To: Information Security Advisory Committee  
Information Security Coordinators  
Information Technology Coordinating Council  
Technology Leaders  

From: David Kovarik  

Subject: Monthly Security Report for November 2009  

Date: December 09, 2009  

During the month of November 2009, we experienced 135 Security Events, including 17 Security Incidents, all of Low Severity. For November 2008, we had a total of 120 Events.

<table>
<thead>
<tr>
<th></th>
<th>Security Incidents</th>
<th>NUSA Notifications</th>
<th>Copyright Violations</th>
<th>Total Security Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2009</td>
<td>17</td>
<td>65</td>
<td>53</td>
<td>135</td>
</tr>
<tr>
<td>November 2008</td>
<td>18</td>
<td>89</td>
<td>13</td>
<td>120</td>
</tr>
</tbody>
</table>

We are experiencing a higher number of DMCA complaints (Copyright Violations) this past three months (Sep/40, Oct/55, Nov/53) when compared to a similar period (Sep/22, Oct/28, Nov/13) one year ago. What is contributing to the increase is unclear but we will continue to monitor conditions.

The November Events are separated into the following categories:

<table>
<thead>
<tr>
<th>Administrative Network</th>
<th>Dormitory Network</th>
<th>Remote Access &amp; NetIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>o Suspected malware</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>o Suspicious services</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>o Notices via NUSA</td>
<td>65</td>
<td>0</td>
</tr>
<tr>
<td>o Copyright violations</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>o Other incidents</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Total 85                      Total 3                      Total 47

Total All Incidents: 135

Disaster Recovery  
- Student Enterprise System exercise completed

Vulnerability Assessments  
- Scan of server that was infected and subsequently patched.  
- 4th quarter data center scans currently in progress.

Service Provider Security Assessment  
- Webpage published; public announcement being prepared.
Policy
- Server Certificate Policy approved, awaiting publication.
- Firewall Policy under review by University Compliance Committee.

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.

Suspected malware
An incident indicating that the host was detected doing outbound scans on various TCP ports. This is often how malware spreads.

Suspicious service
An incident indicating that the host has a service that is being used, in violation of university policies. These services include a FTP server for file transfers and spam relays that allow the host to be used to send bulk commercial email, installed on it. These hosts can also have bots installed on them. Bots are a series of remote hosts that will follow the commands of the controlling host. Often these are used to attack other networks. Typically these actions are done as part of an infection and is used to share various, often illegal content.

Other incidents
Includes incident-related activities, e.g., research conducted at request of Human Resources or University Police. Also includes reported phishing activities that require some action and response by ISS/C and/or NUIT personnel.

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.
**Summary Report of Security Incidents**  
**Severity 2 and 3, November 2008 – November 2009**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Severity</th>
<th>Action / Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-09</td>
<td>On June 15 and 22, ISS/C discovered two staff members who appeared to have been victims of a successful phishing attack. The compromised accounts were used to generate large amounts of spam, resulting in the temporary blacklisting of NU mail servers by several ISPs.</td>
<td>3</td>
<td>The users appeared to have responded to phishing e-mail with personal information. Users were instructed to change account passwords and monitor the accounts for unusual behavior.</td>
</tr>
<tr>
<td>Feb-09</td>
<td>On February 13, notification was received of possible compromise of two NU accounts assigned to a student and visiting scholar. The NetIDs were suspended and users contacted.</td>
<td>3</td>
<td>The users appeared to have responded to phishing e-mail with personal information. Users were instructed to change account passwords and monitor the accounts for unusual behavior.</td>
</tr>
<tr>
<td>Jan-09</td>
<td>A computer that was used to process reports for a research project was compromised. The exact date of the compromise is unknown. The compromise happened at least as far back as November 2008. The machine had been moved to the department in 2007. It was not being properly maintained and was discovered to have more than 50 different viruses and adware. The computer contained a file that contained research data on approximately 1700 individuals.</td>
<td>3</td>
<td>The department mailed notices to the individuals contained in the file, in early February, and the computer was secured and returned to service. Additional measures and technical support were recommended to help minimize risk of future occurrence.</td>
</tr>
<tr>
<td>Apr-09</td>
<td>Several hosts on the Northwestern network were found to be using a Ukrainian Domain Name Server (DNS) instead of the Northwestern DNS. ISS/C’s investigation discovered approximately 70 hosts with Microsoft Windows or Apple OS-X infected with malware.</td>
<td>2</td>
<td>NU-IT instituted a block of DNS (port 53) traffic to the Ukrainian network. The malware could not be removed by the then available anti-viral solutions, so a rebuild of infected machines was recommended.</td>
</tr>
<tr>
<td>Security Incidents: Severity 1, 2 and 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td><strong>Symptoms</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **3**<br>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**<br>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 |
| **1**<br>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><strong>Legend</strong></th>
<th><strong>Security Incidents: Severity 1 (Low)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td><strong>Explanation</strong></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>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</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</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>
</tbody>
</table>
Security Events by Month (by Category)

Nov  Dec  Jan  Feb  Mar  Apr  May  Jun  Jul  Aug  Sep  Oct  Nov
2008 - 2009

NUSA Notifications  Copyright Violations  Incidents
Security Events by Year (by Category)

- **2005**: September-December

- **2005**: 388 NUSA Notifications, 118 Copyright Violations, 938 Incidents
- **2006**: 673 NUSA Notifications, 123 Copyright Violations, 1136 Incidents
- **2007**: 2127 NUSA Notifications, 223 Copyright Violations, 304 Incidents
- **2008**: 282 NUSA Notifications, 445 Copyright Violations, 953 Incidents
- **2009**: 300 NUSA Notifications, 344 Copyright Violations, 964 Incidents
Security Events by Calendar Year

- 2003: 3523
- 2004: 10145
- 2005: 5655
- 2006: 1932
- 2007: 2654
- 2008: 1680
- 2009: 1608
For information on NU – BAYU “Be Aware You’re Uploading”, see http://www.it.northwestern.edu/security/nubayu/