10 years of experience in incident response in Russian Federation
About

- 1998. Start as RIPN (Russian Institute of Public Networks) project 1998 as CSIRT of RBNET (NREN)

- FIRST, TI member

- 2011. RU-CERT - non-commercial organization that plays a role of a national level CSIRT team of Russian Federation

- Hours of work - 10:00-18:00 every day, except weekends and national holidays

- Responsibility domain – whole Russian address space

- Funding model - sponsorship
OPERATIONAL DETAILS

Environment - reality

• No authority over ISPs, domain registrars, etc.
• No IP resources under control

Mode of operation

1. Gathering (getting) all the information about malicious Russian resources and network activity related to Russian address space
2. Information analysis and verification
3. Attempting to solve the problem
Mode of operation (continued)

RU-CERT
Operational DB

Analysis / Verification

E-Mails
Phone calls
Feeds

Resource owner contact
Authority contact
Another operational mode

• Dispatching urgent requests to Russian LEA

Requests direction

1. Foreign countries -> Russia  95%
2. Russia  -> Foreign countries 1%
3. Russia  -> Russia                  4%
INPUT details
Incidents processed

All kinds of «typical» incidents, except SPAM cases
Feed sources

• Arbor Networks
• Shadowserver
• Abuse.ch bundle
• MalwareDomainList
• CleanMX
• Phishtank
• Malc0de
• Team Cymru
• Some other’s (3-4, incl. temporary)
# Feed data volume (average/ per day)

<table>
<thead>
<tr>
<th>Type</th>
<th>New</th>
<th>Unique</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>62</td>
<td>176</td>
<td>199</td>
</tr>
<tr>
<td>MW</td>
<td>250</td>
<td>508</td>
<td>523</td>
</tr>
<tr>
<td>C&amp;C</td>
<td>4</td>
<td>31</td>
<td>32</td>
</tr>
</tbody>
</table>
# Top list of e-mails input (5 months)

<table>
<thead>
<tr>
<th>Email Address</th>
<th>MW</th>
<th>Phishing</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mycert@mycert.org.my">mycert@mycert.org.my</a></td>
<td>126</td>
<td></td>
<td>105</td>
</tr>
<tr>
<td><a href="mailto:auscert@auscert.org.au">auscert@auscert.org.au</a></td>
<td>219</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:ftsteam@paypal.com">ftsteam@paypal.com</a></td>
<td>14</td>
<td>189</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:cert@cert.br">cert@cert.br</a></td>
<td>100</td>
<td></td>
<td>68</td>
</tr>
<tr>
<td><a href="mailto:csirt@bradesco.com.br">csirt@bradesco.com.br</a></td>
<td>70</td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>@markmonitor.com</td>
<td>76</td>
<td></td>
<td>19</td>
</tr>
<tr>
<td>@brandprotect.com</td>
<td>32</td>
<td></td>
<td>83</td>
</tr>
<tr>
<td>@markmonitor.com</td>
<td>95</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# CC/TO balance statistic

<table>
<thead>
<tr>
<th></th>
<th>RU-CERT in TO field</th>
<th>RU-CERT in CC field</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:mycert@mycert.org.my">mycert@mycert.org.my</a></td>
<td>110</td>
<td>121</td>
</tr>
<tr>
<td><a href="mailto:auscert@auscert.org.au">auscert@auscert.org.au</a></td>
<td>17</td>
<td>208</td>
</tr>
<tr>
<td><a href="mailto:ftsteam@paypal.com">ftsteam@paypal.com</a></td>
<td>4</td>
<td>198</td>
</tr>
<tr>
<td><a href="mailto:cert@cert.br">cert@cert.br</a></td>
<td>168</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:csirt@bradesco.com.br">csirt@bradesco.com.br</a></td>
<td>104</td>
<td>24</td>
</tr>
<tr>
<td>@markmonitor.com</td>
<td>67</td>
<td>14</td>
</tr>
<tr>
<td>@brandprotect.com</td>
<td>92</td>
<td>23</td>
</tr>
<tr>
<td><a href="mailto:cais@cais.rnp.br">cais@cais.rnp.br</a></td>
<td></td>
<td>65</td>
</tr>
<tr>
<td><a href="mailto:afcc@rsa.com">afcc@rsa.com</a></td>
<td>57</td>
<td></td>
</tr>
</tbody>
</table>
Information processing

Security event – any information related to computer security case

Incident – SE, that RU-CERT reacts to in some way
Will **SE** be transformed into **Incident** or not significantly depends on results of verification:

**Phishing**

- 95-98% of all requests are really phishing resources
- ~80% of phishing resources are located on compromised servers
- Second level domains used for phishing sites – lately occurs very seldom
- Most cases - non-Russian banks and payment systems

**Malware** 70-75% can be verified (MHR, etc)

**Attacks** Unverified

**C&C** 10-15% can be verified
Contact details

1. Resource owners – more than 600 contacts in RU-CERT database
2. LEA’s – 3-4 cases/per month
3. CCTLD (Coordination Center of Russian TLD zone) (domains in .ru/.рф zones)
Incident processing software

Type: malware
Created: 2011-04-29 11:57:03
Changed: 2011-05-04 18:40:01
Status: measures taken
Flags: Auto-processed, Postprocessing required

Comments:

Contacts:
- abuse@redcom.ru

Sources:
- 212.19.3.130 (AS8749, RU)

History:
- 2011-04-29 11:58:09: Outgoing incident mail #2108011860
- 2011-04-29 11:57:03: Incident #2108011860 created by lich
INCIDENT PROCESSING STATS
Summary (mw/phishing) 2010
## Destination geographic distribution

<table>
<thead>
<tr>
<th>City</th>
<th>MW</th>
<th>Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moscow</td>
<td>3054 (47.07%)</td>
<td>191 (12%)</td>
</tr>
<tr>
<td>St. Petersburg</td>
<td>609 (9.38%)</td>
<td>22 (1.4%)</td>
</tr>
</tbody>
</table>
Difficulties (technical)

- Incorrect information in RIPE database
- Small net objects often not listed in database
- AS’s ownership often can’t be discovered without ISP support (VPN)
Effectiveness

Not easy to estimate – but performance index is positive because of:

• We have a lot of established contacts with ISPs/domain registrars
• Better chance to find out correct contacts (5-6 calls chain is normal)
• Requests coming from a Russian organization are usually treated in a more friendly manner
Questions

ganev@cert.ru, info@cert.ru
http://www.cert.ru/

12-17 June 2011 Vienna