Design and Implementation of NECOMAtter

Takuji Iimura

The University of Tokyo

Motivation

NECOMAtter provides a holistic view for operators to grasp incidents, based on curation of threat information from security devices, insight of security analyst/operators.

It also facilitates the operators to initiate incident response to each device.

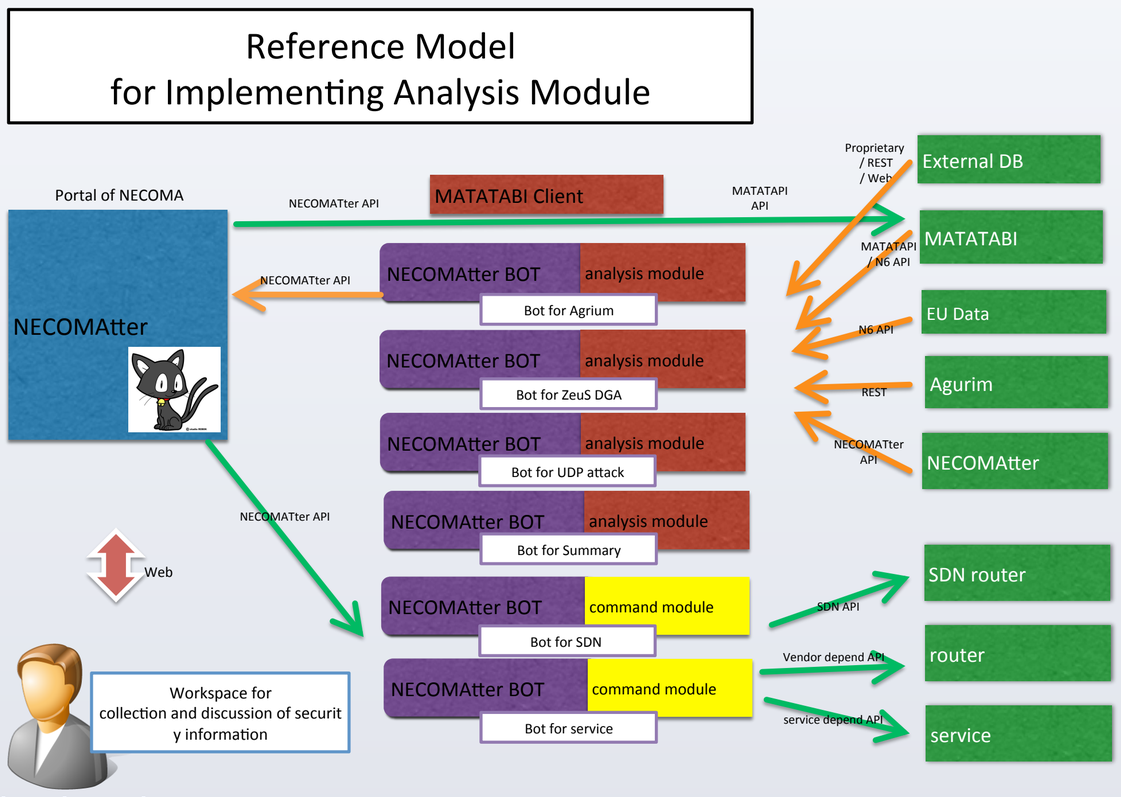
Challenges

1. large amount and diverse of data
2. various stakeholders with different expertise
3. ad-hoc collaboration is key
4. improvised defences against improvised attacks

Use Case

The users of NECOMAtter can be classified as follows.

- User: security operator/analyst
- Agent: NECOMAtter bot for providing cyber threat information
- Executor: NECOMAtter bot for executing cyberdefense at PEP



Agent

This NECOMAtter bot inputs the cyber threat information to NECOMAtter (= ***mew***).

It also has a function of streaming watch to react mew from users and other bots, and provides related information and/or its pointer that the bot has.

Executor

This NECOMAtter bot monitors users' mew to receive commands to security devices (PEP), and operate the devices to execute cyberdefense.

Users

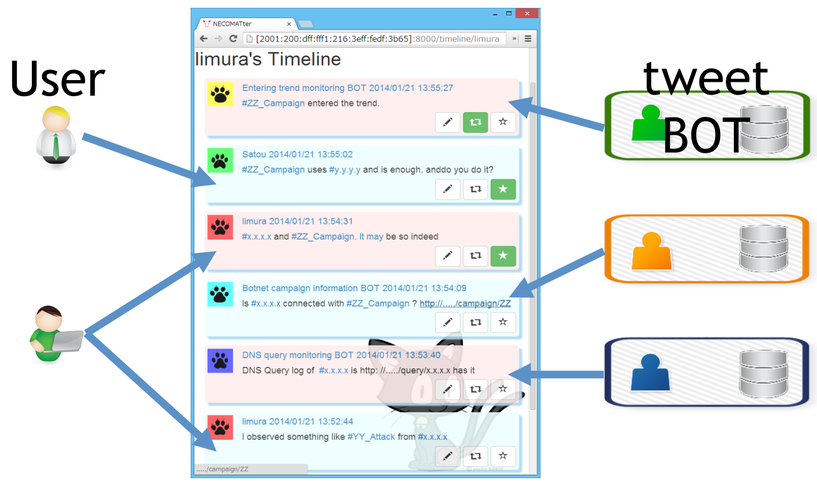
A user obtains cyber threat information from bots and other users, shares the important information (***remew***), collaborates to other users in adhoc, and outputs commands to executor bots.

- Mew (output)

curl -H "content-type: application/json" -d '{"user_name": "YOUR ACCOUNT NAME", "api_key": "YOUR APIKEY", "text": "MEW TEXT"}'
https://necomatter.necoma-project.jp/post.json

- Streaming watch (monitor)

curl -H "content-type: application/json" -d '{"user_name": "YOUR ACCOUNT NAME", "api_key": "YOUR APIKEY", "regexp": "reguler expression string", "description": "BOT description"}'
https://necomatter.necoma-project.jp/stream/regexp.json



available to download at:
https://github.com/necoma/NECOMAtter

Contact
Takuji Iimura
iimura@nc.u-Tokyo.ac.jp