WMI

The infrastructure for management data and operations that enables local and remote management of Windows personal computers and servers[1][2]

ID: DS0005
ⓘ Platform: Windows
ⓘ Collection Layer: Host
Contributors: Center for Threat-Informed Defense (CTID)
Version: 1.0
Created: 20 October 2021
Last Modified: 10 November 2021

Version Permalink

Data Components

WMI: WMI Creation

Initial construction of a WMI object, such as a filter, consumer, subscription, binding, or provider (ex: Sysmon EIDs 19-21)

Domain	ID	Name	Detects
Enterprise	T1546	Event Triggered Execution	Monitor for newly constructed WMI Objects that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
	.003	Windows Management Instrumentation Event Subscription	Monitor WMI event subscription entries, comparing current WMI event subscriptions to known good subscriptions for each host. Tools such as Sysinternals Autoruns may also be used to detect WMI changes that could be attempts at persistence. [3] [4] Monitor for the creation of new WMI `EventFilter`, `EventConsumer`, and `FilterToConsumerBinding` events. Event ID 5861 is logged on Windows 10 systems when new `EventFilterToConsumerBinding` events are created.[5]
Enterprise	T1027	Obfuscated Files or Information	Monitor for the creation of WMI Objects and values that may highlight storage of malicious data such as commands or payloads.
	.011	Fileless Storage	Monitor for the creation of WMI Objects and values that may highlight storage of malicious data such as commands or payloads.
Enterprise	T1021	Remote Services	Monitor for newly constructed WMI objects that is often used to log into a service that accepts remote connects.
Enterprise	T1047	Windows Management Instrumentation	Monitor for newly constructed WMI objects that will execute malicious commands and payloads. Analytic 1 - WMI object creation events