Crowd Sourced Security

Applying the Wisdom of the Crowd to Cyber Defenses

John ‘Lex’ Robinson
Anti-Phishing / Cyber Security Strategist
The Wisdom of Crowds

A theory which proposes the answers to difficult questions are best reached by a group of alert, intelligent individuals rather than by single, even respected, experts alone.

The author highlights tragedies that could have been avoided had a greater number of persons been consulted before crucial decisions were made.
The Intelligence Process

**Actionable Intelligence** consists of bits of data, that when grouped together, reveal trends and a "big picture" of a corner of the world. The requested data are delivered by a field agent to the case officer. A case officer sometimes has a network of field agents who do his legwork, giving him small bits of information from various sources. An example might be production numbers for several units of a business that's owned by U.S. interests, but operated by the native population in different locations throughout the country. The case officer assembles these bits of information and either performs his own analysis or sends them to the U.S., where other analysts collate them with more data from other case officers and field agents.
Application to Cyber Security

User Recognition

A group of alert, intelligent individuals…

Reporting Capability

The requested data are delivered to experienced incident responders…

Advanced Analysis and Resolution

Collated data is analyzed and acted upon to avoid breaches.
The Cyber Kill Chain

NOTE: With development of crowd sourced intelligence capabilities, it’s possible to get ‘Left of Breach’
Use Case - Minutes, Not Months

11:48 Spear Phishing Campaign launched

11:49 Phishing emails begin to be reported

12:00 Tier One Analyst escalates to Second Tier

12:07 Initial investigation completed and email team notified

12:07 Email team begins removing threat from their environment

NOTE: Median time for internal discovery of breach is 80 days and external discovery is 107 days
DOES YOUR ORGANIZATION HAVE THE CAPABILITY TO RESIST AN ACTIVE PHISHING THREAT?
WHAT YOU NEED TO KNOW

Understand how your organization is being attacked and model as simulations in your anti-phishing program.

Active Threats

Recognition and Reporting Capability

- Average Client Resiliency Rate
  - Mar-17: 0.81
  - Apr-17: 1.20
  - May-17: 3.83
  - Jun-17: 6.23
  - Jul-17: 4.40
  - Aug-17: 5.63

Resiliency Rate vs Benchmark Resiliency
Developing Crowed Sourced Capabilities

User Recognition
Help your users recognize active threats through immersive simulations.

Reporting Capability
Provide users an automated reporting process to ensure appropriate collection of data.

Advanced Analysis and Resolution
Enable incident responders with solutions that prioritize data for analysis and assist the mitigation process.
Program Best Practices

1) Be transparent with your users – encourage self reporting
2) Focus measures on recognition and reporting – NOT susceptibility
3) Be consistent with presentation of active threat simulations
4) Enable in-line analysis and mitigation capabilities
**Encourage Self Reporting**

### Behavior Analysis

<table>
<thead>
<tr>
<th>Reported</th>
<th>Response</th>
<th>Behavior</th>
<th>Count</th>
<th>%</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Report</td>
<td>Opened the Attachment</td>
<td>Undesirable</td>
<td>76</td>
<td>14.23%</td>
<td>User viewed the phishing email then clicked the scenario link</td>
</tr>
<tr>
<td></td>
<td>(Did not Report)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Viewed Email</td>
<td>Neutral</td>
<td>0</td>
<td>0.00%</td>
<td>User viewed the phishing email but did not report the email</td>
</tr>
<tr>
<td></td>
<td>(Did not Report)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Action</td>
<td>No Response</td>
<td>Neutral</td>
<td>213</td>
<td>39.89%</td>
<td>Due to technical restrictions, we were unable to track these users.</td>
</tr>
<tr>
<td>Reported</td>
<td>Responded and Reported</td>
<td>Desirable</td>
<td>12</td>
<td>2.25%</td>
<td>User fell susceptible for the phishing email but did report it</td>
</tr>
<tr>
<td></td>
<td>Reported Only</td>
<td>Very Desirable</td>
<td>233</td>
<td>43.63%</td>
<td>User viewed the phishing email and reported it</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>534</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Because reporting is the behavior you want to increase, focus on those that fall susceptible and don’t report.
Consistency Drives Capability

Note: Trend recognition and reporting capabilities over time.
Enable In-Line Incident Response

1. **Filter**: Cut spam, internal emails
2. **Group**: Emails and attack patterns
3. **Match**: Rules on content, URLs and attachments
4. **Integrate**: With 3rd party threat analysis technologies

Actionable intelligence to enhance security investments
DEVELOPING RECOGNITION, REPORTING AND RESOLUTION CAPABILITIES LEADS TO MITIGATION OF ACTIVE THREATS
NOTE: As of February 2018, users across 30 organizations were reporting ~ 2,500 potential threats. Of these the percentage of malicious emails ranged from 10-12%. That is roughly 250 malicious (mitigated) emails making it past perimeter defenses (per month / per company).
• Check out our weekly blog @ phishme.com/blog
• Threat alerts – sign up for them @ phishme.com/threat-alerts
• Phishing Defense & Resiliency Report @ phishme.com/whitepaper/enterprise-phishing-resiliency-and-defense-report/