Request Tracker for Incident Response (RTIR)

Andy Bone

JANET-CERT Manager
Presentation
Overview

• Brief history
• Time Line to JANET-CERT Implementation
• Training
• W G Findings
Changes from original RT

- IRT specific workflows
- ‘clicky’ metadata extraction and tracking
- whois integration
- separate “threads” for each conversation
- high-level overviews
- convenient searching
- simple scriptable actions
- new reporting functionality
RTIR Information

**Structures**

**Incident Reports**
- Someone has a problem of some kind

**Investigations**
- IRT attempts to get to the root of the problem

**Blocks**
- Track network level intervention against threat

**Incidents**
- Ties it all together. May have many related incident reports, investigations and blocks
### 10 new unlinked Incident Reports...

<table>
<thead>
<tr>
<th>#</th>
<th>Subject</th>
<th>State</th>
<th>Owner</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Denial of Service from 10.0.0.1</td>
<td>new</td>
<td>Nobody</td>
<td>in 22 min</td>
</tr>
<tr>
<td>10</td>
<td>MAKE MONEY FAST ($$$$$)</td>
<td>new</td>
<td>Nobody</td>
<td>in 22 min</td>
</tr>
<tr>
<td>11</td>
<td>Port scan from 192.168.6.5</td>
<td>new</td>
<td>Nobody</td>
<td>in 24 min</td>
</tr>
</tbody>
</table>

### 2 of 2 most due incidents owned by johng (and unowned)...

<table>
<thead>
<tr>
<th>#</th>
<th>Subject</th>
<th>Owner</th>
<th>State</th>
<th>Priority</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>An OpenRelay on 192.168.1.1</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>8 min ago</td>
</tr>
<tr>
<td>13</td>
<td>Copyright material on 192.168.9.9</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>in 26 min</td>
</tr>
</tbody>
</table>

### 3 of 3 most due incidents...

<table>
<thead>
<tr>
<th>#</th>
<th>Subject</th>
<th>Owner</th>
<th>State</th>
<th>Priority</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>An OpenRelay on 192.168.1.1</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>5 min ago</td>
</tr>
<tr>
<td>16</td>
<td>Scan from 192.168.55.24</td>
<td>rt</td>
<td>open</td>
<td>50</td>
<td>in 6 days</td>
</tr>
<tr>
<td>13</td>
<td>Copyright material on 192.168.9.9</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>in 26 min</td>
</tr>
<tr>
<td>Incident 18: An OpenRelay on 192.168.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Owner: john</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State: open</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject: An OpenRelay on 192.168.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description: (no value)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority: 50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Worked: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Constituency: JANET-CERT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function: AbuseDesk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification: Spam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 5 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>19: An OpenRelay on 192.168.1.1 (open)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 6 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created: Fri Jun 20 11:23:40 2003</td>
</tr>
<tr>
<td>Due: Not set</td>
</tr>
<tr>
<td>Updated: Fri Jun 20 11:28:07 2003 by john</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Jun 20 11:23:40 2003</td>
</tr>
<tr>
<td>john - Ticket created</td>
</tr>
<tr>
<td>Subject: An OpenRelay on 192.168.1.1</td>
</tr>
<tr>
<td>Hello</td>
</tr>
<tr>
<td>One of your users has an open relay on machine 192.168.1.1</td>
</tr>
<tr>
<td>Please let me know once this matter has been resolved.</td>
</tr>
<tr>
<td>Regards</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Fri Jun 20 11:23:40 2003</td>
</tr>
<tr>
<td>RT_System - Starts changed from Not set to Fri Jun 20 11:23:40 2003</td>
</tr>
</tbody>
</table>
Where we are now

- Version 1.0 released end of August
- In use by a number of teams throughout the world
- Tested and evaluated.
- Only free package (as far as we know) specifically designed for IRT use.
JANET-CERT
Timeline to Implementation

- Late 2002 began requirements document with BestPractical.
- Early 2003 BestPractical began coding
- Mid 2003 final code handover.
- Internal systems changeover was still progressing.
- November new systems in place and operational.
- Dec 1st (Monday morning) mail began entering RTIR system, legacy incidents continued to be handled by old IMAP based system
- End of December Only 2 legacy incidents remaining. 9,480 incident
- Reports, 9,096 of misdirected spam. Launched 101 investigations.
- Immediate issues.
Immediate Issues

- Some speed problems, work progressing on optimisation.
- Need a spam remedy to prevent it entering RT. Careful evaluation of Spamassassin ongoing
- Minor bugs
- Integration with our probe/scan system ongoing.
Finding out more

rtir-request@lists.bestpractical.com

- Closed list for incident response team staff

http://www.training@bestpractical.com

http://www.bestpractical.com

http://www.bestpractical.com/rtir/
RTIR Working Group
The training course for RT development was delivered yesterday by BestPractical, it was attended by 15 students and included the following subject areas:

- RT's system architecture
- A guided tour of the RT source code
- Extension mechanisms you can use to customize RT
- How to tie RT into your existing authentication infrastructure
- Building your own tools that talk to the RT backend
- Automating common procedures
- Customizing RT's workflow to match your own
- How to write custom reports based on RT's data

Possibility of another if enough interest could be generated
Teams Involved:

- UNIRAS (UK)
- LITNET-CERT (Lit)
- SUNET-CERT (SU)
- DFN-CERT (DE)
- ACONET-CERT (AC)
- IRIS-CERT (SP)

- JANET-CERT (UK)
- CERT-POLSKA (PL)
- GOVCERT.NL (NL)
- SWITCH-CERT (CH)
- CERTA (FR)
- CERNET (CRO)
RTIR
WG

Agenda:

1. Welcome: (each team provided the following information)
   - Their current RTIR Status
   - Their expectations (Where they want RTIR to go)
2. Support
   - Bug Fixes
   - Major Work fixes
3. New areas of development
4. Funding
5. Organisation of work group actions
6. AOB
7. Next Meeting
Teams are at various stages of RTIR implementation: from testing, through to full implementation, such as ACOonet and CERT-Polska.

Many have made changes to incorporate local working practices.
Support:

- Bug fixes
- Major work areas
- Bestpractical support packages.

New Area’s of development:

- Multiple Instances on the same source
- IODEF Integration
- PGP/GPG
  - Validation
  - Updates by email
  - Signing/encryption from the front end
- Integrated Incidents (adding in advisories, published material etc) ?
Funding:

General agreement that teams will help fund this project. BestPractical have stated that if support is purchased by teams then even major costs could be kept to a minimum, or completed as part of the support contract.

Possibility of using TERENA acting as a channel for contract and payments, possibly through the TI.
WG Organisation and Agreements:

Some discussion on organisation was decided:

- Possibility of using a modified version of the eCSIRT code of conduct, to aid working relationships.
- Use the TF-CSIRT or RTIR mailing list for communication (which ever is deemed appropriate)
- A WG requirement will need to be created for BestPractical.
- A Statement of work will be required from BestPractical, which will require the signature of all parties.
- The Agreement with BestPractical will have milestones, which will need to be signed of with a majority of the teams in agreement (% to be decided).
AOB:

- Possibility of a code security audit (Is there anyone out there?)

Next Meeting:

- To Be Arranged (hopefully beginning of Feb)
- Location (possibly London)
- Will be more of a requirements workshop
- If anyone would like to join the WG then contact me
Questions