PHISHING in your own pond...

Gary Blackburn
May 2014
WHY?

* Valuable Training,
* Common attack vector,
* Attacks are successful

People are social creatures, with predictable behaviors!

Sophisticated technical controls aren’t enough…
Enter your bank account number.

OKEY-DOKEY.
THE APPROACH

1. Select targets – Random, representative
2. Execute Phish
3. Train victims, immediate feedback
4. Collect and analyze metrics
5. Report and train ALL USERS
MANAGING RISK

• Minimize operational impact
  • Small sample of users targeted; less than 15% of organization

• Contain exercise activity, reduce political risks
  • “Rogue” web site is hosted internally
  • Email blocking capability

• Reduce legal risks
  • No impersonation / only fictitious entities used
  • No Personally Identifiable Information (PII) collected on victims
MANAGING RISK

• De-confliction
  • Strong event communications plan

• Coordination
  • Stakeholders identified, trusted insiders established

• Event Integrity
  • A ‘safe
    • training event’, anonymous results

• Feedback
  • Victims immediate, users overall summary
EVENT OVERVIEW

1. Coordinate and select event date
2. Author/select phish email
3. Facilitate legal review
4. Develop landing page
5. Configure local DNS
6. Configure email gateway
7. Identify email recipients
8. Configure attack script and test phishing email
9. Notify stakeholders / trusted agents of event
10. Execute attack
11. Collect metrics
12. Prepare/send executive summary
13. Praise reporters
14. Prepare event recap training
15. Publish event recap
16. Publish final report

Legend
- CIO
- Analytics
- Lead
- Execution Team
- Network Defenders

---

10% Victim Rate
15% Report Rate
EVENT OVERVIEW

1. Rest assured, your personal identity will remain anonymous. The point of the exercise is to provide a realistic training experience that helps prepare you to face real-world phishing threats, not to take you over the coals.
2. BUT... don’t rest too easy. Take another look at the email you just received. Recognize the phishing attempt. Understand how to report it. It’s all part of your commitment to be prepared.
3. Complete the survey and participate in the hands-on demonstration. The training videos combined will take about an hour.
4. Be ready for the next email notification. It’s a phishing attempt. Remember... it’s only bait!!!
5. Select the next button...
1. Coordinate and select event date
2. Author/select phish email
3. Facilitate legal review
4. Develop landing page
5. Configure local DNS
6. Configure email gateway
7. Identify email recipients
8. Configure attack script and test phishing email/URL
9. Notify stakeholders/trusted agents of event
10. Execute attack
11. Collect metrics
12. Prepare/send executive summary
13. Praise reporters
14. Prepare event recap training
15. Publish event recap
16. Publish final report

Legend:
- Event Coordinator
- Network Defenders
- Execution Team
- Analytics Lead
- CIO

- 2 weeks
+ 2 weeks
**TECHNICAL APPROACH**

- **Pitcher** sends an email.
- The email is delivered to an **Email Security Device**.
- The Email Security Device identifies the email as phishing and forwards it to a **Catcher**.
- The Catcher redirects the email to a **“Rogue” Website**.
- The recipient/client clicks the link, which redirects them to a **Local DNS Server**.
- The recipient/client is directed to a **Rogue Website**.

Network Boundary:
- **WWW**
- **Phishing Recipient/Client**
- **Clicks link**
- **Replies or forwards**
- **E-Mail Server**
- **Local DNS Server**
EVENT OVERVIEW

1. Coordinate and select event date
2. Author/select phish email
3. Facilitate legal review
4. Develop landing page
5. Configure local DNS
6. Configure email gateway
7. Identify email recipients
8. Configure attack script and test phishing email/URL
9. Notify stakeholders / trusted agents of event
10. Execute attack
11. Collect metrics
12. Prepare/send executive summary
13. Praise reporters
14. Prepare event recap training
15. Publish event recap
16. Publish final report

Legend
- Event Coordinator
- Network Defenders
- Execution Team
- Analytics Lead
- CIO

- 2 weeks
- Event Execution
+ 2 weeks
Do your users know what to do?

