Machine Learning-based Detection of C&C Channels with a Focus on Locked Shields

Nicolas Känzig\textsuperscript{(1)}, Roland Meier\textsuperscript{(1)}, Luca Gambazzi\textsuperscript{(2)}, Vincent Lenders\textsuperscript{(2)}, Laurent Vanbever\textsuperscript{(1)}
UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Brand  |  May 12, 2017, 11:36am EDT

A massive ransomware attack has shut down work at 16 hospitals across the United Kingdom. According to The Guardian, the attack began at roughly 12:30PM local time, freezing systems and encrypting files. When employees tried to access the computers, they were met with a message demanding a payment for the decryption key in the cryptocurrency Monero.

The attack was particularly devastating for the hospitals involved, as it led to the cancellation of surgeries and a postponement of non-emergency appointments. The situation was further complicated by the fact that many of the hospitals were already facing resource constraints due to the ongoing coronavirus pandemic.

The incident has drawn widespread attention and has raised concerns about the vulnerability of healthcare systems to cyber threats. It has also highlighted the need for better preparedness and response plans to deal with such attacks.

The hacking group behind the attack is still unidentified, but种种迹象表明 it is likely to be a group with ties to Russian intelligence. The incident has also sparked a debate about the effectiveness of current cybersecurity measures and the potential for such attacks to escalate in the future.

In an effort to mitigate the impact of the attack, the government has announced plans to provide additional funding for cybersecurity measures in healthcare facilities, including the deployment of more advanced security systems and the training of staff on how to respond to such incidents.

The situation remains fluid, and authorities are working to contain the damage and prevent further disruptions. The attack has served as a stark reminder of the ongoing threats posed by cybercrime and the need for robust cybersecurity measures in all sectors, including healthcare.
A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

The cyber-security company Information Systems Security Partners (ISSP) has linked the incident to a hack and blackout in 2015 that affected 225,000.
Cyber defenders fight hackers in high-tech Estonia war

Attacks on vital systems and fake news

Daniel McLaughlin in Tallinn

The attack on the airbase began with a salvo of fake news. “A report appeared saying drones were using nerve gas,” said Lauri Luht, crisis management chief for the cyber security department of Estonia’s information system authority.
Cyber defenders fight hackers in high-tech Estonia war games

Attacks on vital systems and fake news are all part of Locked Shields exercise

Fri, Apr 28, 2017, 01:00

Daniel McLaughlin in Tallinn

Locked Shields, now taking place in Estonia involving 20 teams from Europe and the US, is the world's most advanced live-fire cyber defence exercise. Photograph: Daniel McLaughlin

The attack on the airbase began with a salvo of fake news. “A report appeared saying drones were using nerve gas,” said Lauri Luht, crisis management chief for the cyber security department of Estonia’s information system authority.
Locked Shields is the largest live-fire global cyber defense exercise
Locked Shields is the largest live-fire global cyber defense exercise

- **Red Team** vs. **Blue Team** exercise

<table>
<thead>
<tr>
<th>Attackers</th>
<th>Defenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Team</td>
<td>1 Team / country</td>
</tr>
</tbody>
</table>
Locked Shields is the largest live-fire global cyber defense exercise

- **Red Team** vs. **Blue Team** exercise
  - Attackers: 1 Team
  - Defenders: 1 Team / country

- 1’200 experts from 30 nations
- 4’000 virtualized systems
- 2’500 attacks

**CYCON**
If the Swiss Blue Team had used our system at Locked Shields 2018, it would have discovered more than 80% of the C&C servers within 30 minutes.
Overview

Locked Shields: the largest cyber defense exercise

Identifying C&C channels in real time and with little resources

Evaluation on real data from Locked Shields 2017 and 2018
Locked Shields: the largest cyber defense exercise

Identifying C&C channels in real time and with little resources

Evaluation on real data from Locked Shields 2017 and 2018
Each Blue Team has its own network (“Gamenet”) to defend.

e.g. a military air base

[Diagram of interconnected nodes representing a network]
Each Blue Team has its own network ("Gamenet") to defend
One Red Team attacks all Gamenets
One Red Team attacks all Gamenets (partially) using C&C infrastructure
The setting for the Red Team during Locked Shields resembles the one for real attackers

- Skilled attackers
- Exploit various weaknesses of a network
- Run attacks (partially) via a C&C infrastructure
Blue Teams can run tools and sniff traffic inside the Gamenet
Blue Teams can run tools and sniff traffic inside the Gamenet *with some constraints*

- Small bandwidth
- Little resources (CPU, memory)
The setting for Blue Teams during Locked Shields resembles the one for real defenders:

- Arrive when the network is already under attack
- Systems are already compromised and poorly documented
- Users demand availability of the infrastructure
Locked Shields: the largest cyber defense exercise

Identifying C&C channels in real time and with little resources

Evaluation on real data from Locked Shields 2017 and 2018
We aim at a classifier that classifies between normal and C&C traffic.
We aim at a classifier that classifies between normal and C&C traffic.
Training happens offline, classification happens online

