Detecting malware even when it is encrypted

Machine Learning for network HTTPS analysis

František Střasák
strasfra@fel.cvut.cz
@FrenkyStrasak

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote
František Střasák

- Student
- CTU FEE Prague, Artificial Intelligence
- strasfra@fel.cvut.cz
- @FrenkyStrasak
- https://github.com/frenky-strasak/HTTPSDetector
Sebastian Garcia

- Researcher and lecturer
- CTU FEE Prague, Department of computer science
- Founder and head of Stratosphere IPS
  (https://stratosphereips.org)
- sebastian.garcia@agents.fel.cvut.cz
- @eldracote
Introduction

- Over half of global web traffic is encrypted
  - https://transparencyreport.google.com/https/overview
  - https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web
  - https://letsencrypt.org/stats/
Introduction

- 10% - 40% of all malware traffic is encrypted
The encryption interferes with the efficacy of classical detection techniques
TLS inspection
TLS inspection

- Advantages
  - TLS inspection can use classical detection techniques

- Disadvantages
  - TLS inspection can be expensive
  - TLS inspection is computationally demanding (can be slow)
  - TLS inspection does not respect the original idea of HTTPS (privacy)
Without decryption

- Find and discover new features and methods to detect malware without decrypting the traffic
Without decryption

● Advantages
  ○ No SSL inspection

● Disadvantages
  ○ The need to discover new features and methods
Goal

- To detect the malware HTTPS traffic without decryption with high accuracy, low false positive rate and false negative rate
Goal

- True Positive (TP) - “we predicted malware and it is malware”
- True Negative (TN) - “we predicted normal and it is normal”
- False Positive (FP) - “we predicted malware and it is normal”
- False Negative (FN) - “we predicted normal and it is malware”

Accuracy = \( \frac{TP + TN}{TP + TN + FP + FN} \)

False Positive Rate = \( \frac{FP}{FP + TN} \)

False Negative Rate = \( \frac{FN}{FN + TP} \)
HTTPS

- HTTPS = HTTP + SSL/TLS
- Verifying that you are talking directly to the correct server
- Ensuring that only the server can read what you send and only you can read what it sends back
SSL/TLS handshake

- Client and server Hello
- Certificate Exchange
- Key Exchange
SSL/TLS handshake

Client Hello

Server Hello with certificate and decision about the parameters.

If the certificate is trusted, creates a symmetric session key and encrypts it with the server's asymmetric public key.

Server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.

Server and Browser now encrypt and decrypt all transmitted data with the symmetric session key.
Certification path

- A root CA
- An intermediate CA
Privacy does not mean Security!
Dataset
Dataset

- Flows with HTTPS traffic
- Malware and Normal
- 4 sub dataset
- 163 malware and normal captures
Dataset

- **CTU-13 dataset - public**
  - Malware and Normal captures
  - An Empirical Comparison of Botnet Detection Methods research

- **MCFP dataset - public**
  - Malware and Normal captures
  - Malware Capture Facility Project
  - [https://stratosphereips.org/category/dataset.html](https://stratosphereips.org/category/dataset.html)
Dataset

● Own normal dataset - public
  ○ Normal captures
  ○ 3 days of accessing to secure sites (Alexa 1000)
  ○ Google, Facebook, Twitter accounts
  ○ https://stratosphereips.org/category/dataset.html

● Normal CTU dataset - almost public
  ○ Normal captures
  ○ 22 known and trusted people from department of FEE CTU
Dataset

- Size of log files in dataset (include background):
  - Normal: 331 GB
  - Malware: 44 GB
  - Total: 375 GB

- All SSL/TLS flows:
  - Normal: 1,357,112
  - Malware: 552,919
  - Total: 1,910,031

- All unique certificates:
  - Normal: 7,040
  - Malware: 1,579
  - Total: 8,619

Most of datasets are public!
Features and Methods
conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
  - Timestamp
conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
  - Timestamp
  - State of connection
conn.log

- TCP/UDP/ICMP connections
- Some of the available data:
  - Source and destination IP and Ports
  - Number of packets
  - Number of bytes
  - Timestamp
  - State of connection
  - Duration
ssl.log

- SSL/TLS handshake info
- Some of the available data:
  - Version of SSL/TLS
  - Ciphersuite
ssl.log

- SSL/TLS handshake info
- Some of the available data:
  - Version of SSL/TLS
  - Ciphersuite
  - Server name
ssl.log

