Agenda

- Welcome
- Role of the Security Liaison
- Changes in University Security Philosophy
- University Policies: A Review
- Current Threats
- Raising Awareness: Resources
ROLE OF SECURITY LIAISONS

November 8th, 2012

Dr. Joy Hughes
Role of Security Liaison

- Communicates about desired, proposed, and approved policies:
  - ITSO to/from SL, to/from Business Unit
  - SL to/from ITSO, repeat as needed, then...
  - ITSO to the University

- Point of contact for security incidents in the Business Unit

- Advocates for training, support, tools, etc. from the ITSO

- Advocates within the Business Unit for risk assessments, remediation, and compliance
CIO’s Update

Changes in University Security Philosophy
The Old Model

- Heavy on policies
- Weak on enforcement
- Over emphasis on voluntary participation and compliance
The New Model

- Servers move to the data center
- Sys Admins who manage applications receive training/certification
- ITU uses technology tools to identify infractions and enforce security
Rationale to Change Models

- 3rd party and internal audit assessments
- Greater commitment to reliability of service, sustainability of operations, and reputation
University Policies

http://universitypolicy.gmu.edu/

- Use and Reproduction of Copyrighted Materials Policy 1104
- Data Stewardship Policy 1114
  - Authorization to Store Sensitive Data Procedures
- Removal of University Data from Electronic Media Policy 1114A
- Responsible Use of Computing Policy 1301
- Wireless Networking Policy 1302
- Public Internet Address Policy 1304
- Reporting Electronic Security Incidents and for Data Breach Notification Policy 1305
- Physical and Logical Access Security Policy 1312
- Remote Access Policy 1313
- Physical Access to Sensitive IT Facilities Policy 1314
Highlights

- Data Stewardship and Storing Highly Sensitive Data
- Responsible Use of Computing
- Public Internet Address Policy
CURRENT THREATS
OCTOBER STATISTICS
November 8th, 2012
Curtis McNay
## Phish Email & Compromised Accounts

### Phish Email – Date and Number

<table>
<thead>
<tr>
<th>Date</th>
<th># Phish</th>
<th>Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 9</td>
<td>2</td>
<td>13201</td>
</tr>
<tr>
<td>Oct 10</td>
<td>1</td>
<td>501</td>
</tr>
<tr>
<td>Oct 11</td>
<td>1</td>
<td>349</td>
</tr>
<tr>
<td>Oct 22</td>
<td>3</td>
<td>774</td>
</tr>
<tr>
<td>Oct 24</td>
<td>1</td>
<td>1581</td>
</tr>
<tr>
<td>Oct 28</td>
<td>1</td>
<td>1226</td>
</tr>
<tr>
<td>Totals</td>
<td>9</td>
<td>17632</td>
</tr>
</tbody>
</table>

### Comp. Accts. by Date and Class

<table>
<thead>
<tr>
<th>Date</th>
<th>Number</th>
<th>Students</th>
<th>Fac / Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 6</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Oct 9</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Oct 10</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Oct 12</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Oct 15</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Oct 23</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Oct 25</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Oct 26</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Oct 28</td>
<td>5</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Oct 29</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Oct 31</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>20</td>
<td>3</td>
<td>16</td>
</tr>
</tbody>
</table>
Infected Workstations – CnC Call backs

Number of Call backs to Bot Controllers

Affected Networks/Addresses
- SSID-MASON-SECURE
- SSID-Mason
- SSID-MasonResNet
- residents-NATted-129-174-190-40
- residents-NATted-129-174-190-73
- residents-NATted-129-174-176-2
- residents-NATted-129-174-188-94
- residents-NATted-129-174-180-71
- residents-NATted-129-174-178-25
- residents-NATted-129-174-178-14
- 129.174.54.180
- 129.174.180.71
- 71.187.249.66
- 74.67.92.251
- 108.240.189.176
- 129.174.19.86
- 129.174.39.64
- 129.174.45.75
- 129.174.53.213
- 129.174.68.151
- 129.174.70.70
- 129.174.70.99
Infected Workstations - Persistence of Infection

Days Infected

Affected Networks/Addresses
- SSID-MASON-SECURE
- SSID-Mason
- SSID-MasonResNet
- residents-NATted-129-174-190-40
- residents-NATted-129-174-190-73
- residents-NATted-129-174-176-2
- residents-NATted-129-174-188-94
- residents-NATted-129-174-180-71
- residents-NATted-129-174-178-25
- residents-NATted-129-174-178-14
- 129.174.54.180
- 129.174.180.71
- 71.187.249.66
- 74.67.92.251
- 108.240.189.176
- 129.174.19.86
- 129.174.39.64
- 129.174.45.75
- 129.174.53.213
- 129.174.68.151
- 129.174.70.70
- 129.174.70.99
- 129.174.70.168
Foreign Source - By Type & Geolocation

<table>
<thead>
<tr>
<th>Attack by Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspected Attacker - Allowed in Network</td>
<td>2940</td>
</tr>
<tr>
<td>Repeat Attack-Login Same Source</td>
<td>1115</td>
</tr>
<tr>
<td>Possible Outbreak-Excessive Connections</td>
<td>332</td>
</tr>
<tr>
<td>Repeat Attack-Foreign Source</td>
<td>321</td>
</tr>
<tr>
<td>Possible Malware - Multiple Alerts</td>
<td>105</td>
</tr>
<tr>
<td>Firewall Allow After Repetitive Block</td>
<td>4</td>
</tr>
<tr>
<td>Grand Total</td>
<td>4923</td>
</tr>
</tbody>
</table>
October Threat Summary

- 30,000(+/-) unique systems connected to George Mason’s Network.
- 26 - # of identified and remediated infected workstations
- 9 Phishing Email with 17632 recipients
- 20 Compromised Accounts
- 4923 Foreign Source Attack Events
RAISING AWARENESS:
REVIEW OF RESOURCES

November 8th, 2012
Sarah Morehouse
Resources Available

- **IT Security Website**
  - [http://itsecurity.gmu.edu](http://itsecurity.gmu.edu)
  - “Awareness” ➔ “Cyber Security Awareness”
    - Handouts, presentations, and online resources
  - “Security Liaisons” ➔ “For Your Review”
    - Monthly Security Newsletters, Security Liaison Toolkit information
- **Announcements**
  - *Coming Soon:* IT Security Alerts on IT Security Page
  - *Coming Soon:* Subscription to RSS Feed to Security Tip of the Day on IT Security Site
Resources Available (cont’d)

- IT Services Web Site
  - Security Alerts
  - Report malicious e-mails and other security alerts
  - First point of contact for any account issues, phishing attacks, etc.

- IT Security Alert Module – myMason
  - IT Security Tip of the Day
Raising Awareness

- Cyber Security Awareness Month 2012
  - IT Security Office hosted 4 seminars
  - All presentations and handouts available for use to help raise awareness

- Communications
  - First to hear of new communications efforts
  - Access to all available resources
  - Any ideas, comments, concerns, questions, etc., please contact Communications Coordinator
Contact

- Questions?
- Contact:
  - Sarah Morehouse, Communications Coordinator
  - ITU Security and Project Management Office
  - ex. 3-2906
  - smoreho3@gmu.edu
Questions and Wrap Up

☐ Questions?

☐ The next meeting will be Spring of 2013

☐ The IT Security Office will be in contact throughout the year

☐ Please continue to check the IT Security Office web site for the latest information