IRT-Object in the RIPE Database, "interim" meeting

Overview

Ulrich Kiermayr, Wilfried Wöber: ACOnet-CERT TF-CSIRT, 10th meeting – Amsterdam, NL

September 26, 2003
What does the IRT-Object do?

- documents Incident Response Teams in the RIPE Database
  - registers contact information: PGP-Keys, ...
- supports a more fine grained and scalable approach than individual 'abuse-c, security-c, spam-c, .....'
- links to resource objects (inetnum, inet6num)
- only one object needs maintenance
What does it look like?

irt:          IRT-JANET-CERT
address:      Atlas Centre
address:      Chilton
address:      DIDCOT, Oxon
address:      OX11 0QS UK
phone:        +44 1235 822 340
fax-no:       +44 1235 822 398
e-mail:       cert@cert.ja.net
signature:    PGPKEY-836D7141
encryption:   PGPKEY-836D7141
admin-c:      AB2554-RIPE
tech-c:       RT644-RIPE
auth:         PGPKEY-3EA2BD2B
remarks:      JANET-CERT coordinates security in JANET.
remarks:      http://www.ja.net/cert/
remarks:      JANET is the UK education and research network.
irt-nfy:      ripe-admin@cert.ja.net
notify:       ripe-admin@cert.ja.net
mnt-by:       JANET-CERT
changed:      cert@cert.ja.net 20020808
source:       RIPE

eMail Address to notify about references

Team's PGP-key used for signing
Team's PGP-key used for encryption
Team's PGP-key used to authenticate references
What to do with it?

Attach the mnt-irt attribute to the resources:

- requires authorization from both parties:
  - maintainer of the address resource
  - signature of the IRT with the `auth:` PGP-Key

Search for the most specific inet(6)num referencing a mnt-irt:

`whois -c <IP-Addr>`
Search without -c

[uk@worf AcoNet]$ whois -r -Tinetnum 193.171.255.0

<table>
<thead>
<tr>
<th>inetnum:</th>
<th>193.171.255.0 - 193.171.255.95</th>
</tr>
</thead>
<tbody>
<tr>
<td>netname:</td>
<td>ACONET-VIX-SERVICES</td>
</tr>
<tr>
<td>descr:</td>
<td>ACOnet Services Network</td>
</tr>
<tr>
<td>country:</td>
<td>AT</td>
</tr>
<tr>
<td>admin-c:</td>
<td>GW13-RIPE</td>
</tr>
<tr>
<td>admin-c:</td>
<td>AP135-RIPE</td>
</tr>
<tr>
<td>tech-c:</td>
<td>CP8-RIPE</td>
</tr>
<tr>
<td>status:</td>
<td>ASSIGNED PA</td>
</tr>
<tr>
<td>notify:</td>
<td><a href="mailto:domain-admin@univie.ac.at">domain-admin@univie.ac.at</a></td>
</tr>
<tr>
<td>mnt-by:</td>
<td>AT-DOM-MNT</td>
</tr>
<tr>
<td>changed:</td>
<td><a href="mailto:andreas.papst@univie.ac.at">andreas.papst@univie.ac.at</a> 19970324</td>
</tr>
<tr>
<td>changed:</td>
<td><a href="mailto:Woeber@CC.UniVie.ac.at">Woeber@CC.UniVie.ac.at</a> 19970328</td>
</tr>
<tr>
<td>source:</td>
<td>RIPE</td>
</tr>
</tbody>
</table>
Search with -c included

[uk@worf AcoNet] $ whois -r -c -Tinetnum 193.171.255.0

inetnum:            193.170.0.0 - 193.171.255.255
descr:              ALLOCATED BLOCK
descr:              Provider Local Registry
descr:              ACOnet
country:            AT
admin-c:            WW144
tech-c:             WW144
tech-c:             WK42
tech-c:             CP8–RIPE
status:             ALLOCATED UNSPECIFIED
mnt-by:             RIPE–NCC–HM–MNT
mnt-lower:          ACONET–LIR–MNT
mnt-irt:            IRT–ACOnet–CERT
changed:            roderik@ripe.net 19950315
[ ... ]
changed:            hostmaster@ripe.net 20011018
source:             RIPE
How to get one (1)?