First report within one minute of attack

Total reporting: 15.2%
TIMING OF VICTIMS VS NOTIONAL NET DEFENSE RESPONSE

1. First report (7 victims)
   Network defenders receive 1st user report of suspicious activity

2. Attack + 15 mins (24 victims)
   Reflects the point at which outbound web traffic to malicious IP(s) might be blocked, effectively blocking command and control

3. Attack + 2 hours (41 victims)
   Reflects the point at which phishing emails might be removed from infected mailboxes, removing the threat footprint and any associated footholds

Forbes had to repeat this response curve 3 times Over a 36 Hour period!

615 Phish
745 2nd Phish
815 Warning
1000 Administrative shutdown
OTHER METRICS

• Email Forwarding
  • On average, 4% of recipients attempt to forward email externally

• Email Replies
  • On average, 6% of recipients attempt to reply to fictitious sender
  • Most are the result of “out of office” agents (auto-replies)
  • Use of “out of office” can increase risk to the organization
PREDICTORS AND SCORING MODEL

Personalization

1. Low: no personalized characteristics (more likely to appear as SPAM)
2. Medium: refers to at least one characteristic familiar to the user (e.g., industry, region, company name)
3. High: contains highly personalized elements (spear-phishing by name or department)

Appeal/Applicability

1. Low: applicable to only a small number of recipients
2. Medium: applicable to a large number of recipients
3. High: potentially applicable to all recipients

Perceived Urgency

1. Low: recipient has a lot of time to respond (unlimited to weeks/days)
2. Medium: recipient has limited time to respond (day/hours)
3. High: recipient has very little time to respond (hour/minutes)

Consequence/Opportunity Lost

1. Low
2. Medium
3. High

TOTAL DIFFICULTY SCORE

4 Easy
5 Moderate
6 Difficult

Volley

1-3-4-8
EVENT OVERVIEW

1. Coordinate and select event date
2. Author/select phish email
3. Facilitate legal review
4. Develop landing page
5. Configure local DNS
6. Configure email gateway
7. Identify email recipients
8. Configure attack script and test phishing email/URL
9. Notify stakeholders / trusted agents of event
10. Execute attack
11. Collect metrics
12. Prepare/send executive summary
13. Praise reporters
14. Prepare event recap training
15. Publish event recap
16. Publish final report

Legend
- Event Coordinator
- Network Defenders
- Execution Team
- Analytics Lead
- CIO
# EVENT REPORTS

<table>
<thead>
<tr>
<th>Deliverable/Report</th>
<th>Target Audience</th>
<th>Periodicity/Timeline</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>CIO</td>
<td>Within 2 hours of event end</td>
<td>Executive summary of the event properties and event results (e.g., 37% failure rate).</td>
</tr>
<tr>
<td>Event Recap Article</td>
<td>All users</td>
<td>Within 24 hours of event end</td>
<td>Non-attributional summary and result of the phishing event. Identifies indicators of phishing attempt and how users should respond/report.</td>
</tr>
<tr>
<td>Detailed Report</td>
<td>CIO</td>
<td>Within two weeks of event end</td>
<td>Detailed report showing event approach, metrics, results and analysis.</td>
</tr>
<tr>
<td>Quarterly Progress Report</td>
<td>CIO</td>
<td>Quarterly, within two weeks of event end</td>
<td>Detailed report highlighting successes, challenges, trends, etc. Identifies whether objectives were met/unmet.</td>
</tr>
</tbody>
</table>

“Event training recap” provides an opportunity for all users to learn from each training scenario.
SUMMARY

- Steady **increase** in user reporting in both real-world and exercise phishing scenarios
- Organizational victim rate has remained largely unchanged since the start (Average: 10%)
- Participant survey results overwhelmingly positive: 97% say live phishing scenarios realistic and impactful

**Insure your users know how to respond!**
DISCUSSION / QUESTIONS