Detecting Lateral Movement
A Data Analysis & Visualization Approach

Maddy Longo, Jeff Martin, & Ian Vossoughi

Steven Gomez     George Heineman     Diane Staheli
MIT LL - 0558     WPI                MIT LL - 0551
The Advanced Persistent Threat (APT)

- APT is a contemporary form of cyberattack
- Stealthy, advanced infiltration to steal valuable data

**Critical Stage: Lateral Movement**
- Progress from initial compromised computer across network
- Use available resources to steal user credentials and access new computers
- Slowly and steadily increase network reach while remaining camouflaged in network traffic
Threat Detection: Process and Problems

• Automated intrusion detectors learn normal activity
  – Raise alerts for anomalous activity

• Automated detectors often have high false positive rates
  – Faced with many false positives, analysts lose focus

• Malicious activity represents only a small portion of the total events
  – Rare but devastating
Where Are The Malicious Events?

Los Alamos National Laboratory cybersecurity dataset

<table>
<thead>
<tr>
<th>Time</th>
<th>Source User</th>
<th>Destination User</th>
<th>Source Computer</th>
<th>Destination Computer</th>
<th>Auth. Type</th>
<th>Logon Type</th>
<th>Auth. Orientation</th>
<th>Success / Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>190</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C2707</td>
<td>C2707</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
</tr>
<tr>
<td>191</td>
<td>U1048@DON\U1048@DON\C17693</td>
<td>C2846</td>
<td>NTLM</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C3430</td>
<td>C3430</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
</tr>
<tr>
<td>193</td>
<td>U1048@DON\U1048@DON\C2846</td>
<td>C2846</td>
<td>?</td>
<td>Network</td>
<td>LogOff</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>194</td>
<td>U5254@DON\U5254@DON\C17693</td>
<td>C636</td>
<td>NTLM</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>195</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C2892</td>
<td>C2892</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOff</td>
<td>Success</td>
</tr>
<tr>
<td>196</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C2892</td>
<td>C2892</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
</tr>
<tr>
<td>197</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C3331</td>
<td>C3331</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOff</td>
<td>Success</td>
</tr>
<tr>
<td>198</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C3331</td>
<td>C3331</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
</tr>
<tr>
<td>199</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C1823</td>
<td>C1028</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
</tr>
<tr>
<td>200</td>
<td>U6146@DON\U6146@DON\C14053</td>
<td>C612</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>201</td>
<td>U6146@DON\U6146@DON\C612</td>
<td>C612</td>
<td>?</td>
<td>Network</td>
<td>LogOff</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>202</td>
<td>U6146@DON\U6146@DON\C2331</td>
<td>C2331</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOn</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>203</td>
<td>U6146@DON\U6146@DON\C2331</td>
<td>C2331</td>
<td>?</td>
<td>Network</td>
<td>LogOff</td>
<td>Success</td>
<td></td>
<td></td>
</tr>
<tr>
<td>204</td>
<td>U66@DOM1</td>
<td>U66@DOM1</td>
<td>C3430</td>
<td>C3430</td>
<td>Kerberos</td>
<td>Network</td>
<td>LogOff</td>
<td>Success</td>
</tr>
</tbody>
</table>
Objective
- Explore the use of data analysis and data visualization for the purpose of detecting lateral movement
- Develop a proof-of-concept tool for lateral movement detection

Hypothesis One
- Ensemble of anomaly detectors will improve accuracy

Hypothesis Two
- Visualization that uses event’s time, location, and suspicion level will allow an analyst to isolate lateral movement

Framework developed as a proof-of-concept tool to evaluate both hypotheses
The Analyst Workflow

1. Cybersecurity Dataset
2. Shell
3. Visualization

Cybersecurity Analyst
Visualization – Heatmap

Source_User: C1085$@DOM1
Destination_Computer: C2106
Visualization – Dashboard

When clicking a block:

Filter rows by number of blocks they contain (in total data):
Minimum: 1
Maximum: 20

Update Rows

Filter columns by number of blocks they contain (in total data):
Minimum: 1
Maximum: 20

Update Columns

Legend (Volume of Events):

1

Reset all Data

Keep previous axis orders/filters when resetting
Visualization – Sorting and Filtering
Visualization – Isolated Timeplot

When clicking a block:
- Shift Column to Left
- Reset of Data
- Keep previous axis orders/limits when resetting

Legend (Suspicion of Events):
- 0
- 1

Reset all Data

Destination Computer

Time
Evaluating Hypothesis One - Experiment

Hypothesis: *Ensemble of anomaly detectors will improve accuracy*

1) Preprocessed Los Alamos dataset (~1.5B → ~150K events)
2) Implemented machine learning (random forest) and synthetic detectors
3) Trained, tested, and computed performance metrics for each detector and ensemble across 10 trials
Evaluating Hypothesis One - Results

