Identifies usage of hh.exe executing recently modified .chm files.

b25aa548-7937-11e9-8f5c-d46d6d62a49e

detect

medium

windows

08/08/2019

09/26/2019

Defense Evasion, Execution

T1223 Compiled HTML File

```
sequence with maxspan=1d
   [file where file_name == "*.chm"]
   [process where subtype.create and process_name == "hh.
```

Atomic Red Team: T1223

- Dan Beavin

Previous Next