On the Feasibility of Automating Stock Market Manipulation

Carter Yagemann, Simon Chung, Erkam Uzun, Sai Ragam, Brendan Saltaformaggio, Wenke Lee

December 10th, 2020
Markets change with technology...
Unknowns of automated market manipulation…

- What can bots automate?
- How can they automate, communicate?
- Who will they compromise?
- How will they evade detection?
• What is layering manipulation? How does it work?
• What are the current defenses?
• How could a trading malware work?
• What would its impact be?
• The future…
What is *layering* manipulation? How does it work?
What are the current defenses?
How could a trading malware work?
What would its impact be?
The future…
Market basics (simplified)…

Seller → Exchange → Order Book → Buyer

Ask → Bid
Order book...

**Spread**

- **Bids**
- **Asks**

**Layers**
Layering example...

<table>
<thead>
<tr>
<th>Bids</th>
<th>Asks</th>
<th>Spoofs</th>
<th>Real Bid</th>
<th>Cancels</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>35</td>
<td>10</td>
<td>10</td>
<td>35</td>
</tr>
<tr>
<td>15</td>
<td>40</td>
<td>40 (25)</td>
<td>35</td>
<td>40</td>
</tr>
<tr>
<td>35</td>
<td>35</td>
<td>75 (40)</td>
<td>35</td>
<td>30</td>
</tr>
<tr>
<td>20</td>
<td>20</td>
<td>80 (40)</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>70 (40)</td>
<td></td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>50 (40)</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>40 (25)</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>35</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>
• What is *layering* manipulation? How does it work?
• What are the current defenses?
• How could a trading malware work?
• What would its impact be?
• The future…
Incomplete views poorly suited to detecting large-scale collusion.

We’ll come back to them at the end.
What is *layering* manipulation? How does it work?
What are the current defenses?
*How could a trading malware work?*
What would its impact be?
The future...
Bot2Stock...

1. Victim’s Browser
2. Malware Browser
3. Bot2Stock Controller
4. HTTP(S) Proxy
5. Brokerage Website
6. Email Website

Steps:
- (1) Sniff Cookies
- (2) Insert Email Filters
- (3) Bot2Stock Orders
- (4) Edit History

Processes:
- Legitimate Orders
- Legitimate History
What is layering manipulation? How does it work?
What are the current defenses?
How could a trading malware work?
What would its impact be?
The future...
Simulation challenges…

- Modeling slippage
- Stock value beliefs
- Factoring computation, communication
Value beliefs...

Agent (Trader)

Order Book

Agent (Exchange)

subscriptions

P + n

Agent ("Belief Oracle")

True Fundamental Value
Findings…

- Attack Duration: < 1 minute
- Network Latency Tolerance: > 200% added (3x)
- Required Trade Volume: 1.5%
- Per-Session ROI: 2.8% ROI
- Annual ROI: 1022%
Example...

- IBM, March 2020: 9,120 shares traded per minute
- $9,120 \times 1.5\% \times \text{Market Price} \approx \$5,000\text{/session}$
- 2.8\% \text{ROI} \times 1 \text{ session per day} \times 252 \text{ trading days} \times \$100k \text{ initial investment}$
- **Profit**: \textbf{\$1 million}
- **Botnet Loss**: Commission Fees
- **Self-Sustaining**
• What is *layering* manipulation? How does it work?
• What are the current defenses?
• How could a trading malware work?
• What would its impact be?
• The future...
The future...

• Mandating 2FA? No.
• More brokerage anomaly detection? Suboptimal.
• Improve alerting? Yes!
• Consolidated Audit Trail (CAT)