- SSL/TLS handshake info
- Some of the available data:
  - Version of SSL/TLS
  - Ciphersuite
  - Server name
  - Certificate path
Certificate path

ssl.log

<table>
<thead>
<tr>
<th>Certificate path</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElseAT2YTirnFNwwa, TlQLQ4i1LMP060KenK9, FzMjTn2WvGlBjQmAdE</td>
</tr>
<tr>
<td>fycUl32jvPwlbeg85d, FmYVT3wUsvW6p0Ko8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSL records</th>
</tr>
</thead>
<tbody>
<tr>
<td>3511.617809 Ctg353XKjtCwYMPXd 10.0.2.109 443 TLSv10</td>
</tr>
<tr>
<td>3652.492566 Cfg2BM3PUzkFjD4L22 10.0.2.109 443 TLSv10</td>
</tr>
<tr>
<td>3654.509631 CeZN8N3d5uxTGKh51g 10.0.2.109 443 TLSv10</td>
</tr>
</tbody>
</table>

x509.log

<table>
<thead>
<tr>
<th>Certificate records</th>
</tr>
</thead>
<tbody>
<tr>
<td>3504.673635 FlCtgE1o1SORuUafe 3 02FC2E</td>
</tr>
<tr>
<td>3511.621231 FlseAT2YTirnFNwwa 3 0D335238E52B18BE</td>
</tr>
<tr>
<td>3511.736478 FtLQ4i1LMP060KenK9 3 0676549500C6A380</td>
</tr>
<tr>
<td>3513.557920 FzMJtN2WvGlBjQmAdE 3 7C653E7DFE20BF0E</td>
</tr>
<tr>
<td>3513.573938 F5v6ic30yxSRz40Fv 3 49853ED8F7165597</td>
</tr>
</tbody>
</table>

Certificate path in Google Chrome

- GeoTrust Global CA
- Google Internet Authority G2
- *.google.cz
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key
  - Signature algorithm name
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key
  - Signature algorithm name
  - Issuer
x509.log

- X.509 certificate info
- Some of the available data:
  - Serial number
  - Common name
  - Validity of the certificate
  - Public key
  - Signature algorithm name
  - Issuer
  - SAN DNS (Subject alternative name extension of the certificate)
Interconnection of logs

conn.log

_____________________
_____________________
_____________________
_____________________
key ...................
_____________________
_____________________

ssl.log

_____________________
_____________________
_____________________
_____________________
key ...................
_____________________
_____________________
SSL aggregation

- conn.log
- ssl.log
- x509.log

SSL aggregation
### SSL Aggregation

#### conn.log

<table>
<thead>
<tr>
<th>IP</th>
<th>ClientSID</th>
<th>Date</th>
<th>Port</th>
<th>SourceIP</th>
<th>DestinationIP</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>131.728991</td>
<td>CgFZEVv44wSP9QljnR6</td>
<td>10.0.2.15</td>
<td>49163</td>
<td>104.108.46.209</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
</tr>
<tr>
<td>128.944596</td>
<td>CK8hoP3M4XoQDJSxRi</td>
<td>10.0.2.15</td>
<td>49162</td>
<td>52.222.174.197</td>
<td>80</td>
<td>tcp</td>
<td>http</td>
</tr>
<tr>
<td>132.428801</td>
<td>Cjkxw3NuUE41WtAB</td>
<td>10.0.2.15</td>
<td>49167</td>
<td>52.222.171.204</td>
<td>443</td>
<td>tcp</td>
<td>ssl</td>
</tr>
<tr>
<td>132.428803</td>
<td>D0wDN17bo5uKw07kf</td>
<td>10.0.2.15</td>
<td>49166</td>
<td>52.222.171.204</td>
<td>443</td>
<td>tcp</td>
<td>ssl</td>
</tr>
<tr>
<td>132.430278</td>
<td>CFPuv4I7yFo9h3tP6</td>
<td>10.0.2.15</td>
<td>49169</td>
<td>52.222.171.204</td>
<td>443</td>
<td>tcp</td>
<td>ssl</td>
</tr>
</tbody>
</table>

