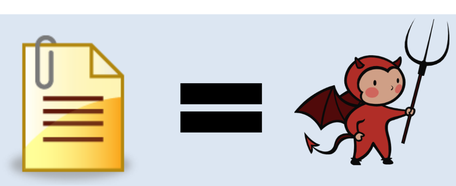
Malware Detection Method Focusing on Anti-Debugging Functions

Kota Yoshizaki and Toshihiro Yamauchi
(*Graduate School of Natural Science and Technology, Okayama University*)
yoshizaki@swlab.cs.okayama-u.ac.jp

Background

Many antivirus software programs detect malware by using a provided signature.



Detectable

Some malware, including Agobot, with Anti-Debugging functions evade detection.

Undetectable

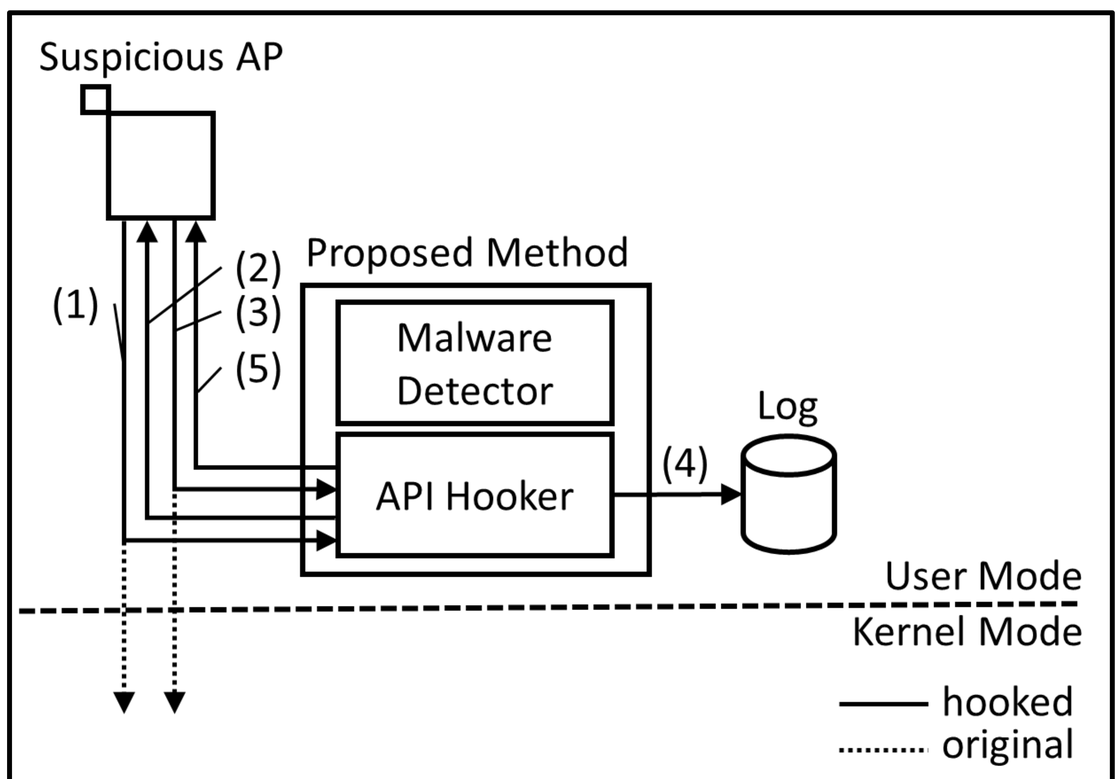
A new method to detect evasive malware is required.

Detectable?

