Responsible Vulnerability Disclosure

A State’s Perspective

Marc Henauer
January 20, 2020
The State’s Responsibility in the Security Domain
The State’s Role in Cyber Security

• It can draft up and enact Law, such as:
  • Mandatory Reporting of Vulnerabilities
  • Enforcing the Application of Security Measures

• It can support Initiatives, such as:
  • Bug Bounty Programs (i.e. eVoting-Systems)
  • (Sectorial) Information Sharing

• It can be a key player in RVD, such as:
  • National Contact and Information Point
  • International Coordination
The State’s Role in National Security

• It must ensure working and efficient Law Enforcement and Security Services, hence:
  • It must provide for the legal framework to access communication systems.
  • It must enable Law Enforcement and Services to keep up with the technological development.

• It must also ensure readiness in regard to its Defense, hence:
  • It must provide for the development of offensive capabilities.
  • It must provide for a clear doctrine on how such capabilities are to be used.
The Swiss Approach

Vulnerability “Harvesting” is neither financially, nor practically feasible.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.500</td>
<td>November 3, 2005</td>
<td>C&amp;C server registration</td>
</tr>
<tr>
<td>0.500</td>
<td>November 15, 2007</td>
<td>Submit date to a public scanning service</td>
</tr>
<tr>
<td>0.500</td>
<td>July 4, 2009</td>
<td>Infection stop date</td>
</tr>
<tr>
<td>1.001</td>
<td>June 22, 2009</td>
<td>Main binary compile timestamp</td>
</tr>
<tr>
<td>1.100</td>
<td>March 1, 2010</td>
<td>Main binary compile timestamp</td>
</tr>
<tr>
<td>1.101</td>
<td>April 14, 2010</td>
<td>Main binary compile timestamp</td>
</tr>
<tr>
<td>1.x</td>
<td>June 24, 2012</td>
<td>Infection stop date</td>
</tr>
</tbody>
</table>

Securing the Nation’s Industry and CNI always enjoys Priority
Some Thoughts To Ponder

• States have a key role to play in setting up a functioning and efficient Responsible Vulnerability Disclosure by engaging the relevant stakeholders.

• States must set up a transparent, clear and concise process in order to balance the need for RVD and lawful interception.

• Any effort should be guided by existing international frameworks, norms and principles.