#### ssl.log

<table>
<thead>
<tr>
<th>IP</th>
<th>ClientSID</th>
<th>Date</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>132.478442</td>
<td>Cjkxw3NuUE41WtAB</td>
<td>10.0.2.15</td>
<td>443</td>
<td>TLSv12</td>
</tr>
<tr>
<td>132.481833</td>
<td>CFPuv4I7yFo9h3tP6</td>
<td>10.0.2.15</td>
<td>443</td>
<td>TLSv12</td>
</tr>
<tr>
<td>132.483473</td>
<td>CHPgsdpxqT1k2pxl</td>
<td>10.0.2.15</td>
<td>443</td>
<td>TLSv12</td>
</tr>
<tr>
<td>132.495937</td>
<td>CIPPIms5VQsGp4Si</td>
<td>10.0.2.15</td>
<td>443</td>
<td>TLSv12</td>
</tr>
<tr>
<td>132.494901</td>
<td>CAFZdW3MYCNWgYLuuv</td>
<td>10.0.2.15</td>
<td>443</td>
<td>TLSv12</td>
</tr>
</tbody>
</table>

#### x509.log

<table>
<thead>
<tr>
<th>IP</th>
<th>ClientSID</th>
<th>Date</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>132.527217</td>
<td>5A9C64361BFC92A79B1DD9CFB99E48EC</td>
<td>3</td>
<td>0CA9</td>
<td>CN=</td>
</tr>
<tr>
<td>132.527217</td>
<td>FZy2zo28cimnSKCR01</td>
<td>3</td>
<td>01FDB3EB6ECA75C888438B724BFCB91</td>
<td>CN=</td>
</tr>
<tr>
<td>133.579209</td>
<td>FA8t03GcfnculzHud</td>
<td>3</td>
<td>5A000529CF2A5A6396D3FD74EC0001000529CF</td>
<td>CN=Microsoft IT SSL SHA2,OU</td>
</tr>
<tr>
<td>133.579209</td>
<td>F5bw2G14fJaazLlloc</td>
<td>3</td>
<td>0727A</td>
<td>CN=</td>
</tr>
<tr>
<td>134.111336</td>
<td>F5bw2G14fJaazLlloc</td>
<td>3</td>
<td>5A000529CF2A5A6396D3FD74EC0001000529CF</td>
<td>CN=</td>
</tr>
</tbody>
</table>
ssl-connect-unit

ssl-connect-unit ID:
- Source IP
- Destination IP
- Destination Port
- Protocol

1. SSL aggregation
2. SSL aggregation
3. SSL aggregation
4. SSL aggregation
1. SSL aggregation
   \{SrcIP, DstIP, DstPort, protocol\}

2. SSL aggregation
   \{SrcIP, DstIP, DstPort, protocol\}

N. SSL aggregation
   \{SrcIP, DstIP, DstPort, protocol\}

ssl-connect-unit ID:
\{SrcIP, DstIP, DstPort, protocol\}
High level features

● 40 different features
1. Number of SSL aggregations

ssl-connect-unit

1. SSL aggregation
2. SSL aggregation
   ...
N. SSL aggregation

Number of SSL aggregations
2. Mean of duration

3. Standard deviation of duration

```
ssl-connect-unit

1. SSL aggregation
2. SSL aggregation
... ...
N. SSL aggregation
```

```
Duration
x_1
x_2
...
... ...
N. SSL aggregation
```

Mean and standard deviation of durations
4. Mean of number of packets
5. Standard deviation of number of packets

<table>
<thead>
<tr>
<th>ssl-connect-unit</th>
<th>Number of packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>inbound</td>
</tr>
<tr>
<td>1. SSL aggregation</td>
<td>$x_1$</td>
</tr>
<tr>
<td>2. SSL aggregation</td>
<td>$x_2$</td>
</tr>
<tr>
<td></td>
<td>$\vdots$</td>
</tr>
<tr>
<td>N. SSL aggregation</td>
<td>$x_3$</td>
</tr>
</tbody>
</table>

Mean and standard deviation of number of packets
6. Mean of number of bytes

7. Standard deviation of number of bytes

ssl-connect-unit

1. SSL aggregation

2. SSL aggregation

\[ \ldots \]

N. SSL aggregation

<table>
<thead>
<tr>
<th>Number of bytes</th>
<th>( x_1 )</th>
<th>( x_1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>inbound</td>
<td>( x_2 )</td>
<td>( x_2 )</td>
</tr>
<tr>
<td>outbound</td>
<td>( x_3 )</td>
<td>( x_3 )</td>
</tr>
</tbody>
</table>

Mean and standard deviation of number of bytes
8. Ratio of established and not established states

ssl-connect-unit

1. SSL aggregation

2. SSL aggregation

N. SSL aggregation

State of connection

Established

Not established

Established

Ratio of established and not established states
9. Mean of 2nd level time difference

