JPCERT/CC Activities Overview Topics

July 1, 2023 - September 30, 2023

JPCERT Coordination Center

October 17, 2023

Activities Overview Topics

－Topic 1－ YAMA customizable malware detection tool released

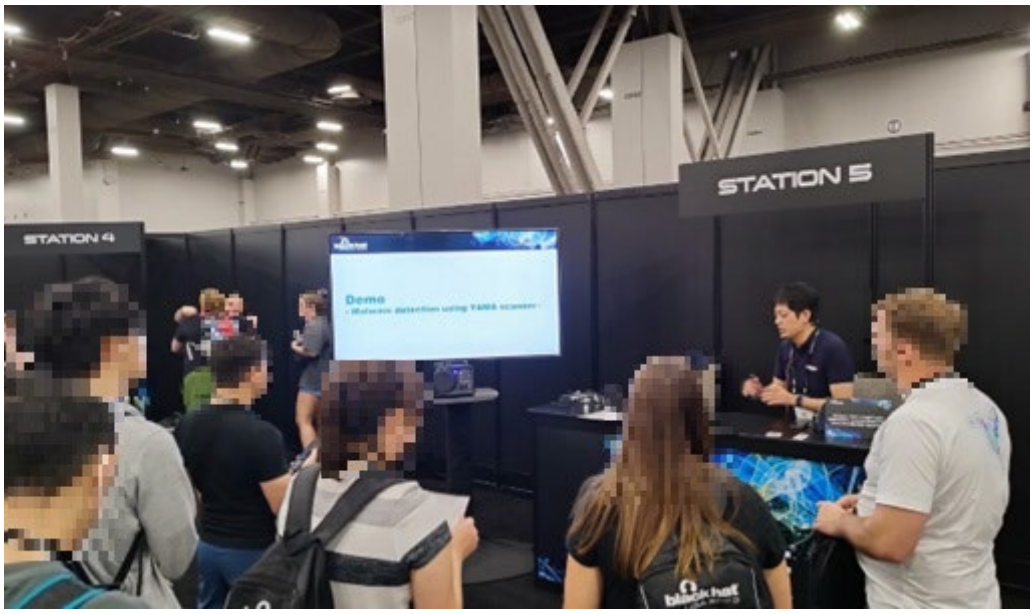
As malware becomes increasingly obfuscated and fileless, it is difficult to detect malware only by assessment with existing file scans. For this reason, it is common to employ malware detection methods using sandboxes and AI, as well as EDR and other technologies to detect malware based on its suspicious behavior after infection.
However, incident responders sometimes encounter malware that cannot be detected even with security products with a sandbox feature or EDR. Whenever this kind of malware is found, an exhaustive investigation needs to be conducted to identify the same types of malware that may be lurking in the network. Since anti-virus software is of no use in such investigations, it was previously necessary to investigate each device manually, which was extremely time-consuming.

To address this issue, JPCERT/CC developed and released a tool called YAMA, which is designed to support malware detection. YAMA uses YARA rules created by the user to conduct memory scans. As such, even fileless malware can be detected if it is deployed on memory. In addition, even if the malware is obfuscated, it may be detected by scanning the deobfuscated malware running on memory. YAMA is available in the following GitHub repository, so please feel free to use it.

GitHub JPCERTCC/YAMA
https://github.com/JPCERTCC/YAMA

We presented this tool at Black Hat USA 2023 Arsenal and exchanged opinions on its features with many security researchers. Based on the feedback, we intend to further enhance its features.

Black Hat USA 2023 Arsenal
https://www.blackhat.com/us-23/arsenal/schedule/#yama-yet-another-memory-analyzer-for-malware-detection-33633



[JPCERT/CC staff presenting YAMA]