Documents

Incident Handling Quarterly Report

Internet Threat Monitoring Quarterly Report

JPCERT/CC Activities Overview Topics

Studies/Research

What's new

- 2024-09-30 JPCERT/CC Eyes:Event Log Talks a Lot: Identifying Human-operated Ransomware through Windows Event Logs
- 2024-09-12 JPCERT/CC Eyes:TSUBAME Report Overflow (Apr-Jun 2024)
- 2024-09-06 Notice of System Maintenance
- 2024-09-05 JPCERT/CC Incident Handling Report [April 1, 2024 - June 30,2024]
- 2024-09-05 JPCERT/CC Internet Threat Monitoring Report [April 1, 2024 - June 30,2024]

Studies/Research

last update: 2017-12-05

Detecting Lateral Movement through Tracking Event Logs

Many recent cyberattacks have been confirmed in which malware infects a host and in turn spreads to other hosts and internal servers, resulting in the whole organization becoming compromised. In such cases, many points need to be investigated. Accordingly, an approach for quickly and thoroughly investigating such critical events, ascertaining the overall picture of the damage as accurately as possible, and collecting facts necessary for devising remedial measures is required.

While the configuration of the network that is targeted by an attack varies depending on the organization, there are some common patterns in the attack methods. First, an attacker that has infiltrated a network collects information of the host it has infected using "ipconfig", "systeminfo", and other tools installed on Windows by default. Then, they examine information of other hosts connected to the network, domain information, account information, and other information using "net" and other tools. After choosing a host to infect next based on the examined information, the attacker obtains the credential information of the user using "mimikatz", "pwdump", or other password dump tools. Then, by fully utilizing "net", "at", or other tools, the attacker infects other hosts and collects confidential information.

For such conventional attack methods, limited set of tools are used in many different incidents. The many points that need to be investigated can be dealt with quickly and systematically by understanding typical tools often used by such attackers, and what kind of and where evidence is left.

For such use of tools, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) extracted tools used by many attackers by investigating recently confirmed cases of targeted attacks. Then, a research was conducted to investigate what kind of logs were left on the server and clients by using such tools, and what settings need to be configured to obtain logs that contain sufficient evidential information. This report is a summary of the results of this research. The details of traces (event logs and forensic architecture) generated upon execution of the tools are

compiled in "Tool Analysis Result Sheet" and published on GitHub.

Tool Analysis Result Sheet
https://jpcertcc.github.io/ToolAnalysisResultSheet/

We hope this document is useful in incident investigation.

Research supported by Internet Initiative Japan Inc.

2017			
Date	title	PDF	PGP
2017-12-05	Detecting Lateral Movement through Tracking Event Logs(Version 2)	PDF Signature 352KB	PGP Signature
2017-06-12	Detecting Lateral Movement through Tracking Event Logs	PDF Signature 2.24MB	PGP Signature

Top

JPCERT CC®
JPCERT Coordination Center
Tozan Bldg. 8F,4-4-2
Nihonbashi-honcho, Chuo-ku
Tokyo 103-0023, Japan