About this site

This site summarizes the results of examining logs recorded in Windows upon execution of the 49 tools which are likely to be used by the attacker that has infiltrated a network. The following logs were examined. Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

A report that outlines and usage of this research is published below. When using Tool Analysis Result Sheet, we recommend you to check the report.

Detecting Lateral Movement through Tracking Event Logs (Version 2)

About Sheet Items

The analysis results for each tool are described in a table format. The content described for each item is explained as follows.

Item	Content
Tool Overview	An explanation of the tool and an example of presumed tool use during an attack are described.
Tool Operation Overview	Privileges for using the tool, communication protocol, and related services are described.
Information Acquired from Log	An overview of logs acquired at tool execution with the default settings (standard settings) as well as when an audit policy is set or Sysmon is installed is described.
Evidence That Can Be Confirmed when Execution is Successful	The method to confirm successful execution of the tool.
Main Information Recorded at Execution	Important information that can be used for the investigation of records in the targeted event logs, registry, USN Journal, MFT, and so on.
Details	All logs to be recorded, except ones included in "Details", are described.
Remarks	Any logs that may be additionally recorded and items confirmed during verification are described.

Notes

Note that a sufficient amount of event logs cannot be acquired with the default Windows settings. In this research, logs that are recorded with the following settings were examined.