Eval Step：15.B.1

检测目标：T1081 - Credentials in Files

所属tactics：TA0010 – Credential Access

检索日志来源：PowerShell

检索规则

Eval Step：16.E.1

检测目标：T1105 - Remote File Copy

所属tactics：TA0010 – Command and Control Lateral Movement

检索日志来源：PowerShell

检索规则

Eval Step：19.A.

检测目标：T1105 - Remote File Copy

所属tactics：TA0010 – Defense Evasion

检索日志来源：PowerShell

检索规则

Eval Step：19.C.1

检测目标：T1048 - Exfiltration Over Alternative Protocol

所属tactics：TA0010 – Exfiltration

检索日志来源：PowerShell

检索规则

Eval Step：19.D.1

检测目标：T1107 - File Deletion

所属tactics：TA0010 – Defense Evasion

检索日志来源：PowerShell

检索规则

Eval Step：19.D.2

检测目标：T1107 - File Deletion

所属tactics：TA0010 – Defense Evasion

检索日志来源：PowerShell

检索规则

Eval Step：20.A.1

检测目标：T1015 - Accessibility Features

所属tactics：TA0010 – Persistence  
Privilege Escalation

检索日志来源：PowerShell

检索规则

Eval Step：20.B.1

检测目标：T1033 - System Owner/User Discovery

所属tactics：TA0010 – Discovery

检索日志来源：PowerShell

检索规则