The IRT Object in the RIPE Database

The direct link from IP numbers to CSIRTs

Don Stikvoort, Elsinore
Wilfried Wöber, Vienna University
Problem Outline

● Despite all high tech, wizardry and risk management in today’s security handling …

● … incidents still need resolution …

● … and that still involves a lot of handwork

● Incident related questions
  − What is it
  − Where does it go to
    ● And who will handle it over there
  − Where does it come from (supposedly)
    ● And who are we going to bother with it there
  − How are we going to solve it
Problem Statement

- Given you done your job and you translated hostnames, domain names, mail addresses, checked logs etcetera, and finally you have:
  - A bunch of IP addresses where the incident might be coming from (or be targeted at)
  - What are you going to do?
  - How to find responsible security people who will seriously deal with what you want to give them

= *How to find the good guys to haunt down the bad guys*
Classical Solutions

- Query RIPE NCC / ARIN / APNIC / LACNIC
- FIRST member list
- Trusted Introducer repository
- Use abuse-c address
- Common mailbox names may work
- Your pile of business cards

.... messy ..... inconclusive ... unreliable ....
A better solution

- Mapping CSIRT info onto the IP numberspace
- Make tools available that:
  - Take IP numbers as input
  - Give the appropriate CSIRT or CSIRTs as output
  - Give authenticity/reliability information on the CSIRT info output -- when available
- Sounds so simple …
So what happened?

- 1994 idea by Wöber and Stikvoort
  - Possibly others too? We don’t know
- Early implementation around 1995
  - Niels den Otter, CERT-NL (SURFnet-CERT today)
  - Not scalable nor maintainable
- In 2000 taken up again
- Summer 2002 “IRT object in the RIPE database”:
  - RIPE technical document
  - Implementation in RIPE database
Interludium

Lesson learned:

Don’t try to push things through in a hurry in the Internet, or even within a smaller organisation like FIRST --- it simply takes time … and patience … and convincing … and hard work 😊
What does the IRT object look like?

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>irt:</td>
<td>IRT-JANET-CERT</td>
</tr>
<tr>
<td>address:</td>
<td>Atlas Centre</td>
</tr>
<tr>
<td>address:</td>
<td>Chilton</td>
</tr>
<tr>
<td>address:</td>
<td>DIDCOT, Oxon</td>
</tr>
<tr>
<td>phone:</td>
<td>+44 1235 822 340</td>
</tr>
<tr>
<td>fax-no:</td>
<td>+44 1235 822 398</td>
</tr>
<tr>
<td>e-mail:</td>
<td><a href="mailto:cert@cert.ja.net">cert@cert.ja.net</a></td>
</tr>
<tr>
<td>signature:</td>
<td>PGPKEY-836D7141</td>
</tr>
<tr>
<td>encryption:</td>
<td>PGPKEY-836D7141</td>
</tr>
<tr>
<td>admin-c:</td>
<td>AB2554-RIPE</td>
</tr>
<tr>
<td>tech-c:</td>
<td>RT644-RIPE</td>
</tr>
<tr>
<td>auth:</td>
<td>PGPKEY-3EA2BD2B</td>
</tr>
<tr>
<td>remarks:</td>
<td>JANET-CERT coordinates security in JANET.</td>
</tr>
<tr>
<td>remarks:</td>
<td><a href="http://www.ja.net/cert/">http://www.ja.net/cert/</a></td>
</tr>
<tr>
<td>remarks:</td>
<td>JANET is the UK education and research network.</td>
</tr>
<tr>
<td>irt-nfy:</td>
<td><a href="mailto:ripe-admin@cert.ja.net">ripe-admin@cert.ja.net</a></td>
</tr>
<tr>
<td>notify:</td>
<td><a href="mailto:ripe-admin@cert.ja.net">ripe-admin@cert.ja.net</a></td>
</tr>
<tr>
<td>mnt-by:</td>
<td>JANET-CERT</td>
</tr>
<tr>
<td>changed:</td>
<td><a href="mailto:cert@cert.ja.net">cert@cert.ja.net</a> 20020808</td>
</tr>
<tr>
<td>source:</td>
<td>RIPE</td>
</tr>
</tbody>
</table>

Team's PGP-key used for signing
Team's PGP-key used for encryption
Team's PGP-key used to authenticate references
eMail Address to notify about references
## How do IP numbers link to IRT objects?