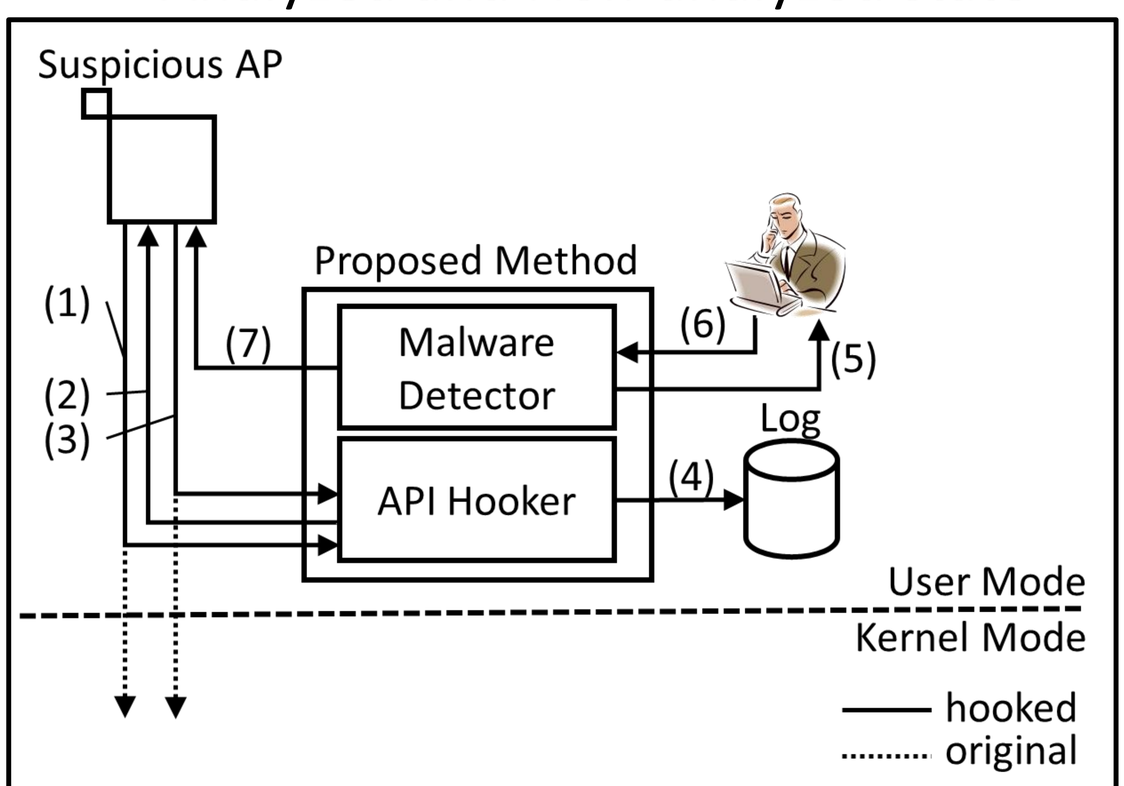
Concept of Proposed Method

Our method executes the AP in both of these two states and focuses on the behavioral difference between them to detect malware.

→ Analyzed and Non-analyzed state



1st execution (analyzed state)



2nd execution (non-analyzed state)

- Benign and malicious APs take evasive measure to evade the analysis.
- API Hooker outputs the log of evasion.

Our method detects evasion

- Benign APs display benign behavior and malicious APs display malicious behavior.
- API Hooker reads the log of evasion and Malware Detector detects malware.

Our method detects malware

Experimental Result

The malware (Agobot) executed debugger detection and evasion when it was in analyzed state, and malicious behavior when it was in non-analyzed state.

```
2013/2/7,16:01:21:294,1752,4028,IsDebuggerPresent,VOID
2013/2/7,16:01:22:567,1752,4028,ExitProcess,VOID
2013/2/7,16:15:25:802,3780,236,IsDebuggerPresent ,VOID
2013/2/7,16:15:26:673,3780,236,RegCreateKeyExA,SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
```

Conclusions

- We proposed a malware detection method that focuses on the Anti-Debugging function.
- An evaluation of our method using malware showed it capable of successfully detecting the malware.