Sonia Burney
Solutions Architect
@soniaburney

Brent Maynard
Security Architect
@baammers
What is Credential Abuse?
Credential Theft: How do they do it?

- Phishing Kits
- Keyloggers
- Hijack Behavior
- Credential Leaks
Leaked credentials lead to credential abuse, which can be used in account takeover. Financial gain follows through shopping, accounts, and data access. The diagram shows the process from buy credentials to log in and financial gain.
### Negative Consequences Resulting from a Credential Stuffing Attack

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application downtime from large spikes in login traffic</td>
<td>67%</td>
</tr>
<tr>
<td>Costs to remediate compromised accounts, including call-center time or manual investigation/analysis by the security or fraud team</td>
<td>63%</td>
</tr>
<tr>
<td>Lower customer satisfaction</td>
<td>50%</td>
</tr>
<tr>
<td>Compromised accounts leading to fraud-related financial losses</td>
<td>43%</td>
</tr>
<tr>
<td>Lost business due to customers switching to competitors</td>
<td>41%</td>
</tr>
<tr>
<td>Damaged brand equity from news stories or social media</td>
<td>17%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

Total annualized cost of credential stuffing, excluding fraud, can average more than $6 million.

Monetary cost of fraud due to credential stuffing attacks ranges from $546K to $54 million.
45 major brand websites
Included retail, banking, travel, media, gaming and other industries
24 hour data collection period during September 2017
420 distinct botnet signatures identified
34,225,052 unique accounts targeted

591,774,594 Total logins observed
393,924,296 Detected as malicious 66%
Evolving bot landscape

DETECTION

- Recorded human behavior
- Behavior anomaly detection
- Browser fingerprinting
- HTTP anomaly detection
- Rate limiting
- IP blocking

Simple  |  Sophisticated

- Single IP
- Multiple IPs
- Low request rate
- Randomized user agent
- Browser impersonation
- Session replay
- Full cookie support
- JavaScript support
Simple Bots

- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

Sophisticated Bots
Simple Bots

- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

Rate Detection

Sophisticated Bots
Simple Bots

- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

Session Tracking

Sophisticated Bots
Simple Bots

- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

Sophisticated Bots

Sliding Window
Script on single machine
Distributed IPs
Low Request Rate
Randomized User Agent
Browser Impersonation
Session Replay
Full Cookie Support
Partial/Full JavaScript Support
Fingerprint Spoofing
Recorded Human Behavior

Simple Bots

Workflow Validation

Sophisticated Bots
Simple Bots

- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

http Anomaly

Sophisticated Bots
**Simple Bots**

- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

**Sophisticated Bots**

**Behavioral Detection**
Evolution of Bot Detection and Mitigation Approach

- Identify
- Slow: 8-10s
- Delay: 1-3s
- Block
- Customized Content
Takeways...

- One password to rule them all?
  - Understand **ALL** login processes and policies
- Understand what real users and bad actors look like
- Identify multiple detection and mitigation strategies
- Foreshadowing the credential abuse landscape
Next Steps...

• Pivot in focus of threat surface
• Growth of API/IoT traffic
• Expansion of Native Application Endpoints
• AI and Machine Learning