Eval Step：12.E.1.6.2

检测目标：T1082 - System Information Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

$Lastupdate = Get-HotFix

Eval Step：12.E.1.7

检测目标：T1012 - Query Registry

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

WIN32\_OperATiNgSYstEm

Eval Step：12.E.1.8

检测目标：T1007 - System Service Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

ServiceStatus = (Get-service | where-object { $\_.DisplayName -eq $ServiceName}).status

Eval Step：12.E.1.9.1

检测目标：T1135 - Network Share Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

win32\_share

Eval Step：12.E.1.10.1

检测目标：T1063 - Security Software Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

Antivirusproduct

Eval Step：12.E.1.10.2

检测目标：T1063 - Security Software Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

$FirewallRule

Eval Step：12.E.1.11

检测目标：T1016 - System Network Configuration Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

win32\_networkadapterconfiguration

Eval Step：12.E.1.12

检测目标：T1049 - System Network Connections Discovery

所属tactics：TA0007 – Discovery

检索日志来源：PowerShell

检索规则

NetConnectionStatus