Support of Security Operations

Most security equipment operates on limited information. Therefore, to develop countermeasures based on a multi-lateral understanding of information from various sources, an expert must first interpret the information before adjusting individual device settings. NECOMATter, which is a framework to support these operations, aims to collect information from individual security devices, analysts, and operators. This aggregate information can be browsed easily, allowing users to give appropriate instructions to each device.

Composition of NECOMATter

NECOMATter is a twitter-like website with three types of users:

- Information Providing BOT
- User (person)
- Equipment Operation BOT

- Information Providing BOTs seek and provide information to NECOMATter (mew). They also react to user directions and inputs from other BOTs (streaming monitoring), summarize such information, and disseminate it and URL links.
- Users can share (re-mew) important information obtained from the URL links provided by Information Providing BOTs or other users. The extracted information can then be given to Equipment Operation BOTs, if desired.
- Equipment Operation BOTs are devices such as security machinery. These BOTs monitor information from administrators and specified users to ensure that the equipment is operated as intended.

Timeline for NECOMATter

NECOMATter operates in plain text to facilitate communications (read and write) between humans and machines. A markdown format is used to render the web interface for humans. Web information outside of NECOMATter can also be viewed (Fig. 1).

Figure 1: Timeline for NECOMATter
NECOMATter: Timeline and summary of cyber threat information

Various BOTs

To exchange information, people (operators) and a variety of BOTs (machines) are connected to NECOMATter. Example BOTs are outlined below.

- **ZeuS DGA BOT**
  Using DNS query information received by the DNS server, this BOT writes to NECOMATter by discovering DNS queries used by botnet from regulator expressions indicated by Zeus-DGA. For example, a DNS query such as

  q2cuacaaknsmaag46adosaqaabjafstpeioqwwozaaaahwbiaa3aaaabkpa.yildacaiaaaqamy6sx5iss6umwav7t5rru3f3azshqcz7y.a.j.e5.sk.

  can be detected and written to NECOMATter.

- **Phishing decision BOT**
  Phishing decision BOTs monitor specified example characters (@is_a_phish http://example.com...) written to NECOMATter and determine the probability of phishing at a specified URL. The results are returned in the form of an answer.

Bot sample code

NECOMATter and BOTs communicate using the REST API. A few simple examples are shown below.

- **writing input (mew)**
  curl -H "content-type: application/json" -d '{ "user_name": "YOUR ACCOUNT NAME", "api_key": "YOUR APKEY", "text": "MEW TEXT" }' https://NECOMATter.necoma-project.jp/post.json

- **monitoring (stream monitoring)**
  curl -H "content-type: application/json" -d '{ "user_name": "YOUR ACCOUNT NAME", "api_key": "YOUR APKEY", "regexp": "regular expression string", "description": "BOT description"}' https://NECOMATter.necoma-project.jp/stream/regexp.json

Operational performance

As of February 2016, 20 active BOT accounts post 10,000 mews daily, and more than 500,000 mews have been accumulated on NECOMATter.

Download

NECOMATter can be downloaded from the following URL:
https://github.com/necoma/NECOMAtter (illustration from studio ROBIN)

Contact
Internet Engineering Lab
Graduate School of Information Science
Nara Institute of Science and Technology
NECOMA Project Secretariat
Mail: fp7-necoma-pr@is.naist.jp
Web: http://www.necoma-project.jp

[NECOMA]
Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis