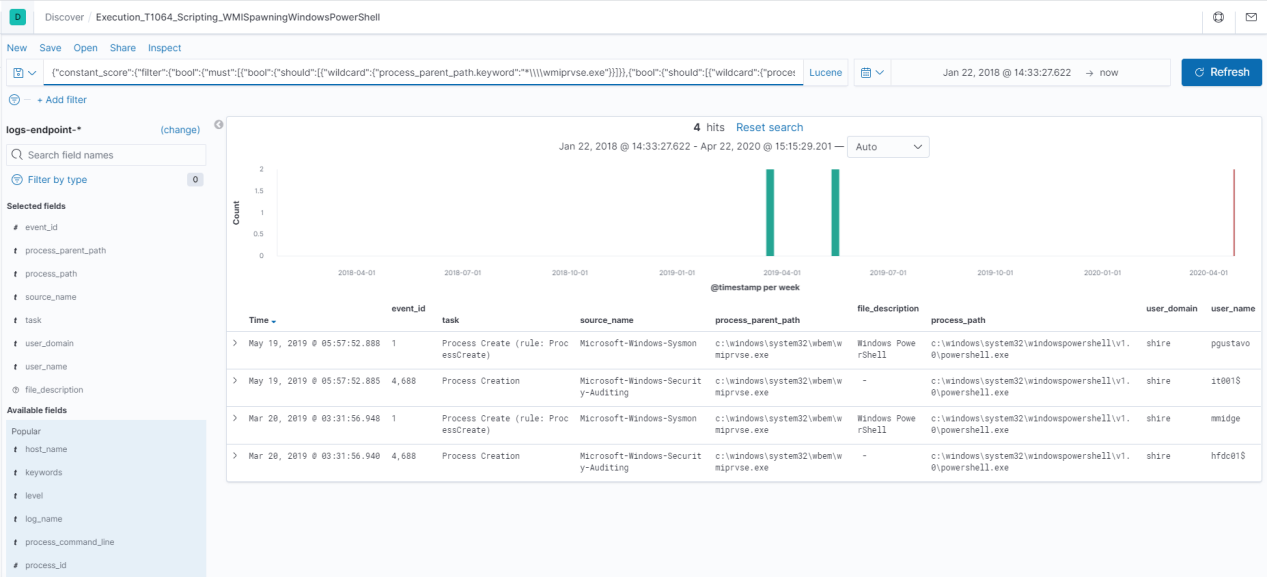


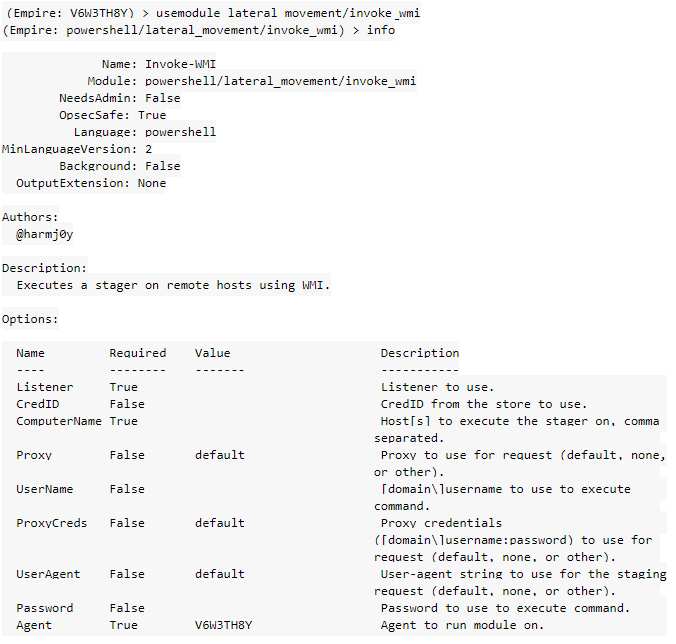


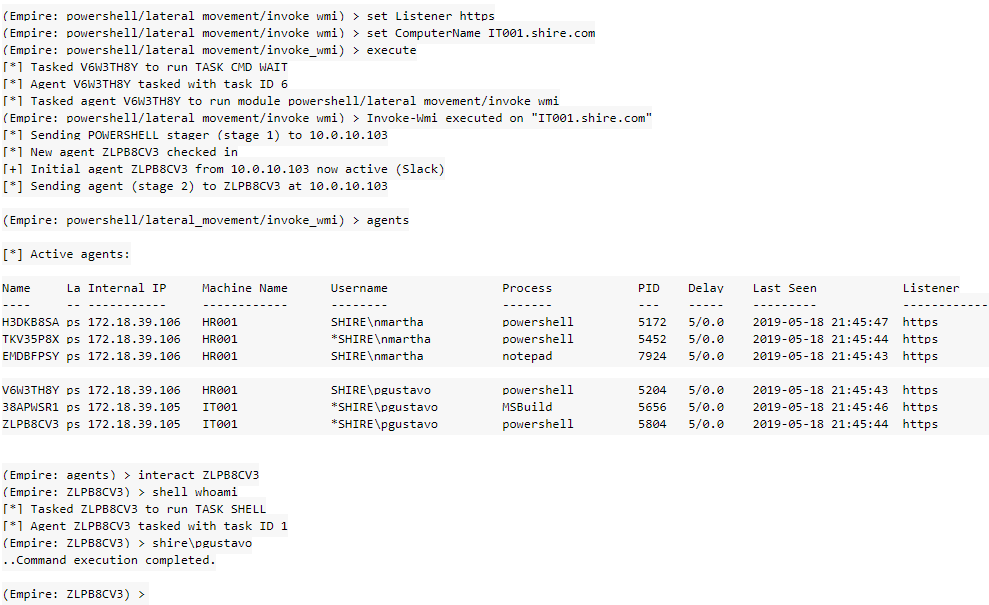


21、

此数据集表示对手使用 WMI 方式远程地在主机上执行恶意代码。

