RT for Incident Response (RTIR)

Andy Bone

JANET-CERT Manager
Plan of action

Brief Introduction
RTIR Update
Future of RT
Discussion & Views
W G Proposal
mini BOF

Me
John
Me (again)
You lot (I hope)

With your cooperation
RT for Incident Response (RTIR)

John Green

JANET-CERT
Overview

It’s designed to track issues
- It doesn’t really care what sort

What it gets used for
- Bug tracking, helpdesk, customer service, abuse, network operations, sales lead tracking, todo lists….

Mason, perl, mysql, apache
#31: Sample ticket

## Results
- Ticket 31 created in queue 'General'

## The Basics
- **Id:** 31
- **Status:** new
- **Worked:** 0 min
- **Priority:** 0/0
- **Queue:** General

## Dates
- **Created:** Tue Apr 22 16:39:51 2003
- **Starts:** Not set
- **Started:** Not set
- **Last Contact:** Not set
- **Due:** Not set
- **Closed:** Not set
- **Updated:** Tue Apr 22 16:40:45 2003 by root

## Custom Fields
- **TestingCF:** (no value)

## People
- **Owner:** root
- **Requestors:** root@localhost
  - **Cc:**
  - **AdminCc:**

## History

<table>
<thead>
<tr>
<th>Date</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tue Apr 22 16:39:51 2003</td>
<td>root - Ticket created</td>
</tr>
<tr>
<td></td>
<td>Subject: Sample ticket</td>
</tr>
<tr>
<td></td>
<td>This is a sample</td>
</tr>
</tbody>
</table>

## Relationships
- Depends on:
- **Depended on by:**
  - **Parents:**
  - **Children:**
  - **Refers to:**
  - **Referred to:**

---

*© JANET Association trading as UKERNA 2003*

TF-CSIRT Amsterdam 24 September 2003
#3: **binary attachment test**

**基本資訊**

<table>
<thead>
<tr>
<th>編號</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>現況</td>
<td>新建立</td>
</tr>
<tr>
<td>處理時間</td>
<td>0 分鐘</td>
</tr>
<tr>
<td>優先順位</td>
<td>0/0</td>
</tr>
<tr>
<td>表單</td>
<td>General</td>
</tr>
</tbody>
</table>

**日期**

- 新增日：2003-04-17 17:20:39 星期四
- 應起始日：尚未設定
- 實際起始日：尚未設定
- 上次聯絡：尚未設定
- 到期日：尚未設定
- 已解決：尚未設定
- 前次更新：2003-04-17 17:21:56 星期四 (root)

**人員**

- 承辦人：Nobody
- 申請人：root@localhost
- 副本：
- 管理員副本：

**附件**

- 2003-04-17 17:20:39 星期四 (43b)
  - spacer.gif

**記錄**

- 2003-04-17 17:20:39 星期四
  - root - 申請單新增完畢
  - From: root@localhost
  - To: root@localhost
  - Subject: binary attachment test
What we wanted to do

• Allow JANET-CERT staff to manage increasing workload effectively
• Provide a base for other IR teams to build new tools
• Be easily extensible as new services need to be provided
• Save money
Starting over

• JANET-CERT contacted Best Practical
• We put together a plan to extend RT for Incident Handling
• RT was close, but didn’t have everything we needed
New functionality in RTIR

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
How RTIR carves things up

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
### RT for Incident Response

#### 10 new unlinked Incident Reports...

<table>
<thead>
<tr>
<th># Subject</th>
<th>State</th>
<th>Owner</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 An OpenRelay on 192.168.1.1</td>
<td>new</td>
<td>Nobody</td>
<td>in 45 min</td>
</tr>
<tr>
<td>9 Denial of Service from 10.0.0.1</td>
<td>new</td>
<td>Nobody</td>
<td>in 38 min</td>
</tr>
<tr>
<td>10 MAKE MONEY FAST ($$$$$$$)</td>
<td>new</td>
<td>Nobody</td>
<td>in 38 min</td>
</tr>
<tr>
<td>11 Port scan from 192.168.6.5</td>
<td>new</td>
<td>Nobody</td>
<td>in 50 min</td>
</tr>
</tbody>
</table>

#### 1 of 1 most due incidents owned by johng (and unowned)...

<table>
<thead>
<tr>
<th># Subject</th>
<th>Owner</th>
<th>State</th>
<th>Priority</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 Copyright material on 192.168.9.9</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>in 52 min</td>
</tr>
</tbody>
</table>

#### 2 of 2 most due incidents...

<table>
<thead>
<tr>
<th># Subject</th>
<th>Owner</th>
<th>State</th>
<th>Priority</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 Scan from 192.168.55.34</td>
<td>rt</td>
<td>open</td>
<td>50</td>
<td>in 6 days</td>
</tr>
<tr>
<td>13 Copyright material on 192.168.8.9</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>in 52 min</td>
</tr>
</tbody>
</table>
Incident Reports
Incident Report #8: An OpenRelay on 192.168.1.1

The Basics

State: new
Incident: (no Incidents) [Link] [New]
Time Worked: 0 min
How Reported: Email
Reporter Type: external individual
SLA: Full service

People

Owner: john
Correspondents: john@giggled.org
Cc:
AdminCc:

Dates

Created: Fri Jun 20 10:52:34 2003
Starts: Fri Jun 20 10:52:34 2003
Due: Fri Jun 20 11:52:34 2003
Updated: Fri Jun 20 11:15:55 2003 by john

More about John Green

Comments about this user:
No comment entered about this user
This user's 10 highest priority tickets:
- 8: An OpenRelay on 192.168.1.1 (new)
- 11: Port scan from 192.168.6.5 (new)
- 9: Denial of Service from 10.0.0.1 (now)
- 12: Copyright material on 192.168.9.9 (new)
- 10: MAKE MONEY FAST ($$$$$$$$) (new)
- 15: Scan from 192.168.25.34 (open)

History

Fri Jun 20 10:52:34 2003  john@giggled.org - Ticket created

Subject: An OpenRelay on 192.168.1.1
Date: Fri, 20 Jun 2003 10:44:08 +0100
To: cert-bmg@cert.ja.net
Cc: John Green <john@giggled.org>

Hello,
One of your users has an open relay on machine 192.168.1.1

Please let me know once this matter has been resolved.

