Categoria	Efecto	Clase evento lanzadora	Filtro adicional	Espacio de nombres	WQL
Enumeración	Enumeración remota de procesos	MSFT_WmiProvider_CreateInstanceEnumAsyncEvent_Pre	Win32_Process	root\cimv2	SELECT * FROM MSFT_WmiProvider_CreateInstanceEnumAsyncEvent_Pre WHERE ClassName='Win32_Process'
Enumeración	Enumeración remota de sistema	MSFT_WmiProvider_CreateInstanceEnumAsyncEvent_Pre	Win32_ComputerSystem	root\cimv2	SELECT * FROM MSFT_WmiProvider_CreateInstanceEnumAsyncEvent_Pre WHERE ClassName='Win32_ComputerSystem'
Movimiento lateral	Ejecución remota de procesos	MSFT_WmiProvider_ExecMethodAsyncEvent_Pre	Win32_Process	root\cimv2	SELECT * FROM MSFT_WmiProvider_ExecMethodAsyncEvent_Pre WHERE ObjectPath='Win32_Process' AND MethodName='Create'
Movimiento lateral	Manipulación remota de registro	MSFT_WmiProvider_ExecMethodAsyncEvent_Pre	StdRegProv	root\cimv2	SELECT * FROM MSFT_WmiProvider_ExecMethodAsyncEvent_Pre WHERE ObjectPath='StdRegProv'
Movimiento lateral	Pass The Hash	__InstanceCreationEvent	Win32_LogonSession	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 1 WHERE TargetInstance ISA 'Win32_LogonSession'
Exfiltración	Exfiltración a traves de espacios de nombres propios	__NamespaceCreation	¿?	root\cimv2	¿ SELECT * FROM __NamespaceCreation ?
Evasión Defensas	Uso de clases WMI propias para almacenamiento de datos	__ClassCreationEvent	¿?	root\cimv2	¿ SELECT * FROM __ClassCreationEvent ?
Evasión Defensas	Uso de proveedor WMI propio	__InstanceCreationEvent	__Provider	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA '__Provider'
Persistencia	Eventos WMI persistentes	__InstanceCreationEvent	__FilterToConsumerBinding	root\subscription	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA '__FilterToConsumerBinding'
Persistencia	Creación de nuevos servicios	__InstanceCreationEvent	Win32_Service	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_Service'
Persistencia	Creación de nuevas tareas programadas	__InstanceCreationEvent	Win32_ScheduledJob	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_ScheduledJob'
Persistencia	Creación de nuevas tareas programadas	__InstanceCreationEvent	MSFT_ScheduledTask	root\Microsoft\Windows\TaskScheduler	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'MSFT_ScheduledTask'
Persistencia	Creación de nuevos elementos de autoarranque	__InstanceCreationEvent	Win32_StartupCommand	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 10 Where TargetInstance ISA 'Win32_StartupCommand'
Persistencia	Creación de nuevos drivers	__InstanceCreationEvent	Win32_SystemDriver	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_SystemDriver'
Elevación de privilegios	Copia de seguridad de NTDS.dit	__InstanceCreationEvent	Win32_ShadowCopy	root\cimv2	SELECT * FROM __InstanceCreationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_ShadowCopy'