To: Patricia Todus, Sean Reynolds  
From: David Kovarik, Roger Safian  
Subject: Monthly Security Report for May, 2011  
Date: June 06, 2011

During the month of May 2011, we experienced 136 Security Events including 23 Security Incidents, all of Low Severity. For May 2010, we had a total of 182 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>May 2011</td>
<td>23</td>
<td>82</td>
<td>31</td>
<td>136</td>
</tr>
<tr>
<td>May 2010</td>
<td>59</td>
<td>87</td>
<td>36</td>
<td>182</td>
</tr>
</tbody>
</table>

The May 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>7</td>
<td>16</td>
<td>23</td>
</tr>
<tr>
<td>NUSA Notifications</td>
<td>0</td>
<td>82</td>
<td>82</td>
</tr>
<tr>
<td>Copyright Violations</td>
<td>27</td>
<td>4</td>
<td>31</td>
</tr>
<tr>
<td>Total Events</td>
<td>34</td>
<td>102</td>
<td>136</td>
</tr>
</tbody>
</table>

Botnets and Malware

- We saw instances of what appears to be Artro, Downadup and Spyeye malware, one rogue DNS, and several instances of participation in botnets.

Phishing

- Several successful instances of Phishing were realized.

Communications

- Weekly podcasts: 5/5, 5/12, 5/18 and 5/26  
  [http://www.it.northwestern.edu/security/podcast.html](http://www.it.northwestern.edu/security/podcast.html)
- eCommunicator: “I’m Wishing We Could Stop the Phishing”  

Staffing

- Search for a candidate to fill the Data Security Analyst position continues.
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.
# Summary Descriptions of Security Incidents

**Severity 1 and 2, May 2010 – May 2011**

**Severity 3 / May 2011**

<table>
<thead>
<tr>
<th>Description</th>
<th>Severity</th>
<th>Action / Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>None reported</td>
<td><strong>1</strong></td>
<td>No action required</td>
</tr>
<tr>
<td>None reported</td>
<td><strong>2</strong></td>
<td>No action required</td>
</tr>
<tr>
<td>Botnet Participation / IRC Bot</td>
<td><strong>3</strong></td>
<td>Workstation/server rebuild, malware removal</td>
</tr>
<tr>
<td>FTP Server</td>
<td><strong>3</strong></td>
<td>Workstation/server rebuild, malware removal</td>
</tr>
<tr>
<td>Malware Infection</td>
<td><strong>3</strong></td>
<td>Workstation/server rebuild, malware removal</td>
</tr>
<tr>
<td>Outbound Scanning</td>
<td><strong>3</strong></td>
<td>Workstation/server rebuild, malware removal</td>
</tr>
<tr>
<td>Phishing</td>
<td><strong>3</strong></td>
<td>User educated/password changed</td>
</tr>
<tr>
<td>Spam Relay, Spamming</td>
<td><strong>3</strong></td>
<td>Workstation/server rebuild, malware removal</td>
</tr>
<tr>
<td>Rogue DNS</td>
<td><strong>3</strong></td>
<td>Workstation/server rebuild, malware removal</td>
</tr>
</tbody>
</table>

Classified: INTERNAL
Legend

Security Incidents: Severity 1, 2 and 3

<table>
<thead>
<tr>
<th>Severity</th>
<th>Symptoms</th>
</tr>
</thead>
</table>
| 1 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. |
| 2 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 |
| 3 Low    | A. Adverse 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><strong>Legend</strong></th>
<th><strong>Security Incidents: Severity 3 (Low)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td><strong>Explanation</strong></td>
</tr>
<tr>
<td>BotNet Participation, IRC Bot</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>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>Malware Infection</td>
<td>Malicious software designed to alter the operation of a computer, usually to the user’s disadvantage. It is usually transmitted and installed without the user’s knowledge or consent. It comes in a number of forms, the best-known and longest standing being “Trojan”, “Virus” or “Worm” programs.</td>
</tr>
<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>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>
<tr>
<td>Rogue DNS</td>
<td>A rogue DNS (Domain Name System) server is used to redirect the resolution of DNS names to other, sometimes illegitimate, destinations. This is often done for malicious purposes such as phishing.</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>
</tbody>
</table>
Security Events by Month by Category

2010 - 2011

- NUSA Notifications
- Copyright Violations
- Incidents
Security Events by Calendar Year by Category

- **2005**: September-December

- NUSA Notifications
- Copyright Violations
- Incidents

---

- Total NUSA Notifications for 2005: 3,888
- Total Copyright Violations for 2005: 118
- Total Incidents for 2005: 123

- Total NUSA Notifications for 2006: 673
- Total Copyright Violations for 2006: 1,136
- Total Incidents for 2006: 1,236

- Total NUSA Notifications for 2007: 2,127
- Total Copyright Violations for 2007: 2,127
- Total Incidents for 2007: 2,127

- Total NUSA Notifications for 2008: 2,826
- Total Copyright Violations for 2008: 2,826
- Total Incidents for 2008: 2,826

- Total NUSA Notifications for 2009: 3,482
- Total Copyright Violations for 2009: 3,482
- Total Incidents for 2009: 3,482

- Total NUSA Notifications for 2010: 4,552
- Total Copyright Violations for 2010: 4,252
- Total Incidents for 2010: 4,252

- Total NUSA Notifications for 2011: 1,181
- Total Copyright Violations for 2011: 1,631
- Total Incidents for 2011: 416
Security Events by Calendar Year

- 2003: Aug-Dec

2003: 3523
2004: 10145
2005: 5655
2006: 1932
2007: 2654
2008: 1680
2009: 1765
2010: 2061
2011: 728
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/)