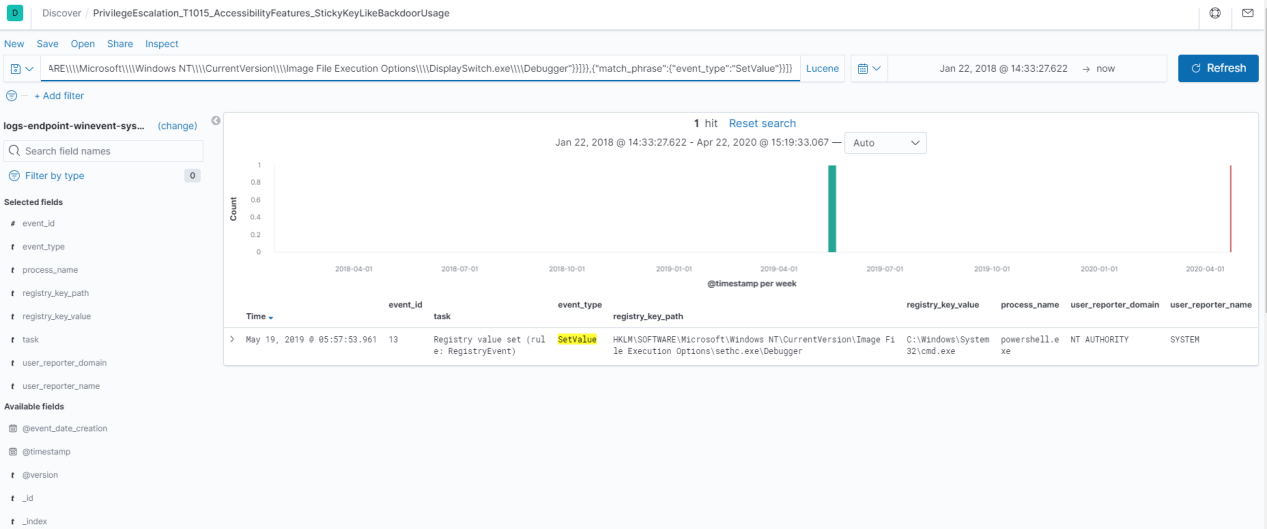


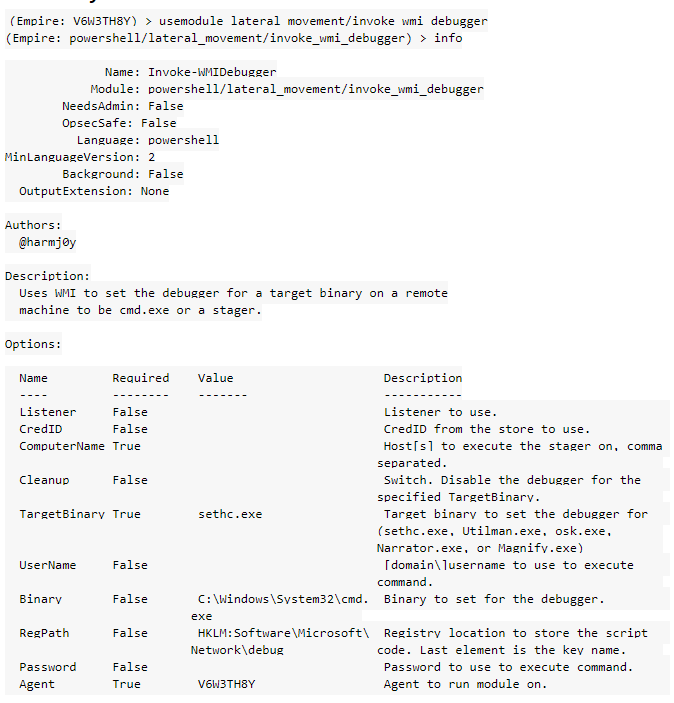




22、

.此数据集表示攻击者通过 WMI 在远程计算机上为目标二进制文件设置调试器。将 sethc.exe 设置为 C：Windows\System32\cmd.exe。

