To: Information Security Committee
   Information Security Coordinators
   Information Technology Coordinating Council
   Technology Leaders
From: David Kovarik
Subject: Monthly Security Report for October, 2010
Date: November 15, 2010

During the month of October 2010, we experienced 245 Security Events including 47 Security Incidents, all of Low Severity. For October 2009, we had a total of 143 Events.

<table>
<thead>
<tr>
<th></th>
<th>Security Incidents</th>
<th>NUSA Notifications</th>
<th>Copyright Violations</th>
<th>Total Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 2010</td>
<td>47</td>
<td>157</td>
<td>41</td>
<td>245</td>
</tr>
<tr>
<td>Oct 2009</td>
<td>35</td>
<td>53</td>
<td>55</td>
<td>143</td>
</tr>
</tbody>
</table>

The October Events are separated into the following categories:

<table>
<thead>
<tr>
<th></th>
<th>NetIDs</th>
<th>IP Addresses</th>
<th>Total Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incidents</td>
<td>11</td>
<td>36</td>
<td>47</td>
</tr>
<tr>
<td>NUSA Notifications</td>
<td>0</td>
<td>157</td>
<td>157</td>
</tr>
<tr>
<td>Copyright Violations</td>
<td>33</td>
<td>8</td>
<td>41</td>
</tr>
<tr>
<td>Total Events</td>
<td>44</td>
<td>201</td>
<td>245</td>
</tr>
</tbody>
</table>

NU saw an outbreak of the Zeus bot on the Chicago campus, accounting for 28 of the 47 total security incidents. It was reported that the infected hosts had outdated versions of Adobe Reader.

Vulnerability Assessments

- Continuation of Quarterly Data Center Web Scans
- Network Scan of Audit Subnet
- Monthly network assessment for Proteomics Center of Excellence

Service Provider Security Assessments

- Symplicity Corporation
- GeneGo LLC
Table and Category Descriptions

Security Incidents
Actual compromise of a system or application; includes investigations conducted as a result of a suspected or actual incident.

Security Events
The combination of Security Incidents (as defined above) and the following:

- **Copyright violations**
  Events that are usually indicated by receipt of external notification that one of our hosts is being used to distribute copyrighted material in violation of the DMCA. Often these hosts are running various forms of Peer to Peer networking software.

- **NUSA notifications**
  Events indicated by our remote vulnerability scanning software that detected a potential security problem (vulnerability) with the host. We put this information into NUSA to notify the system administrator so that the problem may be addressed before it is exploited.

NetIDs
Events where a specific Northwestern NetID is identified and typically occurring on either the wireless or wireless networks. Events include instances where a compromise of the NetID may have occurred, usually as a result of phishing or other social engineering activities.

IP Addresses
Events where a NetID might not be able to be determined or is not directly involved, e.g., a compromised host.
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Severity</th>
<th>Action / Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2010</td>
<td>On March 3, 2010 it was reported by a department that a personal computer had been compromised. A spreadsheet containing personal health information had potentially been exposed to unauthorized access. Absent any evidence to the contrary, it was assumed the data had been exposed and notification of 221 individuals was required in accordance with NU policy and Illinois law.</td>
<td>3</td>
<td>The department identified all 221 individuals and prepared and sent notification letters. As all individuals were identified, no public announcement was required. The computer was rebuilt and restored to service.</td>
</tr>
<tr>
<td>Severity</td>
<td>Symptoms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **High** | A. Network or system outage with significant impact to user population or operation of the University  
B. High probability of propagation  
C. Probable or actual release or compromise of sensitive data (financial records, personal data, passwords)  
D. Requires immediate remedial action to prevent further compromise of data or adversity to network  
E. Notification of entities outside the University is required.  
F. Coded Red. |
| **Medium** | A. Some adverse impact to the operation of the University.  
B. Adverse effects are localized or contained, or minimal risk of propagation.  
C. No sensitive data was released or compromised.  
D. Remedial but not immediate action is required.  
E. Notification of entities within the University may be recommended.  
F. Coded Orange |
| **Low** | A. Minimal impact to small segment of user population or operation of the University.  
B. Completely localized, with few individuals affected, and presenting little or no risk to other entities.  
C. No apparent loss or compromise of data.  
D. Remedial action is required.  
E. No notification required.  
F. Coded Yellow |
<table>
<thead>
<tr>
<th>Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Scanning</td>
<td>This host was detected performing outbound scans on various TCP ports. This condition is often indicative of malware infestation and its attempt to propagate.</td>
</tr>
<tr>
<td>FTP Server</td>
<td>This host was subjected to the installation of an FTP server, typical of many types of infections. The FTP server is used to transfer files of various types and often illegal content.</td>
</tr>
<tr>
<td>BotNet Participation</td>
<td>The host has been determined to be executing comparisons of DNS requests to hosts that are known BotNet controllers. Bots are a series of remote hosts that follow the commands of the controlling host. Often these hosts are used to attack other networks.</td>
</tr>
<tr>
<td>Spam Relay, Spamming</td>
<td>This host is being used to originate various types of bulk email. Often these hosts are infected with a backdoor virus that allows spammers to use the host to send e-mail of their choice.</td>
</tr>
<tr>
<td>Notices via NUSA</td>
<td>Indicates that our remote vulnerability scanning software detected a potential security problem with the host. This information is placed into NUSA, and notification sent to the NUSA contact to address the problem before it is exploited. Notices are included in the total incident account as it is assumed an unresolved vulnerability has a high probability of compromise.</td>
</tr>
<tr>
<td>Copyright Violations, DMCA Notice</td>
<td>These are usually external notifications we receive indicating that one of our hosts is being used to distribute copyrighted material in violation of the DMCA. Often these hosts are running various forms of Peer to Peer networking software.</td>
</tr>
<tr>
<td>Phishing</td>
<td>An attempt to steal your personal information, most often through e-mail. Phishing e-mails usually appear to come from a well-known organization and ask for your personal information, e.g., credit card number, social security number, account number or password. Phishing e-mails frequently instruct you to click a link that takes you to a site where your personal information is requested, harvested and used to compromise legitimate accounts or take over identities.</td>
</tr>
</tbody>
</table>
Security Events by Calendar Year by Category

- 2005: September-December
Security Events by Calendar Year

- 2003: 3523
- 2004: 10145
- 2005: 5655
- 2006: 1932
- 2007: 2654
- 2008: 1680
- 2009: 1765
- 2010: 1765
For information on NU – BAYU “Be Aware You’re Uploading”, see [http://www.it.northwestern.edu/security/nubayu/](http://www.it.northwestern.edu/security/nubayu/)