# IRT & Trusted Introducer

Srđan Vukovojac: CARNET-CERT
srdjan.vukovojac@carnet.hr

RIPE NCC REGIONAL MEETING DUBROVNIK, HR
September 9, 2011

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# TF-CSIRT & Trusted Introducer(TI)

**TF-CSIRT** – TERENA's task force that promotes collaboration between CSIRTs in Europe, and cooperates with similar organizations elsewhere

**TI** - trusted backbone of the CERT (TF-CSIRT) community in Europe; "web of trust"

# TI Roles

- since year 2000
- lists, accredits and certifies CERTs, and provides them with services
- community-run - it is there for the teams who pay for the services, which are the Accredited (and Certified) teams
- TI Review Board - oversees and steers the TI effort

# TI Services

## PUBLIC SERVICES :

PUBLIC TEAM REPOSITORY

LISTING

ACCREDITATION

MAINTENANCE

## SERVICES FOR MEMBERS ONLY :

MEMBERS TEAM REPOSITORY

ACCREDITATION CERTIFICATION MAINTENANCE

MEMBERS MEETINGS

NETWORKING

TI COMPENDIUM

ONE-CLICK DOWNLOADABLE TEAM INFORMATION

ONE-CLICK DOWNLOADABLE PGP/gpg KEY FILES

**AUTOMATIC IRT-OBJECT REGISTRATION**

TI-PKI. X.509 based TI-PKI

MAILINGLIST FOR ACCREDITED TEAMS

SECURE IN-BAND ALERTING

SECURE OUT-OF-BAND ALERTING

KEY SIGNING

# IRT object in RIPE DB

***IP address space to authoritative incident response team team mapping (e.g. CERT)***

- registers IRT team contact information
- links to inet(6)num objects
- only one object needs maintenance

**EASY WAY TO ROUTE INTERNET SECURITY INCIDENTS!**

# IRT object info – how to get it ?

- to get the smallest specific inet(6)num object containing an "mnt-irt:”

**whois –h whois.ripe.net -c <IP-Addr>**

- to get the **irt** object itself

**whois –h whois.ripe.net -r <IRT-CERT-ORG-COUNTRY>**

# IRT object – how to create one ?

- directly through RIPE NCC -> ripe-254, "IRT Object in the RIPE Database”
- through Trustbroker – currently only TI

# IRT object – example(1)

```
svukovoj@valpovo:~$ whois -h whois.ripe.net -c 193.198.0.0
...
inetnum:      193.198.0.0 - 193.198.255.255
org:          ORG-CAaR1-RIPE
admin-c:      DK2798-RIPE
admin-c:      IV762-RIPE
netname:      HR-CARNET-960508
descr:        Croatian Academic and Research Network
country:      HR
tech-c:       DK2798-RIPE
tech-c:       IV762-RIPE
status:       ALLOCATED PA
mnt-by:       RIPE-NCC-HM-MNT
mnt-irt:      IRT-CARNET-CERT
...
```

# IRT object – example(2)

```
svukovoj@valpovo:~$ whois -h whois.ripe.net -r IRT-CARNET-CERT
….
irt:            IRT-CARNET-CERT
address:        Croatian Academic and Research Network - CARNet
address:        CARNet-CERT
address:        Marohniceva 5
address:        HR-10000 Zagreb
address:        Croatia
phone:          +385 1 666 1 770
phone:          +385 1 666 1 616
fax-no:         +385 1 666 1 767
fax-no:         +385 1 666 1 615
abuse-mailbox:  abuse@carnet.hr
signature:      PGPKEY-2B52583E
encryption:     PGPKEY-2B52583E
admin-c:        TI123-RIPE
tech-c:         TI123-RIPE
auth:           PGPKEY-2B52583E
remarks:        This is a TI accredited CSIRT/CERT
remarks:        emergency phone number +385 1 666 1 770
remarks:        timezone GMT+01 (GMT+02 with DST)
remarks:        https://www.trusted-introducer.org/teams/carnet-cert.html
irt-nfy:        cert@carnet.hr
mnt-by:         TRUSTED-INTRODUCER-MNT
source:         RIPE # Filtered
…
```

# IRT object – why do it

**SECURITY**

**EASIER SECURITY INCIDENT HANDLING**

**SHORTER INCIDENT RESOLUTION TIME**

**CYBERCRIME PREVENTION**

**SAFER INTERNET**

# Resources

- **RIPE DB IRT object FAQ**

  http://www.ripe.net/data-tools/db/faq/irt-faqs

- **RIPE document “IRT Object in the RIPE Database”**

  http://www.ripe.net/ripe/docs/ripe-254.html

- **Additional info on IRT**

  http://www.terena.nl/tech/task-forces/tf-csirt/irt.html

- **Trusted Introducer**

  https://www.trusted-introducer.org/

# Q&A

?