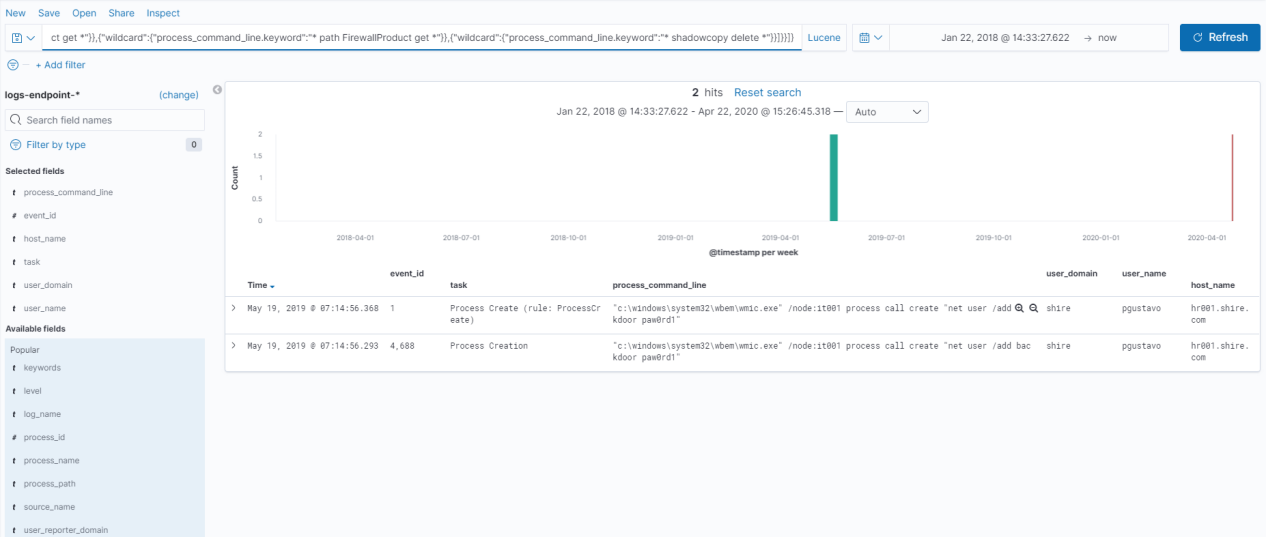


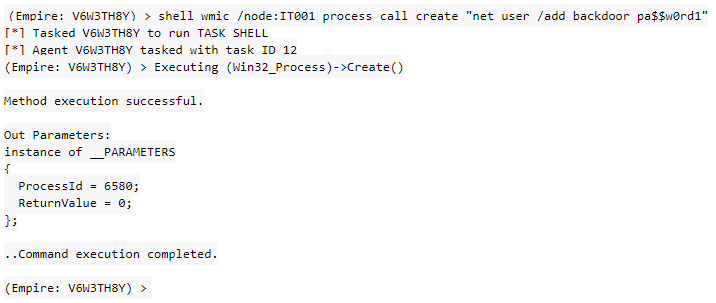




23、

此数据集表示对手通过WMI 在远端主机上远程添加后门用户。





24、

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。