Analysis of Cobalt Strike network traffic obfuscation in C2 communication

Vincent van der Eijk & Coen Schuijt

University of Amsterdam

vincent.vandereijk@os3.nl, coen.schuijt@os3.nl

July 3, 2020
Introduction

- Red and Blue Teaming
- RAT $\rightarrow$ Botnet
- Cobalt Strike
- APTs

Figure 1: Cobalt strike logo [https://cobaltstrike.com/]
Main research question

”How can we distinguish obfuscated Cobalt Strike beacons from genuine traffic based on identifying features?”

Sub questions

1. Which features can we extract from network traffic generated by malleable C2 profiles?
2. Can we detect a Cobalt Strike beacon using a malleable profile with one or more of those features?
Figure 2: Common C2 network setup

- Beacon
- Domain redirection
- Redirector/proxy
- C2 Server
Malleable Profile

- Defines beaconing behaviour
- HTTP parameters
- Encoding
- Highly customizable

```plaintext
set sleeptime "5000";
set jitter "0";
set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";

http-get {
    set uri "/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books";
}
```

Listing 1: Snippet from the amazon.profile
Related work

- Little scientific research on Cobalt Strike
- No research specific to malleable profiles
- Botnet traffic detection researched thoroughly

Sources

- L. van Duijn (2014)
  Beacon detection in PCAP files
- J. Dreijer (2015)
  StealthWare - Social Engineering Malware
Methodology

1. Network Topology
   - Setup Target Machine
   - Configure domain redirection
   - Setup redirector
   - Configure C2 Server

2. Data capturing
   - Configure ncapd listener
   - Configure softflow daemon
   - Install packet capture software

3. Dataset generation
   - Benign: browse amazon
   - Malicious: capture HTTP(S) beacon traffic
   - Mixed: HTTP(S) beacon & tcpplay
   - Mixed: HTTP(S) beacon & office use simulation

4. Feature engineering
   - Parse dataset
   - Group dataset
   - Filter dataset
   - Create identifying feature

5. Testing
   - Test feature on dataset
   - Plot results

Figure 3: Project approach
Infrastructure setup (I/II)

1. **Target**
   - Windows 10 (1909)
   - NAT interface

2. **CDN**
   - Amazon CloudFront
   - Domain redirection (Host Header, Redirector IP)

3. **Redirector**
4. **C2**

Figure 4: Infrastructure setup
Figure 4: Infrastructure setup

3. Redirector
   - socat proxy
   - 443, 80

4. C2 Server
   - Cobalt Strike 4.0
   - amazon.profile
Data gathering (I/V)

- Benign
  - PCAPS for HTTP
- Malicious
  - NetFlow for HTTPS
- Mixed
  - Active beacon
  - Simulate user
    - browsing
    - updating
    - mailing
    - ...
  - Reproduceable dataset
- External
  - CTU-13 (Botnet-43)$^1$
  - 6M flows, university network
  - Stratosphere Research Laboratory (CZ)

Detection algorithm (I/II)

Read NetFlow data
Creating host objects
Append flow to host (src IP)

Figure 5: Detection algorithm pt.1
4 Filter flows
5 Apply feature (Host)
6 Alert

Figure 6: Detection algorithm pt.2
Results

- Amazon.profile traffic analysis (Cobalt Strike)
  - HTTP Beacon
  - Benign Amazon network traffic
  - HTTPS Beacon
- Beacon detection algorithm
- Detection accuracy
## Figure 7: Packet capture for HTTP beacon

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000785</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>2</td>
<td>5.026288</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>3</td>
<td>10.059287</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>4</td>
<td>15.071252</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>5</td>
<td>20.082889</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>6</td>
<td>25.108927</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>7</td>
<td>30.131122</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>8</td>
<td>35.145989</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
<tr>
<td>9</td>
<td>40.157684</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>HTTP</td>
<td>549</td>
<td>GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1</td>
</tr>
</tbody>
</table>

Frame 4: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface Device\NPF_\{FDCE157-1133-4C81-81A8-9FCB5346F432\}, Id 0
Transmission Control Protocol, Src Port: 52250, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
Hyptertext Transfer Protocol
GET /s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books HTTP/1.1

Accept: */*
Host: www.amazon.com
Cookie: skin-noskin; session-token=R4wPMK7XF4mHljQIbLtHnATDuHI53+rf7CZ87xsvmgkl7cc58riu6vynHVYMLOILS2qW840shR+98hULuInfuU/208GY3+AOvgaDL1...
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache

[Full request URI: http://www.amazon.com/s/ref=nb_sb_noss_1/167-3294888-02629499/field-keywords=books]
[HTTP request 1/1]
[Response in Frame: 6]
Amazon profile traffic analysis: Benign (II/V)

