abuse-c roundup

RIPE-49

Marco Hogewoning <marcoh@marcoh.net>
&
Niall O'Reilly <Niall.oReilly@ucd.ie>

The problem:

From: DadCool@XXXXX.de (DadCool)
To: <marcoh@nl.demon.net>
Subject: Scanning my PC for open Ports HeHe
Envelope-to: marcoh@noname.noc.nl.demon.net
Date: Sat, 18 Sep 2004 17:10:03 +0200

Heyho its me Daddy Cool
Why the Hell do you try to scann my Computer?
Do you think I`m Lame?
Do this not anymore otherwise Iwill send a E-Mail to your Provider!!!
Best Regards from Daddy Cool from Paradox
PS: yout Dates are copyed by me so do not make it anymore -be warned !

From: "D.X. K" <freaky_evisu@XXXXXXXX.com>
To: marcoh@nl.demon.net
Subject: scannen
Envelope-to: marcoh@noname.noc.nl.demon.net
Date: Tue, 07 Sep 2004 00:28:05 +0200

wat loop je me fucking poorten te scannen...
dalijk dd0s ik je ff en geef ik je ff aan bij abuse demon... :S
beetje je eigen range lopen scannen :S
pas maar op... mofo

inetnum: 212.238.137.0 - 212.238.238.255
netname: DEMON-NL-DSL
descr: Demon Nederland customers with DSL connections
country: NL
admin-c: DNHG1-RIPE
tech-c: DNDE1-RIPE
tech-c: DIHD-RIPE
mnt-by: AS5417-MNT
remarks: Abuse complaints to abuse@demon.nl, incl. Spam, Port-scans,etc
status: ASSIGNED PA
changed: marcoh@nl.demon.net 20040120
changed: marcoh@nl.demon.net 20040127
changed: marcoh@nl.demon.net 20040204
changed: marcoh@nl.demon.net 20040216
changed: marcoh@nl.demon.net 20040712
source: RIPE

Possible solutions

- modify inetnum and inet6num to support a new attribute ‘abuse-c’

- add abuse-mailbox attribute to various objects (inetnum/inet6num/person/role/...

- modify changed: to support a handle instead of an email address

- in the default database output suppress various fields only relevant to maintaners

‘abuse-c’

Add a new ‘c’ to inetnum/inet6num referring to a person/role who can be contacted

‘abuse-c’

Add a new ‘c’ to inetnum/inet6num referring to a person/role who can be contacted

* Short path of indirection -> lower query/ response overhead

‘abuse-c’

Add a new ‘c’ to inetnum/inet6num referring to a person/role who can be contacted

* Short path of indirection -> lower query/ response overhead

* Target of abuse-c probably has generic contact attribute.
* No aggregation: update is per-inet*num object.

‘abuse-mailbox’

Add an attribute to various objects pointing to an email address (inet*num/irt/person/role)

‘abuse-mailbox’

Add an attribute to various objects pointing to an email address (inet*num/irt/person/role)

* Takes advantage of existing aggregation
* Uses distinguished attribute

‘abuse-mailbox’

Add an attribute to various objects pointing to an email address (inet*num/irt/person/role)

* Takes advantage of existing aggregation
* Uses distinguished attribute

* At cross-purposes with IRT movement (some might see this as 'pro'!)

‘changed changes’

Modify the change attribute to support nic-handles rather then an email address

‘changed changes’

Modify the change attribute to support nic-handles rather then an email address

* Cleaner and more consistent

‘changed changes’

Modify the change attribute to support nic-handles rather then an email address

* Cleaner and more consistent

* Not clear what problem(s) this solution addresses

‘suppress data’

Change default output of the whois server to suppress certain data like notify/upd-to and changed.

‘suppress data’

Change default output of the whois server to suppress certain data like notify/upd-to and changed.

* 'Need-to-know' approach limits confusion

‘suppress data’

Change default output of the whois server to suppress certain data like notify/upd-to and changed.

* 'Need-to-know' approach limits confusion

* Doesn't address problem of how to identify appropriate abuse contact

Consensus ?

Consensus ?

Do nothing ?

Anti-Spam WG

The Anti-spam WG asks the Database WG to take some timely action to improve the availability of abuse contacts for IP addresses allocated through RIPE:

1. to publish an explicit abuse contact address where possible for every address;
2. to lower the profile of other addresses currently in the database and published through whois, which were never intended for the abuse function.

A. modify the IRT object to include an explicit 'abuse-mail' attribute and to remove the mandatory requirement for PGP or similar authentication (or introduce a similar new object with those properties);

and

B. modify the default behaviour of the whois interfaces to find and present an abuse address if there is one and to suppress other e-mail addresses.

Thanks