Countering Security Risks at ccTLD Level and SSR

Jay Rajasekera
International University of Japan
Minamiuonuma City, JAPAN 949-7277
jrr@uij.ac.jp

&

Suvashis Das
Nagaoka University of Technology
Nagaoka, JAPAN 940-2188
Acknowledgement:

We would like to thank Professor Yoshiki Mikami, Professor Ashu Marasinghe, and Dr. Shigeaki Kodama of Nagaoka University of Technology, Niigata, Japan and Japan Science and Technology Agency (JST) for their support for conducting this research.
Critical Factors for ccTLD Security

• How well informed about threats, the end users under a ccTLD are?
• What kind of technologies are being used by the ccTLD?
• How often maintenance and reassessment of current defense policies are done and so on...

Ref:
OECD-2009
Asia Pacific Top Level Domain Association
ICANN
ccNSO
SSR Strategic Plan for ccTLD

• Ref: ICANN-2009

• “Plan for Enhanced Internet Security, Stability and Resiliency”

• The basic role for ccTLDs is to work closely with ICANN to foster enhanced Security, Stability and Resiliency (SSR)
TLD Security, Stability & Resiliency Collaboration

Objectives
- Mature Attack & Contingency Response Program
- Establish joint ISOC/ICANN tech training program
- Establish TLD exercise planning workshops
- Establish program metrics

Deliverables (milestones)
- Conduct ACRP training sessions (5 in 2009); automate planning tool by Aug 09
- Joint technical training with ISOC plan (approve summer 09); first full program conducted fall 2009; two more by 2009
- Conduct exercise planning workshops (initial implementation Oct 2009)
- Prototype metrics based on Resiliency Engineering Framework (fall 2009)

Key Stakeholders
- ccTLD operators
- ccNSO, regional TLD operators
- ISOC/NSRC
- ICANN staff

Resources (FY 10)
Human – 1 FTE
Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs

Ref: ICANN: PLAN FOR ENHANCING INTERNET SECURITY, STABILITY, AND RESILIENCY Approved Draft – 16 May 2009
Ref: Survey among members of the ccNSO Committee

SSR is the most important
Our Mission

Our research aims to find measures at ccTLD level that would eventually lead to an Internet with enhanced Security, Stability and Resiliency (SSR)

• Survey conducted at IGF 2009
• Ongoing survey involving ccTLD administrators
• Security Alert Maps
Survey Results (As of Now)

We sent around 150 questionnaires in seminars in different conference rooms related to ccTLD practices.

Out of them 25 of the questionnaires were returned to us bearing meaningful results. We summarize it here
Question 1: Is regular monitoring and assessment done on risks within the trusted environment

![Bar chart showing frequency of monitoring and assessment]

- **Always**: 2
- **Frequently**: 14
- **Less Frequently**: 2
- **Not at all**: 0
- **No Answer**: 6

Is regular monitoring and assessment done on risks within the trusted environment.
Question 2: What were the most common threats in your ccTLD in the recent past
Question 3: How Frequently are virus and malware database updated

How Frequently are virus and malware database updated

0
2
4
6
8
10
12
14
16
18

Hourly
Daily
Monthly
Yearly
Realtime
others
no answer
Question 4: How effective is the phishing filter in your TLD tree (meaning TLD and its sub domain)
Question 5: How effective is the SPAM guard in the TLD tree (meaning TLD and its sub domains)?

![Bar chart showing the effectiveness of the SPAM guard in the TLD tree.]

- **Very Effective**: 0 responses
- **Moderately Effective**: 2 responses
- **Not Effective at all**: 6 responses
- **Does not Exist**: 12 responses
- **No answer**: 14 responses
Question 6: How does your ccTLD handle malicious redirection

- Reduce Browser hijack
- Adware, Spyware, Vir...
- Reduce Phishing, SPAM
- All
- NONE
- Others
- No Answer
Question 7: Are the websites under the ccTLD checked for compliance with secure coding practices

![Bar chart showing the distribution of responses to the question. The chart indicates that most respondents answered with options like "Yes, While Launched" and "Both," while others chose "No Checking" or did not answer. The y-axis represents the number of responses, ranging from 0 to 14.]
Question 8: What are the policies for taking down a sub-domain found to be spreading malware