Figure 8: Packet capture for benign Amazon traffic
## Amazon traffic analysis: HTTPS Beacon (III/V)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>66</td>
<td>SYN Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1</td>
</tr>
<tr>
<td>2</td>
<td>0.000491</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>60</td>
<td>SYN, ACK Seq=0 Ack=1 Win=64240 Len=0 MSS=1460</td>
</tr>
<tr>
<td>3</td>
<td>0.000649</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>ACK Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>4</td>
<td>0.001061</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TLSv1.2</td>
<td>238</td>
<td>Client Hello</td>
</tr>
<tr>
<td>5</td>
<td>0.001401</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>60</td>
<td>443 → 52424 [ACK] Seq=1 Ack=185 Win=64240 Len=0</td>
</tr>
<tr>
<td>6</td>
<td>0.001356</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TLSv1.2</td>
<td>144</td>
<td>Server Hello</td>
</tr>
<tr>
<td>7</td>
<td>0.001448</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>443 → 52424 [ACK] Seq=185 Ack=91 Win=65535 Len=0</td>
</tr>
<tr>
<td>8</td>
<td>0.001804</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TLSv1.2</td>
<td>68</td>
<td>Change Cipher Spec</td>
</tr>
<tr>
<td>9</td>
<td>0.001857</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>443 → 52424 [ACK] Seq=185 Ack=97 Win=65535 Len=0</td>
</tr>
<tr>
<td>10</td>
<td>0.001934</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TLSv1.2</td>
<td>99</td>
<td>Encrypted Handshake Message</td>
</tr>
<tr>
<td>11</td>
<td>0.001958</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>443 → 52424 [ACK] Seq=185 Ack=142 Win=65535 Len=0</td>
</tr>
<tr>
<td>12</td>
<td>0.001996</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TLSv1.2</td>
<td>105</td>
<td>Change Cipher Spec, Encrypted Handshake Message</td>
</tr>
<tr>
<td>13</td>
<td>0.001563</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>60</td>
<td>443 → 52424 [ACK] Seq=142 Ack=236 Win=64240 Len=0</td>
</tr>
<tr>
<td>14</td>
<td>0.001301</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TLSv1.2</td>
<td>578</td>
<td>Application Data</td>
</tr>
<tr>
<td>15</td>
<td>0.001327</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>60</td>
<td>443 → 52424 [ACK] Seq=142 Ack=760 Win=64240 Len=0</td>
</tr>
<tr>
<td>16</td>
<td>0.001474</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TLSv1.2</td>
<td>339</td>
<td>Application Data</td>
</tr>
<tr>
<td>17</td>
<td>0.005476</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TLSv1.2</td>
<td>85</td>
<td>Encrypted Alert</td>
</tr>
<tr>
<td>18</td>
<td>0.005434</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>443 → 52424 [ACK] Seq=760 Ack=459 Win=65535 Len=0</td>
</tr>
<tr>
<td>19</td>
<td>0.005528</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>FIN, ACK Seq=760 Ack=459 Win=65535 Len=0</td>
</tr>
<tr>
<td>20</td>
<td>0.005125</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>54</td>
<td>RST, ACK Seq=761 Ack=459 Win=0 Len=0</td>
</tr>
<tr>
<td>21</td>
<td>0.005190</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>60</td>
<td>443 → 52424 [ACK] Seq=459 Ack=761 Win=64239 Len=0</td>
</tr>
<tr>
<td>22</td>
<td>0.005206</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>54</td>
<td>RST Seq=761 Win=0 Len=0</td>
</tr>
<tr>
<td>23</td>
<td>0.006431</td>
<td>172.16.22.129</td>
<td>145.100.104.47</td>
<td>TCP</td>
<td>60</td>
<td>443 → 52425 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1</td>
</tr>
<tr>
<td>24</td>
<td>0.006483</td>
<td>145.100.104.47</td>
<td>172.16.22.129</td>
<td>TCP</td>
<td>60</td>
<td>443 → 52425 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460</td>
</tr>
</tbody>
</table>