**Hypothesis:** *Ensemble of anomaly detectors will improve accuracy*

<table>
<thead>
<tr>
<th>Detector</th>
<th>Accuracy Metrics for Detectors and Ensemble</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensemble</td>
<td>0.88</td>
</tr>
<tr>
<td>Imperfect Oracle</td>
<td>0.74</td>
</tr>
<tr>
<td>Random Forest</td>
<td>0.68</td>
</tr>
</tbody>
</table>

**Accuracy Metrics for Detectors and Ensemble**

- Ensemble AUROCC (Area Under the Receiver Operating Characteristic Curve) was 19% greater than the best detector’s AUROCC.
- This evidence supports Hypothesis One.
Hypothesis: *Visualization that uses event’s time, location, and suspicion level will allow an analyst to isolate lateral movement*

- **Classification of User Intent**
  - Given 100 seconds of authentication data from 8 users, determine which users had redteam activity
  - Ground truth: 4 malicious and 4 benign users
Evaluating Hypothesis Two – Results

Hypothesis: Visualization that uses event’s time, location, and suspicion level will allow an analyst to isolate lateral movement

<table>
<thead>
<tr>
<th>Username</th>
<th>U66</th>
<th>U5254</th>
<th>U8601</th>
<th>U1048</th>
<th>U8731</th>
<th>U3451</th>
<th>U640</th>
<th>U6146</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1 Pred.</td>
<td><strong>Malicious</strong></td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
</tr>
<tr>
<td>S2 Pred.</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td><strong>Malicious</strong></td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
</tr>
<tr>
<td>S3 Pred.</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
<td><strong>Malicious</strong></td>
<td><strong>Malicious</strong></td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
</tr>
<tr>
<td>S4 Pred.</td>
<td><strong>Malicious</strong></td>
<td>Benign</td>
<td>Benign</td>
<td><strong>Malicious</strong></td>
<td><strong>Malicious</strong></td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
</tr>
<tr>
<td>Ground Truth</td>
<td><strong>Malicious</strong></td>
<td>Malicious</td>
<td>Malicious</td>
<td>Malicious</td>
<td>Malicious</td>
<td>Benign</td>
<td>Benign</td>
<td>Benign</td>
</tr>
</tbody>
</table>

- Each subject scored within one point of random guessing (4/8)
- This evidence does not support Hypothesis Two
Evaluating Hypothesis Two – Results

• MIT LL Information Security Department (ISD) Evaluation and Qualitative Feedback
  – Visualization shows promise for quickly drawing attention toward anomalous activity
  – Should support detection of more complex anomalies, automated filtering:
    • Logins outside user’s normal diurnal hours
    • Authentications into subnets outside user’s normal access
Conclusion

• **Framework**
  – Supports the analysis of a wide variety of cybersecurity datasets
  – Provides a modular interface for implementing and testing anomaly detectors and ensembles of detectors
  – Supports the aggregation and visualization of data in flexible ways

• **Ensemble**
  – Reduces false positive rate while maintaining detection rate
  – Will be more trustworthy to analysts

• **Visualization**
  – Visualization alone is insufficient to pinpoint malicious activity
  – Most useful for guiding the initial steps of the analyst
  – Allows the analyst to identify anomalies to investigate further
Future Work

- Improve framework security
  - Sandbox detector execution
  - Improve authentication process
- Improve framework efficiency
  - Optimize SQL queries
  - Improve algorithm efficiency
- Make detectors more trustworthy
  - Develop signature-based detectors
  - Display justifications for event suspicion level
- Add support for multi-layered datasets
  - With subnets, user roles, computer roles, etc.
- Evaluate an ensemble of more than two detectors
Acknowledgements

Project Mentors

Steven Gomez  George Heineman  Diane Staheli
MIT LL - 0558  WPI  MIT LL - 0551

MIT LL Employees

Brian Desnoyers  Sandeep Pisharody  Rob Elkind  Chad Meiners  Tamara Yu (51/LRNOC)
(58)  (58)  (58)  (51/LRNOC)

Chris Redinger  Richard Emerson  Steve Castellarin  Helga Wilde  Gregory Burns
(ISD)  (ISD)  (ISD)  (ISD)  (ISD)
| U1@MITLL | | | MITLL | | U2@MITLL | | | MITLL | | U3@MITLL | MITLL | | U4@MITLL | | | MITLL | | U5@MITLL | | | MITLL |

Questions?