Today’s Agenda

- A quick look back: 2008
- Looking forward to 2009
  - New threats
  - Mitigations
  - Predictions
- Incident response procedures
- Q&A
2008: What a year!

- Storm finally moves out
- Mac OS X becomes a target
- Windows: the usual suspects
- Phishing for passwords
- SSN’s for sale...again.
- Data for sale on eBay, cheap!
- TJX, Heartland, and disclosures, oh my!
- ...and, oh yeah, DNS
Looking forward: 2009

Ever considered a career in IT security?
New and Increasing Threats

- Directed custom code
- Spear phishing
- Flash drive madness
- Drive by web infections
- Conficker and other bot nastiness
Bots

Characteristics
- Conficker (Nine million+)
- Massive growth
- Targeted
- Sophistication at a new level

Mitigation
- Firewall hosts
- Apply software updates
- Reimage on schedule
Drive-by web infections

Characteristics
- Browser
- Media players
- Unpatched systems
- Legitimate websites
- Online ads as targets

Mitigation
- Keep browser up to date
- Use latest AV
- Scan for vulnerabilities
- Supporting applications
- Don’t surf as administrator
- Separate browsers
- Strong pop-up and ad blockers
- Sandboxed browsers
## Removable Media

### Characteristics
- Malware mines the registry for USB devices
- iPod aware
- Often resident only in memory
- Fast spreading
- Encryption does not help here

### Mitigation
- Make sure AV scans USB devices
- Do not use USB devices on servers
- Disable autorun!
- Know thy flash drive
Spear Phishing

Characteristics

- Directed e-mail communication
- Phone calls
- Result of a smash and grab
- Not as easy to spot
- Blackmail
- Dredging LinkedIn

Mitigation

- Education
- Communication
- Correlation
<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast evolving / fast deploy</td>
<td>Communication with IT Security Office &amp; ITADmins</td>
</tr>
<tr>
<td>Resource drain to mitigate</td>
<td>Malware analyzers</td>
</tr>
<tr>
<td>Career developers</td>
<td>Forensics</td>
</tr>
<tr>
<td>Structured change control</td>
<td></td>
</tr>
<tr>
<td>Ability to update</td>
<td></td>
</tr>
<tr>
<td>Uses encryption</td>
<td></td>
</tr>
<tr>
<td>Virus eShop</td>
<td></td>
</tr>
</tbody>
</table>
Predictions

- Financial Systems & Problems
- Botnets as political tools
- Cell phone botnets
- Infrastructure as a target - eBombs
- IPv6 as a conduit
- Insider threats (economic hardship)
- Federal regulations and mandates
- Password reset systems
Incident Response

What to do when the inevitable happens

OOPS!!
Step One:
BACK AWAY FROM THE COMPUTER!
Next steps...

- Quick assessment
- Report the problem
- Gather information & take notes
- Determine data classification
- Coordinate response and cleanup
- Forensics may be necessary
Aftermath

- Change all passwords
- Disable accounts if needed
- Review necessary software and services
- Review backups/system images
- Report findings

Format / Reimage
Questions?
THANK YOU FOR COMING

http://cio.uiowa.edu/ITSecurity
319-335-6332
security@uiowa.edu