Training (offline)

- Traffic from past exercises
- Red Team logs

Classification (online)

Classifier

- normal
- C&C

CYCON
Training (offline)

Data acquisition
- Traffic from past exercises
- Red Team logs

Classification (online)

Data preprocessing

Feature extraction

Machine learning

Classifier

normal

C&C

CYCON
Training (offline)

- Traffic from past exercises
- Red Team logs

Data acquisition

Data preprocessing

- IP / hostname mapping
- C&C server identification

Feature extraction

Machine learning

Classification (online)

Classifier

- Normal
- C&C
Training (offline)

- Data acquisition
  - Traffic from past exercises
  - Red Team logs

- Data preprocessing
  - IP / hostname mapping
  - C&C server identification

- Feature extraction

- Machine learning
  - Flow labeling

Classification (online)

- Classifier
  - normal
  - C&C
Training (offline)

Data acquisition:
- Traffic from past exercises
- Red Team logs

Data preprocessing:
- IP / hostname mapping
- C&C server identification

Feature extraction
- Feature extraction

Machine learning:
- Flow labeling
- Feature selection
- Model training

Classification (online)

Classifier

normal
C&C

CYCON
**Training (offline)**

- **Data acquisition**
  - Traffic from past exercises
  - Red Team logs

- **Data preprocessing**
  - IP / hostname mapping
  - C&C server identification

- **Feature extraction**
  - Feature extraction

- **Machine learning**
  - Flow labeling
  - Feature selection
  - Model training

**Classification (online)**

- **Live traffic capture**

---

**Flow**

- Normal
- C&C
Training (offline)

- Traffic from past exercises
- Red Team logs

Classification (online)

- Live traffic capture
- Feature extraction

Data acquisition

Data preprocessing

- IP / hostname mapping
- C&C server identification

Feature extraction

Flow labeling

Feature selection

Model training

Classifier

Normal

C&C

CYCON
Training (offline)

- Data acquisition
  - Traffic from past exercises
  - Red Team logs
- Data preprocessing
  - IP / hostname mapping
  - C&C server identification
- Feature extraction
- Machine learning
  - Flow labeling
  - Feature selection
  - Model training

Classification (online)

- Data acquisition
- Data preprocessing
- Feature extraction
- Machine learning
  - Classifier

Data acquisition, Data preprocessing, Feature extraction, Machine learning

Normal
C&C
We consider 77 widely used network traffic features

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Time-related</th>
<th>Volume-related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow direction</td>
<td>Flow duration</td>
<td>Number of packets</td>
</tr>
<tr>
<td>L3/L4 protocol</td>
<td>Packets / s</td>
<td>Bytes / s</td>
</tr>
<tr>
<td>Internal / external</td>
<td>Inter arrival time</td>
<td>Packet size</td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

**CYCON**
Training (offline)

Data acquisition
- Traffic from past exercises
- Red Team logs

Data preprocessing
- IP / hostname mapping
- C&C server identification

Feature extraction
- Feature extraction

Machine learning
- Flow labeling
  - Feature selection
  - Model training

Classification (online)

Data acquisition
- Live traffic capture

Data preprocessing
- Feature extraction

Feature extraction
- Feature extraction

Machine learning
- Classifier
  - normal
  - C&C

Flow

Data acquisition → Data preprocessing → Feature extraction → Machine learning

CYCON
We label all flows from or to a C&C server as C&C traffic

For each flow:

If (source or destination ∈ List of C&C servers)

Then: flow is C&C

Else: flow is normal

End If
Data acquisition
- Traffic from past exercises
- Red Team logs

Data preprocessing
- IP / hostname mapping
- C&C server identification

Feature extraction
- Flow labeling
- Feature selection

Machine learning
- Model training

Live traffic capture

Classifier

normal
C&C

Training (offline)
Classification (online)
We select the most useful network traffic features
We select the most useful network traffic features

Train a random forest classifier with all features
We select the most useful network traffic features

Train a random forest classifier with all features

Compute the Gini importance of each feature
We select the most useful network traffic features

1. Train a random forest classifier with all features
2. Compute the Gini importance of each feature
3. Remove the feature with the lowest importance score
We select the most useful network traffic features

1. Train a random forest classifier with all features
2. Compute the Gini importance of each feature
3. Remove the feature with the lowest importance score

Feature X
We select the most useful network traffic features

1. Train a random forest classifier with all features
2. Compute the Gini importance of each feature
3. Remove the feature with the lowest importance score

Feature X
We select the most useful network traffic features

Train a random forest classifier with all features → Compute the Gini importance of each feature → Remove the feature with the lowest importance score

Feature X
Feature Y
Feature Z
...

CYCON
We select the most useful network traffic features

1. Train a random forest classifier with all features
2. Compute the Gini importance of each feature
3. Remove the feature with the lowest importance score

Features in increasing order of importance:
- Feature X
- Feature Y
- Feature Z
- ...