- directly by way of RIPE-NCC (see: ripe-254)

  - creation request submitted by the admin-c contact of the irt object.
  - request is authenticated by an existing mntner, referenced by the object. The need to create an irt object cannot be the (only) reason for mntner creation.
  - keys referenced by the irt object are in the database already, the key owner shows affinity to the irt.
  - reason(s) for creation is presented along with the time line for deployment (i.e. referencing the object from where and when).
How to get one (2)?

by a well known trusted body, recognized by the RIPE-NCC

– currently one: Trusted Introducer
– [http://www.ti.terena.nl](http://www.ti.terena.nl)

  – object is maintained by the TI
  – quality of data is assured by this body
– other groups possible, even sought:
  – ISP associations
  – NRENs, ....
Example

[uk@worf AcoNet]$ whois -r irt-aconet-cert

irt: IRT-ACOnet-CERT
address: Vienna University Computer Center
address: Universitaetsstrasse 7
address: A-1010 Vienna
address: AUSTRIA
phone: +43 1 4277 14045
fax-no: +43 1 4277 9140
e-mail: cert@aco.net
signature: PGPKEY-B06F5077
encryption: PGPKEY-B06F5077
admin-c: TI123-RIPE
tech-c: TI123-RIPE
auth: PGPKEY-B06F5077
remarks: Emergency telephone number +43 1 4277 14045 (GMT+1/GMT+2 with DST)
remarks: http://www.trusted-introducer.org/teams/aconet-cert.html
remarks: This is an accredited IRT (level 2)
irt-nfy: cert@aco.net
notify: tiirt@stelvio.nl
notify: cert@aco.net
mnt-by: TRUSTED-INTRODUCER-MNT
changed: gert-henk.bakker@stelvio.nl 20030813
source: RIPE
Current Numbers

Total Objects: 39 (as of 2003-09-25)

"referenced" counts:

- IRT-CERT-NL: 313
- IRT-ITGATE: 19
- IRT-UNINETT-CERT: 18
- IRT-ACOnet-CERT: 23
- IRT-JANET-CERT: 7
- IRT-EPLAN: 7
- IRT-UK: 2
- IRT-CERT-POLSKA: 9
Open Issues

- which other resources should be taggable?
  - AS-Numbers?

- similar facilities in other RIRs?

- deployment

- tools to easily retrieve the information

- authenticity of the data in the database (general problem)

- documentation
TF-CSIRT "interim" Meeting

Just before RIPE46 (Friday, 2003-08-29)

- a big thank you to the TERENA Secretariat for hosting the meeting, and Marco for taking notes
- 10 .. 14 participants (some just for a while)
- very useful mix of participants
  - Government, NRENs, TI, RIPE NCC, ISP assoc.
- minutes (and other stuff) accessible via a link at Marco Thorbruegge's summary page
  - http://www.dfn-cert.de/team/matho/irt-object/
TF-CSIRT "interim" Meeting

Results

- "marketing"
  - (RIPE46, FIRST 2004 @BUD, regional…)
- documentation (technical How-To, FAQ)
- (continue to) work with the NCC on improving access to the information
  - (e.g. web-based whois interface)
- guidelines for "mass-population" - see minutes
- we'll continue to use the TF-CSIRT mailing list (till we get kicked off :-)


Last minute information

Discussion on a more general approach to manage authentication when referencing a (protected) object in the database has started (irt:, mntner:, and maybe org: in the future)

Watch this space :-)

Resources

- ripe-254 document
  - http://www.ripe.net/ripe/docs/irt-object.html
- Ripe Database Manual
- Trusted Introducer
  - http://www.ti.terena.nl
TF-CSIRT "interim" meeting

Questions
Contact Information

Ulrich Kiermayr
Vienna University Computer Center / ACOnet
Universitätsstrasse 7
1010 Vienna, AT
Phone: +43 1 4277 14104
Fax: +43 1 4277 9140
eMail: ulrich.kiermayr@univie.ac.at