
security is not an island
HILTONMALTA
24th Annual
FIRST
Conference
MALTA
17 - 22 June 2012
FIRST
Improving Security Together

Automated Incident Notification Helper

Javier Berciano (@jberciano)
INTECO-CERT (http://cert.inteco.es)

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

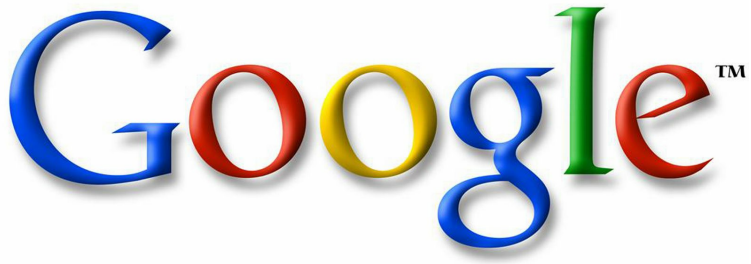
INTECO & INTECO-CERT

Instituto Nacional
de Tecnologías
de la Comunicación

SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
Y PARA LA SOCIEDAD DE
LA INFORMACIÓN

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

Automated Incident Notification Helper



24th Annual FIRST Conference
MALTA
17 - 22 June 2012


OBJECTIVE

Automate notifications during incident handling process.

What we have yet?

- Evidence extraction tools, optimized for big amount of information.
- GenFilesIR: tool to generate splited files for notifications.
- AuRTIR: tool to automate some incident management tasks using RTIR webAPI.

Main problem: Get Abuse contact in an efficient manner

What we need?

Contact information

Information from IP involved in incidents

- Abuse contact from RIRs.
- Private contacts from netblocks or AS.
- National CERT point of contact.

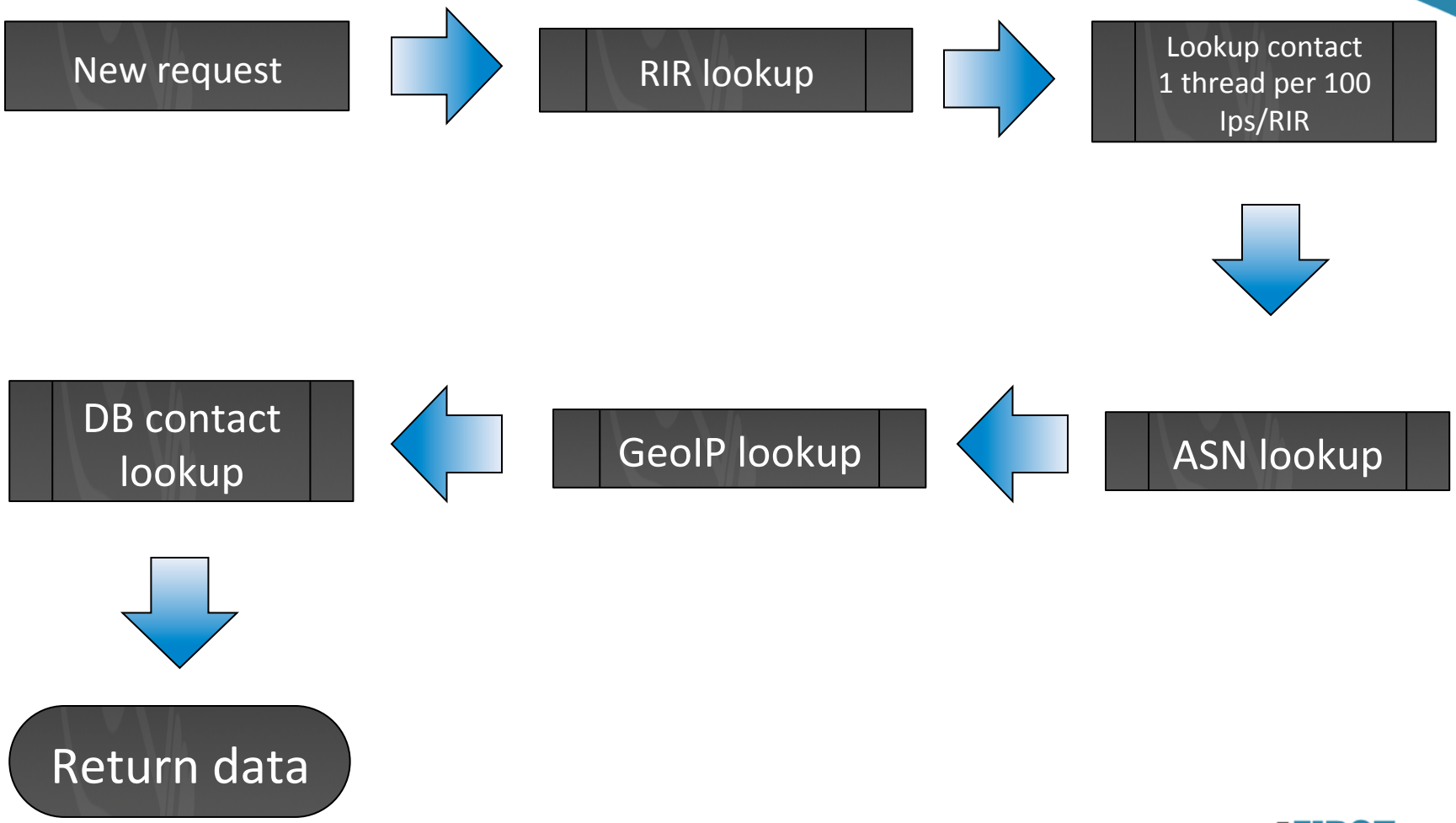
How?