Regards
--
Look up information

WHOIS: 202.32.49.34
Treecert to: 192.168.1.1

WHOIS Results

Results for: jwhois 192.168.1.1
OrgName: Internet Assigned Numbers Authority
OrgID: IANA
Address: 4676 Admiralty Way, Suite 330
City: Marina del Rey
OrgTechEmail: res-ip@iana.org

Incidents: 192.168.1.1
(id Subject State Priority Actions)
8 An OpenRelay on 192.168.1.1 new 0

Investigations: 192.168.1.1
(id Subject State Priority Actions)

Incident Reports: 192.168.1.1
(id Subject State Priority Actions)
8 An OpenRelay on 192.168.1.1 new 0

Blocks: 192.168.1.1
(id Subject State Priority Actions)

Look Up Information

WHOIS: 202.32.49.34
Treecert to: 192.168.1.1

WHOIS Results

Results for: jwhois 192.168.1.1
OrgName: Internet Assigned Numbers Authority
OrgID: IANA
Address: 4676 Admiralty Way, Suite 330
City: Marina del Rey
OrgTechEmail: res-ip@iana.org
Incidents
One of your users has an open relay on machine 192.168.1.1.

Please let me know once this matter has been resolved.

Regards
Incident #18: An OpenRelay on 192.168.1.1

**Incident 18: An OpenRelay on 192.168.1.1**
- **Owner:** john
- **State:** open
- **Subject:** An OpenRelay on 192.168.1.1
- **Description:** (no value)
- **Priority:** 50
- **Time Worked:** 0
- **Constituency:** JANET-CERT
- **Function:** Abuse Desk
- **Classification:** Spam

**Incident Reports**
- **8:** An OpenRelay on 192.168.1.1 (open) in 6 days

**Investigations**
- **19:** An OpenRelay on 192.168.1.1 (open) in 6 days

**Blocks**
- **20:** Block request (pending activation) 58 sec ago

**Dates**
- **Created:** Fri Jun 20 11:23:40 2003
- **Started:** Fri Jun 20 11:23:40 2003
- **Due:** Not set
- **Updated:** Fri Jun 20 11:28:07 2003 by john

**History**
- **Fri Jun 20 11:23:40 2003**
  - **john - Ticket created**
  - Subject: An OpenRelay on 192.168.1.1
  - Hello,
  - One of your users has an open relay on machine 192.168.1.1
  - Please let me know once this matter has been resolved.
  - Regards
  - --

- **Fri Jun 20 11:23:40 2003**
  - **RT_System - Starts changed from Not set to Fri Jun 20 11:23:40 2003**

**Display mode:** [Brief headers] [Full headers]
### RTIR for Incident Response

#### 10 new unlinked Incident Reports...

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

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

<table>
<thead>
<tr>
<th># Subject</th>
<th>Owner</th>
<th>State</th>
<th>Priority</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 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>13 Copyright material on 192.168.9.9</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>in 25 min</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th># Subject</th>
<th>Owner</th>
<th>State</th>
<th>Priority</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 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 Scan from 192.168.55.34</td>
<td>rc</td>
<td>open</td>
<td>50</td>
<td>in 6 days</td>
</tr>
<tr>
<td>13 Copyright material on 192.168.9.9</td>
<td>johng</td>
<td>open</td>
<td>50</td>
<td>in 25 min</td>
</tr>
</tbody>
</table>
Where we are now

• Version 1.0 released end of August
• In use by a number of teams
• Tested and evaluated by many more
• Only package (as far as we know) specifically designed for IRT use
The future

Cross-IRT integration
- IODEF?
- RT-native integration

Cross-tool integration
- PGP signing/validation

Continuing development and bugfixes
Finding out more

rtir-request@lists.bestpractical.com

- Closed list for incident response team staff

http://www.bestpractical.com
http://www.bestpractical.com/rtir/
RT for Incident Response
(RTIR Moving On)

Andy Bone
JANET-CERT Manager
The Dream

Although RTIR is still in its infancy we believe that we need to think about the future:

What can we do:

• Leave it as it is.

• Each team go away and modify to its own specification.

• Create a consortium of teams within the TF-CSIRT to increase spending power and create a standard system.
Training

Possible Training Course on RT/RTIR:
Requested by CERT-POLSKA and ourselves.

Bestpractical agreed but:

• Need minimum of 8 people.
• Facilities
• Smallish cost (negotiable and dependant on attendees)
Discussion

Other Teams using RTIR Views and observations:

- ACOnet-CERT
- CERT-POLSKA
- Anyone out there
Proposal

I would like to propose, that we form a WG through the TF-CSIRT to investigate the future of RTIR.

With a mind to:

• Investigate and prepare requirements for RTIR V 2.

• To form a consortium of like minded teams to cooperate with Bestpractical in the implementation of RTIR V 2.

• Investigate and organise training on RT/RTIR.
BOF

We intend to hold a brief BOF during the tea break if any teams would like to talk about the way forward and are interested in joining a WG, please join us and express your views.
Questions