Reasoning Model API

Draft

February 2009

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

Executive Summary

This report describes the Application Programming Interface (API) for interacting with the reasoning model for bot detection. The reasoning model is implemented as a DLL, and the API provides for the creation and destruction of models, the input of indicator values, and polling the model's output node (probability of bot infection). Possible enhancements to the API are noted as well. The model itself is described in other project documentation.

The contents of this report were produced by SAIC, Inc., under to contract to HBGary, Inc., for contract number NBCHC80048. SBIR Data Rights apply.

Overview

The reasoning model API provides the following capabilities:

- Create a new model (i.e., a new host)
- Destroy a model (i.e., when analysis is complete)
- Input indicator values
- Query the current Bot Likelihood, P(bot), for a particular model

Future capabilities may include:

- Dump a model's values (i.e., for logging or archiving)
- Query for the confidence a model has for the current P(bot)
- Query for the submitted evidence (indicators) supporting and contradicting the current P(bot)
- Query for the unsubmitted evidence (indicators) most likely to have an impact on P(bot)

The sections that follow provide details for each API call.

CreateModel(hostID)

hostID = char[16]

returns = int:
0 = failure
1 = success

DestroyModel(hostID)

hostID = char[16]

returns = int:
0 = failure
1 = success

SetIndicator(hostID, indicatorID, indicatorValue)

hostID = char[16]
indicatorID = char[80]
indicatorValue = real[0,1]

returns = int:
0 = failure
1 = success

GetBot(hostID)

hostID = char[16]

returns = real[0,1]