NECOMA

NECOMATter: サイバー脅威情報のタイムラインとまとめ

BOT

NECOMAtterでは人間以外のユーザを BOT と呼びます。BOT は利用者が設置し、情報の提供や収集、機器の操作など様々な利用をされます。

セキュリティオペレーションの補助

多くのセキュリティ機器は限られた情報で動作しています。そのため、様々な情報源を使って多角的に情報を把握した上で対策等をおこなう場合、専門家がそれら様々な情報源からの情報を解釈した上で個々の機器を設定しています。

NECOMATter はこのような操作を補助するためのフレームワークです。NECOMATter は、個々のセキュリティ機器からの情報や、アナリストやオペレータからの情報をまとめて閲覧したり、それらの情報を集約しより閲覧しやすくする事、個々の機器への指示などを簡便にする事などを目的としています。

NECOMATter の構成要素

NECOMATter は twitter のような Web サイトで、ユーザ毎にその使い方が異なります。ユーザは以下の 3 種類に分けられます。

- 情報提供 BOT
- ユーザ（人間）
- 機器操作 BOT

・情報提供 BOT は、自身が得ることのできる情報を NECOMATter に書き込みます (mew)。また、ユーザからの指示や他の BOT の発言に反応 (streaming watch) する形で、自身の持つ情報の要約と、より深い情報への URL を書き込む事で情報を提供します。

・ユーザは、情報提供 BOT や他のユーザから得られた情報を元に、情報提供 BOT の示した URL でより深い情報を取得し、重要と思われる情報を共有 (re-mew) します。また、他のユーザや情報提供 BOT から情報を引き出し、必要ならば機器操作 BOT への指示を書き込みます。

・機器操作 BOT は、セキュリティ機器などの装置です。この BOT は、管理者や、特定ユーザからの書き込みを監視することで、そのユーザからの指示を受けて機器を操作します。

NECOMATter のタイムライン

NECOMATter は人間と機械のどちらでも読み書きできるように、プレーンテキストでのやりとりが主体となります。人間が閲覧する Web インタフェースでは、Markdown 形式でレンダリングされ、より詳しい情報を提示したい場合などについては、図 1 のように NECOMATter 以外の Web 情報を参照して提示することもできます。

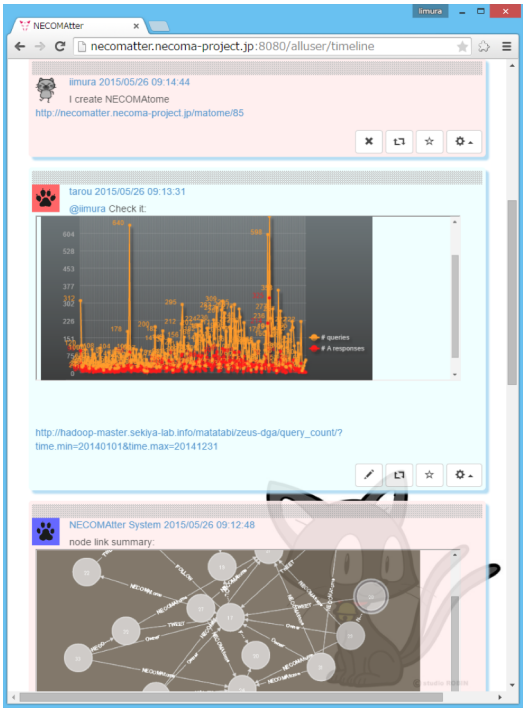

図 1 NECOMATter のタイムライン

NECOMA

NECOMATter: サイバー脅威情報のタイムラインとまとめ

curl

HTTP でのアクセスを行うプログラムです。この例では単に GET リクエストを送信するために使っています。

NECOMA の研究活動ならびに成果についての詳細は、Web サイト www.necoma-project.jp をご覧ください。

様々な BOT

NECOMATter にはオペレータなどの人間以外に、様々な機械(BOT)が接続し、情報を交換します。以下に、実装されているいくつかの BOT の例を挙げます。

・ZeuS DGA BOT

DNS サーバが受けた DNS クエリ情報から、Zeus-DGA で示される正規表現を用いて botnet が用いる DNS クエリを発見し、NECOMATter に書き込みます。例えば、

oq2cuaacaaknsmqaag46adosaqaabjafstfpeioqwoozaaaaahwbiaa3aaaabkp.ayldacaaiaaaqamy6sx5lss6umwaw7dt5rru3f3azshqcz7y.a.j.e5.sk.

といった DNS クエリが検知され、NECOMATter に書き込まれます。

・phishing 判定 BOT

Phishing 判定 BOT は、特定の文字列(@is_a_phish http://example.com...) の書き込みを監視して、そこで指定された URL について phishing の可能性が高いかどうかを判定して、返信の形式で結果を返します。

NECOMATter での人間と BOT の連携

NECOMATter では人間のオペレータと監視を行っている BOT や機器を制御する BOT とが、同じ NECOMATter 上のメッセージを通じて連携を行います。例えば、監視を行っている BOT が異常を検知し、その異常を NECOMATter に書き込むと、人間のオペレータがその情報について詳しく知るために解析 BOT や他の人間に見えるように NECOMATter へと書き込みを行います。その書き込みを見た解析 BOT や人間が、関連する情報を返信などの形式で NECOMATter に書き込むことで情報が集まってきます。この集まった情報のうち特に有用なものを NECOMAtome として纏めたり、それらの情報から問題となる異常を緩和するための指示を NECOMATter に書き込んで、その指示を受けたネットワーク機器が異常の緩和を実行します。

BOT のサンプルコード

NECOMATter と BOT のやりとりは REST API を用いて行われます。簡単なサンプルは以下のようになります。

・書き込み(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
```

・監視(streaming watch)

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

運用実績

NECOMATter では 2016 年 2 月現在、20 の BOT アカウントが動作しており、毎日 1 万件の mew がなされ、合計 50 万件を超える mew が蓄積されています。

ダウンロード

NECOMATter は以下の URL からダウンロード可能です。

https://github.com/necoma/NECOMAtter

(illustration from studio ROBIN)

【お問い合わせ先】
奈良先端科学技術大学院大学　情報科学研究科
インターネット工学研究室内
NECOMA プロジェクト事務局
Mail: fp7-necoma-pr@is.naist.jp
Web: http://www.necoma-project.jp

NECOMA
Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis