15. Februar 2006 Artikel · Web & Cloud · KI

Behaviour Blocker

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/behaviour-blocker/

Der Behaviour Blocker dient zur Erkennung von Malware anhand der aufgerufenen Systemcalls. Er basiert auf Hidden Markov Modellen mit denen die Sequenzen der Systemcalls evaluiert werden.

Anleitung

- Hidden Markov Modelle: ... dienen zur Analyse von Zahlensequenzen verschiedenster Art und werden in vielen unterschiedlichen Bereichen, wie zum Beispiel in der Bioinformatik, zum Erkennen von Proteinsequenzen, oder in der Spracherkennung, verwendet.

HMM's stellen eine doppelt-statistische Methode dar, wobei der darunterliegende statistische Prozess nicht sichtbar ist, daher auch der Name.

- Der Behaviour Blocker besteht aus einer DLL, welche die Hooks (für das Abfangen und Weiterleiten der Systemcalls) beinhaltet, und einem Hauptprogramm, welches die Evaluierung der Systemcall-Sequenzen durchführt.

Die Demoversion beschränkt sich auf das Erkennen von Spy-Trojanern, wobei nur eine Untergruppe aller möglichen Ausprägungen (Banker und Bancos) untersucht wird. Die Laufzeit der Demoversion ist auf 10 min beschränkt. Je nach „Verbose Level" werden unterschiedliche Informationen ausgegeben. Möglich sind die Levels 1 (Default) bis 3 (-v 2 bzw. -v 3). Zusätzlich kann mittels der Option "-o" [Dateiname] die Ausgabe in ein gewünschtes File im aktuellen Verzeichnis geschrieben (angehängt) werden.

Die Scoringpoints werden beim Überschreiten bestimmter Schwellwerte durch die Produktionswahrscheinlichkeit (prod prob) inkrementiert. Erreichen diese den

Wert 5 (Demoversion), deutet dies auf einen Schadprozess der oben angeführten Varianten hin.

- Nach dem Download sind die Dateien madCHooks.dll und msvcr71.dll (sollte kein Visual Studio installiert sein) in das Verzeichnis \windows\system32 zu kopieren, nicht aber bBlockerHooks.dll
- Aufruf:

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

- Ausgabe:

Debuglevel 1: Hier werden nur besondere Ereignisse ausgegeben bzw. sollte ein Prozess als mögliche Malware erkannt worden sein.

Debuglevel 2: Hier werden die Prozesse mit den aktuellen Produktionswahrscheinlichkeiten für die aktuelle Sequenz an Systemcalls ausgegeben.

Debuglevel 3: Wie Debuglevel 2, nur wird zusätzlich die aktuelle Sequenz an Systemcalls ausgegeben, für welche die Produktionswahrscheinlichkeit erreicht wird.

- Warnungen:

Der behaviourBlocker ist eine Demoversion. Es wird für die Funktionalität nicht garantiert. Es wird keinerlei Haftung für Schäden oder Datenverluste, die durch die Benutzung des behaviourBlockers oder der mitgelieferten Dateien entstehen, übernommen.

Referenzen

- 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.

Dieses Tool steht nicht mehr zum Download bereit.