NECOMATter: twitter saves the (cyber) world !

Motivation

Sharing cyber-threat knowledge is an important portion in cyber security, however, it is always difficult even thought analytical skills and correspondence techniques had been studied and employed. It can be explained by the difference in t the form of the information – which is acquired in the various observation points and consists of various cyber threat. Below provides an example of the difference.

- Nature of data and characteristics : Network bandwidth, DNS Query, phishing mail and website, malware programs (Information loss due to the anonymized data is also considered)
- Observation method of data : active measurement (polling); passive measurement (pulling)

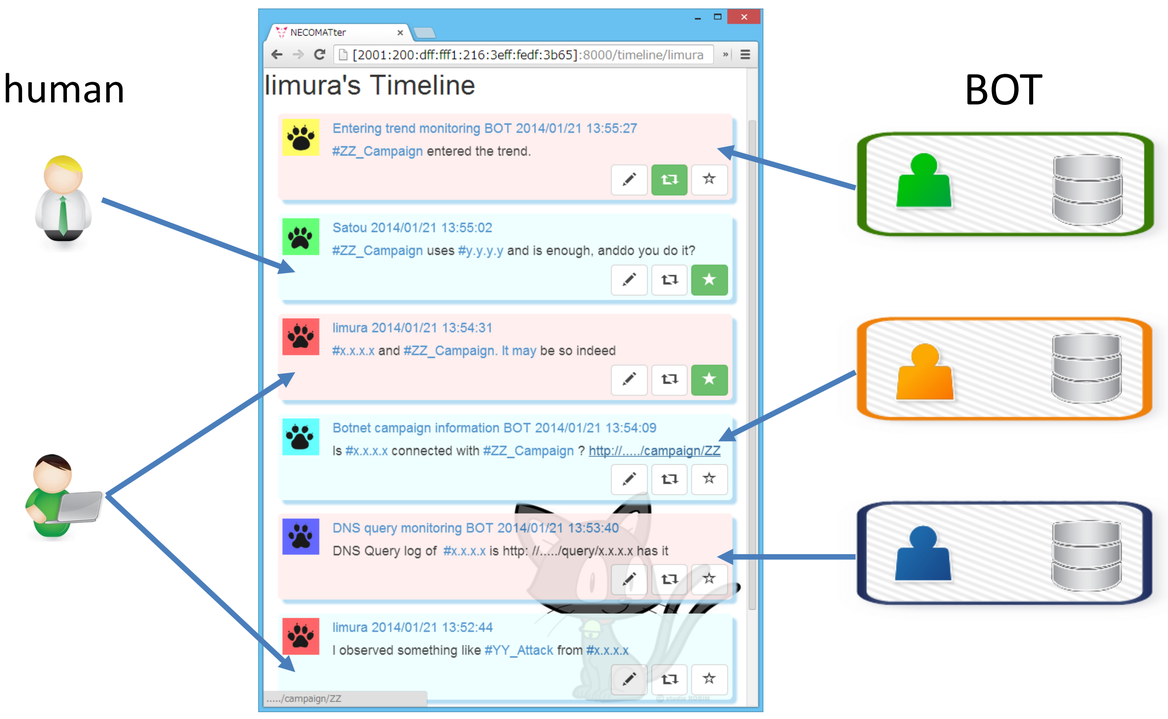
Some useful information sources, such as WOMBAT and/or PhishTank are available, however , there is no tools for retrieving information transversely; it means that we need the seamless solutions for extracting cyber security information regardless of the difference of the information sources. Our key idea is to develop the information sharing system which borrowed an idea from twitter, that is, “to connect plural sources of information and a model of the information in loosely" to solve such a problem.

Approach

- Sharing Information with the text format.
  - It keeps a "loose" connection without defining the data form.
- Expediting it by assigning hash-tag for specific incident
  - It connects individual tweet of TAG.
- Offering a user interface in which the user tends to be easier to read.
  - It can display it in a Web browser.

Such as Twitter!

NECOMATter movement image (the present conditions)



REST API

NECOMATter provides
the following functions as a REST API

- Streaming read (with regular expression match)
- Get user tweets
- Search by hash-tag
- The acquisition of Tweet-tree by the reply
- Get user name list
- Post tweet
- Follow/unfollow user
- Get followed user name list
- Add/delete star
- Retweet/cancel retweet
- Add/delete to list

NECOMATter provides the environment that is the kind of program as above

Use Image

As for the tweet BOTs, they tweet available information which they have. The user can watch fresh information provided by the BOT that I want to use and responding to users. It would helpful to sophisticate while obtaining cyber threat information. In letting an incident and a campaign enter the trend of the user makes it easy to stand out.

Problems

- Range of Information sharing
  - Defining the label of the information.
- Requirements of data anonymization
  - Personal information
- Naming rules for hash-tag
  - By Incidents, Campaign, malware names …