**Figure 9:** Packet capture for Amazon HTTPS beacon
### Figure 10: NetFlow data for HTTPS beacon

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Tos</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-07-02 20:39:39.472</td>
<td>0.064</td>
<td>TCP</td>
<td>172.16.22.129:50223</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>13</td>
<td>1297</td>
</tr>
<tr>
<td>2020-07-02 20:39:44.552</td>
<td>0.056</td>
<td>TCP</td>
<td>172.16.22.129:50224</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>13</td>
<td>1297</td>
</tr>
<tr>
<td>2020-07-02 20:39:49.616</td>
<td>0.059</td>
<td>TCP</td>
<td>172.16.22.129:50225</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:39:54.689</td>
<td>0.058</td>
<td>TCP</td>
<td>172.16.22.129:50226</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:39:59.754</td>
<td>0.060</td>
<td>TCP</td>
<td>172.16.22.129:50227</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:04.827</td>
<td>0.059</td>
<td>TCP</td>
<td>172.16.22.129:50228</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:09.893</td>
<td>0.058</td>
<td>TCP</td>
<td>172.16.22.129:50229</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:14.972</td>
<td>0.064</td>
<td>TCP</td>
<td>172.16.22.129:50230</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:20.046</td>
<td>0.060</td>
<td>TCP</td>
<td>172.16.22.129:50231</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:25.111</td>
<td>0.062</td>
<td>TCP</td>
<td>172.16.22.129:50232</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:30.183</td>
<td>0.055</td>
<td>TCP</td>
<td>172.16.22.129:50233</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:35.248</td>
<td>25.360</td>
<td>TCP</td>
<td>172.16.22.129:50234</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:40.328</td>
<td>0.060</td>
<td>TCP</td>
<td>172.16.22.129:50235</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:45.492</td>
<td>0.059</td>
<td>TCP</td>
<td>172.16.22.129:50236</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:50.466</td>
<td>0.060</td>
<td>TCP</td>
<td>172.16.22.129:50237</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:40:55.540</td>
<td>13.428</td>
<td>TCP</td>
<td>172.16.22.129:50238</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:41:00.608</td>
<td>0.064</td>
<td>TCP</td>
<td>172.16.22.129:50239</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:41:05.684</td>
<td>0.059</td>
<td>TCP</td>
<td>172.16.22.129:50240</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:41:10.755</td>
<td>0.052</td>
<td>TCP</td>
<td>172.16.22.129:50241</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:41:15.819</td>
<td>0.063</td>
<td>TCP</td>
<td>172.16.22.129:50242</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:41:20.892</td>
<td>0.059</td>
<td>TCP</td>
<td>172.16.22.129:50243</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
<tr>
<td>2020-07-02 20:41:25.956</td>
<td>0.063</td>
<td>TCP</td>
<td>172.16.22.129:50244</td>
<td>145.100.104.47:443</td>
<td>APRSF</td>
<td>0</td>
<td>12</td>
<td>1257</td>
</tr>
</tbody>
</table>

Summary: total flows: 22, total bytes: 27974, total packets: 272, avg bps: 2100, avg pps: 2, avg bpp: 102
Total flows processed: 47, Blocks skipped: 0, Bytes read: 3888
Sys: 0.002s flows/second: 20991.5 Wall: 0.000s flows/second: 770491.8
We identified the following features:

- Periodicity
- Consistent byte size of flows
- Short flow duration
- TCP Flags
- Lack of DNS requests
Beacon detection

Figure 11: Linear regression for regular HTTPS network traffic shows a weak correlation ($r=0.854$)

Figure 12: Linear regression for C2 server network traffic shows a high correlation ($r=0.999$)
Results: Accuracy

Table 1: Overview of NetFlow streams that the detection algorithm was able to classify correctly as either benign (good) or malicious (bad)

<table>
<thead>
<tr>
<th>Predicted</th>
<th>Actual</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Good</td>
<td>Bad</td>
</tr>
<tr>
<td>Good</td>
<td>128910</td>
<td>2</td>
</tr>
<tr>
<td>Bad</td>
<td>5</td>
<td>15</td>
</tr>
</tbody>
</table>

$$\text{ACC} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{13 + 128267}{13 + 128267 + 5 + 2} = 99.996\%$$
Difficult to obtain a large dataset with benign network traffic
Only tested on our own malware samples and infrastructure
Q1: Which features can we extract from network traffic generated by malleable C2 profiles?

- Time interval
- Byte size of flow
- Flow duration
- TCP flags
- DNS requests

Q2: Can we detect a Cobalt Strike beacon using a malleable profile with one or more of those features?

- All features except the correlation to DNS requests and the TCP RST flag are useable
How can we distinguish obfuscated Cobalt Strike beacons from genuine traffic based on identifying features?
- Filter rules based on identified features
- Detection algorithm using linear regression
Future Work

- Further research the TCP RST flag behaviour
- Expand the detection algorithm to fingerprint threat actors
- Modify the detection algorithm to support real-time detection
Key findings

- C2 communication of Cobalt Strike shows periodicity
- We are able to detect other profiles than the Amazon profile
- Avoid detection by changing the beaconsing interval regularly