10. Standard deviation of 2nd level time difference

<table>
<thead>
<tr>
<th>Connection records</th>
<th>1st time difference</th>
<th>2nd time difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SSL aggregation</td>
<td>Time = 06:00</td>
<td>20 min</td>
</tr>
<tr>
<td>2. SSL aggregation</td>
<td>Time = 06:20</td>
<td>0 min</td>
</tr>
<tr>
<td>3. SSL aggregation</td>
<td>Time = 06:40</td>
<td>0 min</td>
</tr>
<tr>
<td>4. SSL aggregation</td>
<td>Time = 07:00</td>
<td>15 min</td>
</tr>
<tr>
<td>5. SSL aggregation</td>
<td>Time = 07:05</td>
<td>5 min</td>
</tr>
</tbody>
</table>
11. Ratio of TLS and SSL version

- SSL aggregation
- SSL aggregation
- SSL aggregation

<table>
<thead>
<tr>
<th>TLS version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.0</td>
</tr>
<tr>
<td>SSL 2.0</td>
</tr>
<tr>
<td>TLS 1.3</td>
</tr>
</tbody>
</table>

Ratio of TLS and SSL versions
12. Number of different certificates

ssl-connect-unit

1. SSL aggregation
2. SSL aggregation
N. SSL aggregation

Certificate serial number

aaaaaa

Number of different certificates

bBBBB
13. Mean of certificate validity length
14. Standard deviation of certificate validity length

ssl-connect-unit

1. SSL aggregation
   Length of certificate validity
   5 days

2. SSL aggregation
   2020 days

\[ \ldots \]

N. SSL aggregation

\[ \ldots \]

Mean of unique certificate validity length

\[ 01.01.2010 \quad 01.01.2020 \]
15. Mean of certificate validity during the capture
16. Standard deviation of certificate validity during the capture
17. Weighted mean of public keys

ssl-connect-unit

1. SSL aggregation
2. SSL aggregation
... N. SSL aggregation

Ratio of validity during the capture

Weighted mean of public keys

1024
2048
2048
18. Mean of certificate path length
19. Standard deviation of certificate path length
20. Mean of number of domains in SAN DNS
21. Standard deviation of number of domains in SAN DNS

ssl-connect-unit

1. SSL aggregation
2. SSL aggregation
N. SSL aggregation

SAN dns

*.google.com,*.android.com,
*.appengine.google.com,*.cloud.google.com,
webproces.club, wprocessing.club

Mean of number domains in SAN DNS
22. Ratio of common name and SAN DNS

ssl-connect-unit

1. SSL aggregation
2. SSL aggregation
N. SSL aggregation

Is common name part of SAN DNS?

Yes
No

Ratio of true and false states
## Data model

<table>
<thead>
<tr>
<th>ssl-connect-unit</th>
<th>40 features</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{ 10.0.2.15, 54.201.174.90, 443, tcp }</code></td>
<td>f1 f2 f3 ... f40</td>
<td>Normal</td>
</tr>
<tr>
<td><code>{ 10.0.2.109, 173.194.122.30, 443, tcp }</code></td>
<td>f1 f2 f3 ... f40</td>
<td>Malware</td>
</tr>
</tbody>
</table>
Normal dataset

- **All ssl-connect-units:**
  - Normal: 46,387
  - Malware: 8,313

- **All SSL-aggregation:**
  - Normal: 1,357,112
  - Malware: 552,919

- **All unique certificates:**
  - Normal: 7,040
  - Malware: 1,579
Machine learning algorithms
XGBoost

- Extreme Gradient Boosting
- Tree booster with logistic regression
- Parameters:
  - max depth — describe maximum depth of a tree
  - gamma — minimum loss reduction required to make a further partition on a leaf node of the tree.
  - min child weight — minimum sum of instance weight (hessian) needed in a child.

Random forest

- Random Forest Classifier model that is an estimator that fits a number of decision tree classifiers on various sub-samples
Neural Network

- MLP Classifier (Multi-layer Perceptron classifier)
- stochastic gradient descent with Adam (Adaptive Moment Estimation)

SVM

- Radial Basis Function (RBF) kernel
- perform a non-linear classification using the kernel trick, mapping inputs into high-dimensional feature spaces
Experiments
Experiments

1. Split dataset to N same subsets

- Each subset contains unique malware test data
Experiments

1. Split dataset to \( N \) same subsets
2. For each subset:
   a. Split subset for training and testing data
Experiments

1. Split dataset to N same subsets
2. For each subset:
   a. Split subset for training and testing data
   b. Cross Validation on training data
Experiments