Automated Incident Notification Helper tool

Powered by

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

Request flows



ARIN contact extraction flow

- Obtain IP data (/rest/ip/$IP.xml)
  - Check comments for abuse contact information
  - If customer data is filled (/rest/customer/$CUSTOMER_HANDLE) check it for contact information.
- Check POCs (Points of Contact) for organization (/rest/org/$ORG_HANDLE/pocs/) that owns the IP.
- Check POCs for network (/rest/net/$NET_HANDLE/pocs) that owns the IP.

POC function preference: ABUSE > NOC > TECH > ADMIN

RIPE NCC contact extraction flow

RIPE NCC RESTful service is used to obtain data from RIPE & APNIC.

- Obtain IP data (/whois/search?source=$RIR&query-string=$IP)
- If contact data is being omitted, request contact data using contact handles.

- Check if it is assigned to JPNIC. If it's true request contact data to http://whois.nic.ad.jp/cgi-bin/whois_gw
- Korea has another similar service

Contact preference: irt-nfy > mnt-irt > notify > abuse-mailbox > tech-c > admin-c > generic email field > remarks > trouble

LACNIC contact extraction flow

- LACNIC gives us access to bulk whois only with netnums and contact handle → **agreement required**.
- Parse LACNIC bulk whois data to extract inetnums and their associated contact handle.
- Extract contact data using traditional whois, several IP addresses and a lot of patience.
- Store contacts in MySQL database.

Contact preference: abuse > tech > owner

AfriNIC contact extraction flow

- AfriNIC gives us access to bulk whois only with netnums and contact handle → **agreement required**.

  Still in development, agreement signed two weeks ago.
  It will be implement like LACNIC case.

- Parse AfriNIC bulk whois data to extract inetnums and their associated contact handle.
- Extract contact data using traditional whois, several IP addresses and a lot of patience.
- Store contacts in MySQL database.

Contact preference: abuse > tech > owner

Contacts database

MySQL database also has contacts manually gathered from:

- Netblocks (public or private contacts)
- AS (public or private contacts)
- National CERTs

MySQL™

Input

Single mode: whois query for one ip address

```
whois -h ainh.cert.inteco.es 193.53.165.3
```

Bulk mode:

- One IP per line
- Delimeters: begin … end
- Using netcat tool

Input

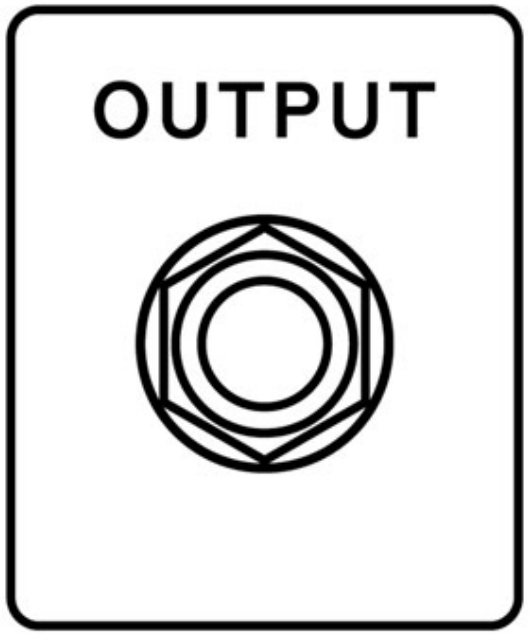
```
$ cat file
begin
verbose
69.60.114.138
91.121.6.93
91.206.30.201
77.79.13.17
91.230.194.54
194.54.80.68
178.238.238.59
195.53.165.3
124.248.207.207
190.123.43.189
193.188.46.32
193.53.165.3
end

$ netcat ainh.cert.inteco.es 43 < file
```

Output format

Output data provided by tool is

- AS Number
- IP address
- BGP Prefix
- Country Code
- RIR
- Abuse Contacts
  - National CERT
  - DB Public contacts
  - Private contacts
  - RIR-extracted
- AS Name



Output format

Abuse contacts field:

- “n:” designates national CSIRT contact in database.
- “a:” ASN or netblock public contact in database.
- “p:” private contact for AS or netblock in database.
- “r:” abuse contacts collected from RIR.

