15 February 2006 Article · Web & Cloud · AI

# Behaviour Blocker

**Archived.** This content is no longer updated. It remains available for reference.

**Source** https://technology2.a-sit.at/en/publications/behaviour-blocker/

The Behaviour Blocker demonstrated the detection of malware by analyzing the system calls it employed. It was based on Hidden Markov Models to evaluate the sequences of system calls.

As the demonstrator has been retired and is no longer available for download, we limit the description to a short overview:

- Hidden Markov Models are used to analyse number sequences in various environments, like bioinformatics, analyzing protein sequences, oder language detection.
- the behaviour blocker was a DLL that used hooks to intercept system calls. The demonstrator was limited to detect spy trojans – a particular type of such trojans (Banker and Bancos) has been analyzed.
- Using different verbose levels various information could be extracted.
- The tool was started using

behaviourBlocker -v [verbose level (1-3)] [-o logfile]

- Output:

At Debuglevel 1 just exceptional event have been shown, like when the demonstrator detected malware.

At Debuglevel 2 processes with the expected production probability of the current sequence were shown

At Debuglevel 3 in addition to Debuglevel 2 the actual sequence of system calls Systemcalls is shown.

References

- madshi.net (License)
- BO GAO, HUI-YE MA, YU-HANG YANG. HMMS (HIDDEN MARKOV MODELS) BASED ON ANOMALY INTRUSION DETECTION METHOD. Proceedings of the First

International Conference on Machine Learning and Cybernetics, Beijing, 4-5 November 2002. 0-7803-7508-4/02/$17.00 ©2002 IEEE

- L. R. Rabiner. A tutorial on hidden Markov models and selected applications in speech recognition. Proceedings of the IEEE, 77(2):257?286, 1989
- E. Fosler-Lussier. Markov models and hidden markov models: A brief tutorial, 1998.
- P. Blunsom. Hidden markov models, 2004.

This tool is no longer available for download.