- Effectively Implemented: 16
- Seldom Implemented: 0
- No policies: 4
- No answer: 0
Question 9: How effective is the ccTLD's defense system against emerging threats
Question 10: How often is the list of malicious domains in the black-list updated

- Hourly
- Daily
- Monthly
- Realtime
- None or no black-list
- No answer
Question 11: Is regular monitoring and assessment done on risks within the trusted environment

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always</td>
<td>1</td>
</tr>
<tr>
<td>Frequently</td>
<td>14</td>
</tr>
<tr>
<td>Less Frequently</td>
<td>2</td>
</tr>
<tr>
<td>Not at all</td>
<td>0</td>
</tr>
<tr>
<td>No Answer</td>
<td>6</td>
</tr>
</tbody>
</table>
Survey Analysis vs Security Alert Rankings

Here we try to comprehend the survey results by objectively looking at the Phishing and Spam alert analysis we have done earlier [Presented at GIGANET Symposium held along with IGF09 in Egypt]
A snapshot of our Data Set after sorting and country-wise organizing

<table>
<thead>
<tr>
<th>Countries</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Brazil</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>7</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>South Korea</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>11</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Poland</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Turkey</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>11</td>
<td>7</td>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>India</td>
<td>12</td>
<td>7</td>
<td>7</td>
<td>11</td>
<td>11</td>
<td>12</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>China</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Argentina</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Russia</td>
<td>13</td>
<td>11</td>
<td>11</td>
<td>12</td>
<td>12</td>
<td>13</td>
<td>13</td>
<td>8</td>
<td>11</td>
<td>8</td>
</tr>
<tr>
<td>Vietnam</td>
<td>14</td>
<td>12</td>
<td>12</td>
<td>13</td>
<td>13</td>
<td>14</td>
<td>14</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Columbia</td>
<td>7</td>
<td>9</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Romania</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Germany</td>
<td>9</td>
<td>13</td>
<td>13</td>
<td>10</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>UK</td>
<td>10</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>10</td>
<td>10</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
</tbody>
</table>
A Phishing Trend Line

- Ranking trend graph for 5 selected countries. We can clearly observe that the plot is rising as time progresses. This means the countries with high rankings in the past are moving towards lower ranks meaning they are successfully reducing phishing levels in their country.

Contrast this finding with Question 4 of the survey on “Phishing”
• From the graph it is evident that historical ranking has negligible impact on the future rankings and with time the countries move to higher ranks irrespective of the historical rankings.

• As we said in the introductory slides defining SPAM it is at the hands of the end user and email service providers to tackle this problem adequately.

Contrast this finding with Question 5 of the survey on “SPAM”
Ongoing Survey

World Internet ccTLD Dynamic Risk Alert Maps
(WIDRA Maps)

ccTLD Security Alerts Questionnaire

We are a group of research students at International University of Japan and Nagaoka University of Technology, Japan. We would appreciate it very much if you kindly fill up this survey and give back to us. Our project is completely an educational research project and has no commercial interests. Thank you very much for your time and participation.

In case of multiple answers, please mark them all accordingly.

* Required

http://elab-ws.iuj.ac.jp/cctld/ccTLDSurvey.htm
Relevance to SSR

- Reduce Risk
- Improve Knowledge
- Exploit Opportunities

ccTLD
- Constant monitoring
- Alerts
- Mapping

- Opinion Survey and analysis
- Recommendation of Enhanced SSR policies
Conclusion

IGF Survey:

• Very few people are aware about ccTLD operations and practices as the No answer field is in all answers
• Real-time updates regarding security needs to be more in practice
• Policies are there but the implementation is seldom done and thus the malicious domains are still free to abuse internet security.
• Survey results on Phishing and Spam, seem to be in agreement with the Security Alert Ranking Analysis [Presented at GIGANET Symposium held along with IGF09 in Egypt]
• Security Alerts needs to be looked carefully in three spheres: metrics, policies and implementation in SSR framework
Thank You Very Much