<table>
<thead>
<tr>
<th><strong>inetnum:</strong></th>
<th>192.87.106.0 - 192.87.106.255</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>netname:</strong></td>
<td>SNET-AT-SARA</td>
</tr>
<tr>
<td><strong>descr:</strong></td>
<td>SURFnet IP LAN at SARA</td>
</tr>
<tr>
<td><strong>descr:</strong></td>
<td>Amsterdam</td>
</tr>
<tr>
<td><strong>country:</strong></td>
<td>NL</td>
</tr>
<tr>
<td><strong>admin-c:</strong></td>
<td>SNS1-RIPE</td>
</tr>
<tr>
<td><strong>tech-c:</strong></td>
<td>NCC1-RIPE</td>
</tr>
<tr>
<td><strong>status:</strong></td>
<td>ASSIGNED PA</td>
</tr>
<tr>
<td><strong>mnt-by:</strong></td>
<td>SN-LIR-MNT</td>
</tr>
<tr>
<td><strong>mnt-irt:</strong></td>
<td>irt-SURFnet-CERT</td>
</tr>
<tr>
<td><strong>notify:</strong></td>
<td><a href="mailto:lir@surfnet.nl">lir@surfnet.nl</a></td>
</tr>
<tr>
<td><strong>changed:</strong></td>
<td><a href="mailto:Derk.Reinders@surfnet.nl">Derk.Reinders@surfnet.nl</a> 20010326</td>
</tr>
<tr>
<td><strong>changed:</strong></td>
<td><a href="mailto:Rogier.Spoor@surfnet.nl">Rogier.Spoor@surfnet.nl</a> 20020605</td>
</tr>
<tr>
<td><strong>changed:</strong></td>
<td><a href="mailto:Wim.Biemolt@surfnet.nl">Wim.Biemolt@surfnet.nl</a> 20040422</td>
</tr>
<tr>
<td><strong>source:</strong></td>
<td>RIPE</td>
</tr>
</tbody>
</table>
And what does that yield?

irt: irt-SURFNET-CERT
address: p/a SURFnet bv
address: Postbus 19035
address: 3501 DA Utrecht
phone: +31 30 2305305
fax-no: +31 30 2305329
e-mail: cert@SURFnet.nl
signature: PGPKEY-A6D57ECE
encryption: PGPKEY-A6D57ECE
admin-c: SAM36-RIPE
tech-c: SAM36-RIPE
auth: PGPKEY-834125A1
auth: PGPKEY-3D10C493
remarks: SURFNET-CERT is the Computer Emergency
remarks: Response Team of SURFnet
remarks: This is a TI accredited CSIRT
remarks: (see http://www.ti.terena.nl/teams/level2.html)
irt-nfy: cert@SURFnet.nl
notify: lir@SURFnet.nl
mnt-by: TRUSTED-INTRODUCER-MNT
Who can create an IRT object?

- A recognised organisation with “member teams”
  - Currently the Trusted Introducer only
  - FIRST mentioned as example in RIPE doc
  - Others can apply at the RIPE NCC
- Individual teams
- Creation/modification is done with signed messages
How reliable is an IRT object

- Please note: only *referencing* from inetnum objects makes the IRT object useful
  - Referencing depends on agreement by BOTH the local IP registry AND the IRT-object “auth” i.e. the CSIRT usually

- Value-added information like:
  - `mnt-by: TRUSTED-INTRODUCER-MNT`
  - Further queries possible based on that
  - E.g. www.ti.terena.nl
Do people use the IRT object?

- 14 May 2004:
  - Europe only
  - 49 IRT objects registered
  - 7.1% of all registered IP numbers references an IRT object

- Gradually picking up now, less than 2 years after introduction
Competition

- Why not have a simple “abuse” role …
- … instead of the “complex” IRT object ??
- IRT object gaining momentum again
  - Not so complex after all
  - FAQ, technical howto available at:
    http://www.ti.terena.nl/links/documents.html
  - flexibility
  - Abuse role cannot cope with multiple-team-one-IP-range situations
  - A CSIRT is a whole other ballgame than an IP NOC
Global development

- ARIN implemented a similar mechanism
- APNIC shows interest (and uses same software as RIPE) but no action taken yet
- Only informal contacts with LACNIC thus far
- Different architectures not a problem
Unifying tools needed

- Tool that will take IP numbers as input
- Then search the RIPE and other databases for IRT objects or similar info
- Display this info with any value added info found
  - Like to the TI
  - Give click-on possibility for the value added info
- Need Webform version and sourcecode tool for integration in CSIRT processes
  - TF-CSIRT community (CERT-POLSKA and others) working on it
Thank you

Woeber@cc.univie.ac.at
&
Don.Stikvoort@elsinore.nl

Will answer questions in e-mail with pleasure
(or now, the chair permitting).