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

From: David Kovarik  

Subject: Monthly Security Report for March 2010  
Date: April 09, 2010  

During the month of March 2010, we experienced 206 Security Events, including 30 Security Incidents of Low Severity and 1 of High Severity. For March 2009, we had a total of 139 Events.

<table>
<thead>
<tr>
<th></th>
<th>March 2010</th>
<th>NUSA Notifications</th>
<th>Copyright Violations</th>
<th>Total Security Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incidents</td>
<td>81</td>
<td>91</td>
<td>34</td>
<td>206</td>
</tr>
<tr>
<td>March 2009</td>
<td>25</td>
<td>86</td>
<td>28</td>
<td>139</td>
</tr>
</tbody>
</table>

A department suffered a compromise where a computer was taken over that contained a spreadsheet with personally identifiable information of 221 individuals. In accordance with University policy and Illinois regulations, the 221 individuals were notified by mail of the potential exposure of personal information.

Torpig/Mebroot/Marisposa malware continued to spread in the first half of the month, causing a rise in the number of Incidents. NUIT issued an advisory e-mail to the University community, warning of the malware and steps to help prevent against infection. Shortly after distribution, the number of new infections quickly dropped off.

The March Events are separated into the following categories:

- **Administrative Network**
  - Suspected malware: 12
  - Suspicious services: 18
  - Notices via NUSA: 91
  - Copyright violations: 6
  - Other incidents: 2

- **Dormitory Network**
  - Suspected malware: 0
  - Suspicious services: 0
  - Notices via NUSA: 0
  - Copyright violations: 1
  - Other incidents: 1

- **Remote Access & NetIDs**
  - Suspected malware: 9
  - Suspicious services: 33
  - Notices via NUSA: 0
  - Copyright violations: 27
  - Other incidents: 6

Total: 129

Total All Incidents: 206

Vulnerability Assessments
- Assessment of Academic and Research Technology
- Quarterly Data Center assessment
Policy
- Appropriate Use of Electronic Resources Policy published but under review by Policy Review 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, March 2009 – March 2010

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Severity</th>
<th>Action / Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar-10</td>
<td>On March 3, it was reported that a department suffered a compromise of a personal computer. 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>2</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>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>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>
</tbody>
</table>

Classified: INTERNAL
### Legend

**Security Incidents: Severity 1, 2 and 3**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Symptoms</th>
</tr>
</thead>
</table>
| **3 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 |
| **1 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>
<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 Month (by Category)

<table>
<thead>
<tr>
<th>Month</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar</td>
<td>25</td>
<td>86</td>
</tr>
<tr>
<td>Apr</td>
<td>28</td>
<td>110</td>
</tr>
<tr>
<td>May</td>
<td>29</td>
<td>122</td>
</tr>
<tr>
<td>Jun</td>
<td>20</td>
<td>107</td>
</tr>
<tr>
<td>Jul</td>
<td>19</td>
<td>75</td>
</tr>
<tr>
<td>Aug</td>
<td>23</td>
<td>34</td>
</tr>
<tr>
<td>Sep</td>
<td>23</td>
<td>18</td>
</tr>
<tr>
<td>Oct</td>
<td>58</td>
<td>31</td>
</tr>
<tr>
<td>Nov</td>
<td>31</td>
<td>35</td>
</tr>
<tr>
<td>Dec</td>
<td>23</td>
<td>35</td>
</tr>
<tr>
<td>Jan</td>
<td>53</td>
<td>55</td>
</tr>
<tr>
<td>Feb</td>
<td>17</td>
<td>48</td>
</tr>
<tr>
<td>Mar</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>April</td>
<td>30</td>
<td>81</td>
</tr>
</tbody>
</table>

NUSA Notifications | Copyright Violations | Incidents

2009 - 2010
Security Events by Year (by Category)

- 2005: September-December

- 2005: NUSA Notifications 388, Copyright Violations 118, Incidents 123
- 2006: NUSA Notifications 673, Copyright Violations 123, Incidents 938
- 2007: NUSA Notifications 2127, Copyright Violations 223, Incidents 673
- 2008: NUSA Notifications 282, Copyright Violations 445, Incidents 953
- 2009: NUSA Notifications 348, Copyright Violations 376, Incidents 1041
- 2010: NUSA Notifications 152, Copyright Violations 126, Incidents 278
Security Events by Calendar Year

- 2003: 3523
- 2004: 5655
- 2005: 10145
- 2006: 2654
- 2007: 1932
- 2008: 1680
- 2009: 1765
- 2010: 556
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/)