1. Split dataset to N same subsets
2. For each subset:
   a. Split subset for training and testing data
   b. Cross Validation on training data
   c. Train on all training data and test on test data
Experiments

1. Split dataset to N same subsets
2. For each subset:
   a. Split subset for training and testing data
   b. Cross validation on training data
   c. Train on all training data and test on testing data
3. Final result is an average of all results in subsets
Measures

Accuracy = (TP + TN) / (TP + TN + FP + FN)

False Positive Rate = FP / (FP + TN)

False Negative Rate = FN / (FN + TP)

Sensitivity = TP / (TP + FN)

F1 score = 2TP / (2TP + FP + FN)
Learning curve - XGBoost
Learning curve - Random Forest
Experiment 1
Experiment 1

● Subset 1
  ○ Training
    ■ Normal: 4,160 ssl-connect-units
    ■ Malware: 4,156 ssl-connect-units
  ○ Testing
    ■ Normal: 4,160 ssl-connect-units
    ■ Malware: 4,160 ssl-connect-units

● Subset 2
  ○ Training
    ■ Normal: 4,160 ssl-connect-units
    ■ Malware: 4,156 ssl-connect-units
  ○ Testing
    ■ Normal: 4,160 ssl-connect-units
    ■ Malware: 4,160 ssl-connect-units
Experiment 1

- **Training: 50% - 50%**
  - Normal: 4,160 ssl-connect-units
  - Malware: 4,156 ssl-connect-units

- **Testing: 50% - 50%**
  - Normal: 4,160 ssl-connect-units
  - Malware: 4,160 ssl-connect-units
Experiment 1

<table>
<thead>
<tr>
<th></th>
<th>Normal</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>4160</td>
<td>4156</td>
</tr>
<tr>
<td>Testing</td>
<td>4160</td>
<td>4160</td>
</tr>
</tbody>
</table>

Legend: Normal  Malware
Experiment 1

- XGBoost
  - Cross validation accuracy: 91.58%
  - Testing accuracy: 92.11%
  - False Positive Rate: 7.5%
  - False negative rate: 8.5%
  - Sensitivity: 91.48%
  - F1 Score: 51.96%
Experiment 1

- Random Forest
  - Cross validation accuracy: 90%
  - Testing accuracy: 90%
  - False Positive Rate: 8.3%
  - False negative rate: 11.7%
  - Sensitivity: 88.2%
  - F1 Score: 89.76%
Experiment 2
Experiment 2

- Subset 1
  - Training
    - Malware: 7,232 ssl-connect-units
    - Normal: 10,205 ssl-connect-units
  - Testing
    - Malware: 1,081 ssl-connect-units
    - Normal: 36,182 ssl-connect-units

- Subset 2
  - Training
    - Malware: 7,232 ssl-connect-units
    - Normal: 10,205 ssl-connect-units
  - Testing
    - Malware: 1,081 ssl-connect-units
    - Normal: 36,182 ssl-connect-units

- Subset 3

- Subset 8
  - Training
    - Malware: 7,567 ssl-connect-units
    - Normal: 10,205 ssl-connect-units
  - Testing
    - Malware: 746 ssl-connect-units
    - Normal: 36,182 ssl-connect-units
Experiment 2

- **Training: 40% - 60%**
  - Malware: 7,232
  - Normal: 10,205

- **Testing: 3% - 97%**
  - Malware: 1,081
  - Normal: 36,182
Experiment 2

- XGBoost
  - Cross validation accuracy: 92.45%
  - Testing accuracy: 94.33%
  - False Positive Rate: 5.54%
  - False negative rate: 10.11%
  - Sensitivity: 89.89%
  - F1 Score: 46.96 %
Experiment 2

- Random Forest
  - Cross validation accuracy: 91.21%
  - Testing accuracy: 95.65%
  - False Positive Rate: 4.05%
  - False negative rate: 14.82%
  - Sensitivity: 85.18%
  - F1 Score: 52.24%
Feature importance

1. Certificate length of validity
2. Inbound and outbound packets
3. Validity of certificate during the capture
4. Duration
5. Number of domains in certificate
6. SSL/TLS version
7. Periodicity
Malware and Certificates

- Certificates used by Malware in Alexa 1000 ~ 50%
- Certificates used by Normal in Alexa 1000 ~ 30%

- Usage of certificate by Malware is almost correct
Did we achieve the goal?
Thanks for attention!

František Střasák
strasfra@fel.cvut.cz
@FrenkyStrasak

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote