Impair Defenses: Indicator Blocking, Sub-technique T1562.006 - Enterprise

Archived: 2026-04-05 15:28:29 UTC

An adversary may attempt to block indicators or events typically captured by sensors from being gathered and analyzed. This could include maliciously redirecting[1] or even disabling host-based sensors, such as Event Tracing for Windows (ETW)[2], by tampering settings that control the collection and flow of event telemetry.[3] These settings may be stored on the system in configuration files and/or in the Registry as well as being accessible via administrative utilities such as PowerShell or Windows Management Instrumentation.

For example, adversaries may modify the `File` value in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security` to hide their malicious actions in a new or different .evtx log file. This action does not require a system reboot and takes effect immediately.[4]

ETW interruption can be achieved multiple ways, however most directly by defining conditions using the PowerShell `Set-EtwTraceProvider` cmdlet or by interfacing directly with the Registry to make alterations.

In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process responsible for forwarding telemetry and/or creating a host-based firewall rule to block traffic to specific hosts responsible for aggregating events, such as security information and event management (SIEM) products.

In Linux environments, adversaries may disable or reconfigure log processing tools such as syslog or nxlog to inhibit detection and monitoring capabilities to facilitate follow on behaviors. [5] ESXi also leverages syslog, which can be reconfigured via commands such as `esxcli system syslog config set` and `esxcli system syslog config reload`.[6][7]

Source: https://attack.mitre.org/techniques/T1562/006