rcATT: retrieving ATT&CK tactics and techniques in cyber threat reports

Marco Caselli, Siemens AG
Valentine Legoy, University of Twente
Andreas Peter, University of Twente, Services and Cybersecurity group
Christin Seifert, University of Twente, Data Science Group

Unrestricted
Problems and motivation

CTI sharing is growing but...

Cyber Threat Reports (CTRs) are mostly unstructured human-readable documents meant for experts.
Proposed Solution

- Automating the extraction of Tactics, Techniques, and Procedures (TTPs)
- Taking advantage of known TTPs such as the MITRE ATT&CK framework for the classification
- Organizing the obtained results in a structured format, namely STIX 2.0
Analysis & Implementation
Available Data Sources

- “ATT&CK - Adversarial Tactics, Techniques, and Common Knowledge”
- MITRE’s Github\(^1\) offers the entire ATT&CK framework represented in STIX 2.0
- Techniques include references to ~1500 different CTRs

\(^1\)https://github.com/mitre/cti
Challenges & Countermeasures

- Multiple techniques and tactics in each report
- Multi-label text classification
- Limited amount of data
  - Imbalanced dataset
- Rebalancing and increasing the dataset by getting more data
- Tactics and techniques are not independent
- Use tactics and techniques relationship in post-processing
Evaluation Measures

\[ \text{precision} = \frac{tp}{tp + fp} \]
\[ \text{recall} = \frac{tp}{tp + fn} \]

\[ F_\beta = \frac{(1 + \beta^2) \cdot (\text{precision} \cdot \text{recall})}{\left( \beta^2 \cdot \text{precision} + \text{recall} \right)} \]

\[ \beta = 0.5 \]

\( tp = \text{true positives}; \ fp = \text{false positives}; \ fn = \text{false negatives} \)
Classification Process Schema

CTR → Pre-processing → Feature Selection → Classification → temp TTPs → Post-processing → Final TTPs

Labeled CTRs
Pre-processing

Removing noise (e.g., with regular expressions)

Removing stop-words (e.g., “a”, “and”, “but”)

Stemming (e.g., attacking → attack)
Feature Selection

Word frequency based
- Term frequency (TF)
- Term frequency-inverse document frequency (TF-IDF)

TF-IDF “Tuning”
- Bags-of-words representation
- Filtering lowest scores

Word embedding
- Word2Vec
Classification

Classification algorithms:
- Naive Bayes, Nearest Neighbors, Support Vector Machine, Decision Trees, Linear Models, etc.

Solving overfit and unbalance
- Re-sampling, fine-tuning on parameters, etc.

Linear SVM to identify both Tactics and Techniques
Post-processing

Goal: making use of the ATT&CK structure

Approaches:
- Deriving tactics from techniques classification
- Confidence propagations
- Association among techniques

Confidence propagation
Classification Process Schema

1. Pre-processing
2. Feature Selection
3. Classification
4. Post-processing

Labeled CTRs

CTR → Pre-processing → Feature Selection → Classification → temp TTPs → Post-processing → Final TTPs
Final Classification Process

CTR

1. Cleaning & Stemming

2a. TF-IDF
2b. TF-IDF

3a. Linear SVM
3b. Linear SVM

Labeled CTRs

Final Tactics

Temp Techs.

Confidence Propagation

Final TTPs
rcATT Report Classifier based on ATT&CK tactics and techniques
rcATT - Report classification by ATT&CK tactics and techniques

- Coming with graphical and command-line interfaces
- Returning the confidence values of all predictions
- Possibility of modifying and feedbacking results to improve tool’s classifier
- Exporting results as STIX 2.0 (referencing the actual ATT&CK STIX objects)
rcATT – Tool structure

- CTR
- Train model
- Predict tactics and techniques
- Trained model
- Labeled CTRs
- Save for training
- TTPs
- Modify results
- Export in STIX format
- Structured result file
“name” and “published” are defined by the user

“Description” contains the report

All references to tactics and techniques defined by MITRE are included in the “object_ref” field

```
"type": "report",
"id": "report-4932ef6d-3e08-4e3b-9862-1d72477a32f7",
"created": "2019-11-17T16:43:59.045Z",
"modified": "2019-11-17T16:43:59.045Z",
"name": "HiddenNasp",
"description": "Overview Intezer has discovered a new, soph1",
"published": "2019-05-25T00:00:00Z",
"object_ref": [
  "x-mitre-tactic--78b23412-0651-46d7-ae50-170a1ce8bd5a",
  "x-mitre-tactic--5bc1d813-693e-4823-9961-afbf9af40be92",
  "x-mitre-tactic--5e29b093-294e-49e9-a803-dab3d73b77dd",
  "x-mitre-tactic--7141578b-e58b-4d08-bfa4-0a86d689e9e",
  "x-mitre-tactic--f72804c5-f15a-449a-a5da-2eece181f813",
  "x-mitre-tactic--4ac45d45-df4d-4613-8980-bac22d278fa5",
  "attack-pattern--43e7dc91-05b2-474c-b9ae-2ed4fe101f4d",
  "attack-pattern--7fd87010-3a00-4da3-b905-410525e8e444",
  "attack-pattern--c6919bb5-9c9f-4c6c-95a5-14761e7b2add",
  "attack-pattern--0f20e3cb-245b-4a61-8a91-29d9374bb09b",
  "attack-pattern--b3d68b2d-9bf2-4fb0-aa3b-b4df07e9a7ed",
  "attack-pattern--c484f6cf7-66b2-4bde-8216-bc157dfab8a",
  "attack-pattern--e1df3350-cc05-4bdf-bdf8-a091a6ed48a",
  "attack-pattern--c21d5a77-d422-4a69-ac7d-2c5314faa34b",
  "attack-pattern--e01be9c5-e763-4caf-aeb7-000416ae657",
  "attack-pattern--3bcebe0-6d3-4334-b543-3ddf8c5642d",
  "attack-pattern--3ce7f7ae-cb5e-48f6-8302-897105f55c"
],
"labels": [
  "threat-report"
]
```
Demo
Conclusion
## Comparison with existing solutions

<table>
<thead>
<tr>
<th>Classification method</th>
<th>rcATT</th>
<th>TTPDrill</th>
<th>Ayoade et al.</th>
<th>Unfetter Insight</th>
<th>TRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Multilabel text classification (Linear SVM)</td>
<td>Ontology</td>
<td>Text classification (SVM+KNN)</td>
<td>Multilabel text classification (Multinomial NB)</td>
<td>Multilabel sentences classification (Logistic regression)</td>
</tr>
<tr>
<td>Features</td>
<td>Word frequency</td>
<td>Threat actions</td>
<td>Word frequency</td>
<td>Word frequency</td>
<td>Word frequency</td>
</tr>
<tr>
<td>Evaluation metrics</td>
<td>F0.5 score</td>
<td>Precision and recall</td>
<td>Accuracy</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Post-processing</td>
<td>Make use of tactics to retrieve techniques</td>
<td>Use techniques to retrieve tactics</td>
<td>Make use of tactics to retrieve techniques</td>
<td>None</td>
<td>/</td>
</tr>
</tbody>
</table>
Final remarks

Lesson learned

• Lack of labeled data
• False positives vs. false negatives
• Plain machine learning vs classification enhancements (e.g., ATT&CK structure)

Key aspects

• Incident response automation
• Open source software
  o rcATT is currently available at: github.com/vlegoy/rcATT
Dr. Marco Caselli
Senior Key Expert
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
E-mail: marco.caselli@siemens.com

Thanks

rcATT is available at:
github.com/vlegoy/rcATT