CYCON
Training (offline)

Data acquisition
- Traffic from past exercises
- Red Team logs

Data preprocessing
- IP / hostname mapping
- C&C server identification

Feature extraction

Machine learning
- Flow labeling
- Feature selection
- Model training

Classification (online)

Data acquisition
- Live traffic capture

Data preprocessing
- Feature extraction

Feature extraction

Machine learning
- Model training

Classifier

normal
C&C
Random Forest models achieve good results in an efficient matter and in little time.

Challenges:
- “normal” traffic is different in each year
- Resources (CPU, Memory) are constrained
- Want (near) real-time classification
Random Forest models achieve good results in an efficient matter and in little time

Challenges:

- “normal” traffic is different in each year
- Resources (CPU, Memory) are constrained
- Want (near) real-time classification
- We found that random forest models performed best while satisfying all constraints
Training (offline)

- Data acquisition
  - Traffic from past exercises
  - Red Team logs

- Data preprocessing
  - IP / hostname mapping
  - C&C server identification

- Feature extraction

- Machine learning
  - Flow labeling
  - Feature selection
  - Model training

Classification (online)

- Live traffic capture

- Feature extraction

- Classifier

Outputs:
- normal
- C&C
Locked Shields: the largest cyber defense exercise

Identifying C&C channels in real time and with little resources

Evaluation on real data from Locked Shields 2017 and 2018
We evaluate 2 models

<table>
<thead>
<tr>
<th>Training</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LS17 model</strong></td>
<td>LS17</td>
</tr>
<tr>
<td><strong>LS18 model</strong></td>
<td>LS18</td>
</tr>
</tbody>
</table>
We evaluate 2 models

<table>
<thead>
<tr>
<th>Training</th>
<th>Testing</th>
<th># Trees</th>
<th>Max. depth</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>LS17 model</em></td>
<td>LS17</td>
<td>LS18</td>
<td>128</td>
<td>10</td>
</tr>
<tr>
<td><em>LS18 model</em></td>
<td>LS18</td>
<td>LS17</td>
<td>128</td>
<td>10</td>
</tr>
</tbody>
</table>
High precision and recall for identifying C&C channels

<table>
<thead>
<tr>
<th>Model</th>
<th>Training</th>
<th>Testing</th>
<th>Precision</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS17 model</td>
<td>LS17</td>
<td>LS18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LS18 model</td>
<td>LS18</td>
<td>LS17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
High precision and recall for identifying C&C channels

<table>
<thead>
<tr>
<th></th>
<th>Training</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS17 model</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LS18 model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Precision**

\[
\text{Precision} = \frac{\# \text{ correctly classified C&C flows}}{\# \text{ C&C flows classified as C&C}}
\]

**Recall**

\[
\text{Recall} = \frac{\# \text{ correctly classified C&C flows}}{\# \text{ existing C&C flows}}
\]
High precision and recall for identifying C&C channels

<table>
<thead>
<tr>
<th>Model</th>
<th>Training</th>
<th>Testing</th>
<th>Precision</th>
<th>Recall</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS17 model</td>
<td>LS17</td>
<td>LS18</td>
<td>99 %</td>
<td>98 %</td>
</tr>
<tr>
<td>LS18 model</td>
<td>LS18</td>
<td>LS17</td>
<td>99 %</td>
<td>90 %</td>
</tr>
</tbody>
</table>
Classification of one flow only takes microseconds

<table>
<thead>
<tr>
<th>Model</th>
<th>Training</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS17 model</td>
<td>LS17</td>
<td>LS18</td>
</tr>
<tr>
<td>LS18 model</td>
<td>LS18</td>
<td>LS17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification</th>
<th>3.1 µs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per flow</td>
<td>3.3 µs</td>
</tr>
</tbody>
</table>
Our model is robust against tampering with up to 8 features.
The Swiss Blue Team did use our system at Locked Shields 2019, and it helped them discovering C&C channels which they would not have seen otherwise.
The Swiss Blue Team used our system successfully in Locked Shields 2019

Changes:
- Models from LS17 and LS18
- Same features (but different feature extraction tool)
The Swiss Blue Team used our system successfully in Locked Shields 2019

Changes:
- Models from LS17 and LS18
- Same features (but different feature extraction tool)

Observations:
- Very high true positive rate
- Detected unknown C&C servers
- Confirmed known C&C servers
Locked Shields: the largest cyber defense exercise

Identifying C&C channels in real time and with little resources

Evaluation on real data from Locked Shields 2017 and 2018
Machine Learning-based Detection of C&C Channels with a Focus on Locked Shields

Locked Shields: the largest cyber defense exercise

Identifying C&C channels in real time and with little resources

Evaluation on real data from Locked Shields 2017 and 2018

Nicolas Känzig*, Roland Meier*, Luca Gambazzi*, Vincent Lenders*, Laurent Vanbever (* attending CyCon)

We thank the Swiss Blue Team for sharing their data and expertise with us and for their constant support throughout this project.