Until know only whois service is working

Output

AS | IP | BGP Prefix | CC | RIR | Abuse Contacts | AS Name
15083 | 69.60.114.138 | 69.60.116.0/22 | US | Arin | n:soc@us-cert.gov r:abuse@serverpronto.net | INFOLINK-MIA-US - Infolink
16276 | 91.121.6.93 | 91.121.0.0/18 | FR | Ripe | n:certa-svp@certa.ssi.gouv.fr r:abuse@ovh.net | OVH OVH Systems
42331 | 91.206.30.201 | 91.206.30.0/23 | UA | Ripe | n:cert@cert.gov.ua r:noc@freehost.ua | FREEHOST PE Freehost
16125 | 77.79.13.17 | 77.79.12.0/23 | LT | Ripe | n:cert@cert.lt r:abuse@aleja.lt | DC-AS UAB Duomenu Centras
49699 | 91.230.194.54 | 91.230.192.0/22 | BG | Ripe | n:cert@govcert.bg r:abuse@icn.bg | ICN-BG Internet Corporated Networks Ltd.
41671 | 194.54.80.68 | 194.54.80.0/22 | UA | Ripe | n:cert@cert.gov.ua r:abuse@server.ua | SERVER-UA-AS SERVER.UA UKRAINE DEDICATED SERVICE
51167 | 178.238.238.59 | 178.238.224.0/20 | DE | Ripe | n:certbund@bsi.bund.de r:abuse@giga-hosting.biz | GIGA-HOSTING Giga-Hosting GmbH
3352 | 195.53.165.3 | 195.53.0.0/16 | ES | Ripe | n:cert@rediris.es n: info@ccn-cert.cni.es n:incidencias@cert.inteco.es a:nemesys@telefonica.es p:XXX@telefonica.es r:mario.garcia@inteco.es | TELEFONICA-DATA-ESPANA TELEFONICA DE ESPANA
38478 | 124.248.207.207 | 124.248.207.0/24 | HK | Apnic | n:hkcert@hkcert.org r:hostmaster@sunnyvision.com | SUNNYVISION-AS-AP SunnyVision Limited
52284 | 190.123.43.189 | 190.123.32/20 | PA | Lacnic | r:ABUSE@PANAMASERVER.COM | Panamaserver.com
12046 | 193.188.46.32 | 193.188.46.0/23 | MT | Ripe | n:mtcert.mitts@gov.mt r:dave.mifsud@um.edu.mt | ASN-CSC-UOM University of Malta

Optimization tricks

- ASN lookup performed in memory using Patricia Trie.
- LACNIC contact lookup performed in memory using Patricia Trie. AfriNIC will be equal.
- RESTful requests to ARIN/RIPE are cached by Squid.
- RESTful requests to ARIN/RIPE are highly parallelized.
- LACNIC contacts are obtained fortnightly and stored in DB. AfriNIC will be equal.

Troubles & solutions

- ASN lookup too slow in DB → Patricia Trie.
- RIPE NCC RESTful block some kind of squid requests → Squid headers must be hidden.
- RIPE NCC hide email data if you do too many requests → balance Squid output over several IP addresses.
- LACNIC contact data extraction rate limit. → several IP addresses and a lot of patience ☺.
- Maybe AfriNIC rate limit ☹ → same solution than LACNIC.

Improvements

- Performance: Beat the current 10 contacts/thread/sec mark
- New RESTful interface
- Replace Shadowserver with MaxMind ASN DB.
- Extraction for domain names contacts?

Improvements: RESTful interface

- Several output formats (Chosen using Content-Type header or file extension):
  - XML
  - Plain Text
  - JSON
- Use of a reverse proxy to improve performance.

Improvements:
RESTful JSON sample


```
{
        'ASN': 3352,
        'IP': '195.53.165.3',
        'BGP Prefix': '195.53.0.0/16',
        'Country': 'ES',
        'RIR': 'RIPE',
        'AS Description': 'TELEFONICA-DATA-ESPANA TELEFONICA DE ESPANA',
        'Contacts': [
                    {'source': 'DB', 'type': 'National CERT', 'visibility':
'public', 'email': 'cert@rediris.es'},
                              {'source': 'DB', 'type': 'National CERT',
'visibility': 'public', 'email': 'info@ccn-cert.cni.es'},
                    {'source': 'DB', 'type': 'National CERT', 'visibility':
'public', 'email': 'incidencias@cert.inteco.es'},
                    {'source': 'DB', 'type': 'AS', 'visibility': 'public',
'email': 'nemesys@telefonica.es'},
                    {'source': 'DB', 'type': 'AS', 'visibility': 'private',
'email': 'XXXXX@telefonica.es'},
                  {'source': 'RIR', 'email': 'mario.garcia@inteco.es'}
        ]
}
```

Collaboration?

Yes, we can !

Thank you!!!

Javier Berciano Alonso

INTECO-CERT Reactive services Team Leader

javier.berciano@inteco.es / jberciano@cert.inteco.es

PGP Key ID: 0xB7952066

PGP Fingerprint: DBEC 1B96 97ED 9641 9B51 E200 CF49 7864 B795 2066

@jberciano