NANOG 67 Security Track

Jelena Mirkovic - SENSS
Ryan Haley – CTF
Christoph Dietzel – RPKI
Michael Sabbota – Automation
You?
John Kristoff – UTRS (time permitting)

Unwanted Traffic Removal Service
https://www.cymru.com/jtk/misc/utrs.html

- Multi-hop, destination-based, community RTBH relay
- As I left it:
  - ~140+ active networks, 150+ inquiries
  - ~5 – 50 announcements / day
  - ~60 networks making announcements
  - ~9500 announcements (~1900 unique) yearly
  - No serious problems known, reasonably safe

Database Tables

```
utrs=> \d
                List of relations
 Schema |         Name          |   Type   |  Owner
--------+-----------------------+----------+---------
 public | blacklist             | table    | utrs_rw
 public | blacklist_seq         | sequence | utrs_rw
 public | contact               | table    | utrs_rw
 public | contact_seq           | sequence | utrs_rw
 public | local                 | table    | utrs_rw
 public | local_seq             | sequence | utrs_rw
 public | network               | table    | utrs_rw
 public | network_seq           | sequence | utrs_rw
 public | networkcontact        | table    | utrs_rw
 public | networkcontact_seq    | sequence | utrs_rw
 public | peer                  | table    | utrs_rw
 public | peer_seq              | sequence | utrs_rw
 public | routes                | table    | utrs_rw
 public | routes_seq            | sequence | utrs_rw
```

\d network

```
 Column |  Type   |          Modifiers
--------+---------+-----------------------------
 row_id | bigint | not null default
                   nextval('network_seq'::regclass)
 asn    | bigint | not null
 asname | text   |
```

\d peer

```
  Column   |     Type                 |        Modifiers
-----------+--------------------------+-------------------------------
 row_id    | bigint                   | not null default
                                        nextval('peer_seq'::regclass)
 localasn  | bigint                   | not null
 localaddr | inet                     | not null
 peerasn   | bigint                   | not null
 peeraddr  | inet                     | not null
 nexthop   | inet                     | not null
 md5       | text                     | not null
 flowspec  | boolean                  | not null default false
 lastseen  | timestamp without
             time zone                |
```

\d routes

```
  Column    |         Type         |           Modifiers
------------+----------------------+-------------------------------------
 row_id     | bigint               | not null default
                                     nextval('routes_seq'::regclass)
 announced  | timestamp without    | not null default
              time zone              date_trunc('seconds'::text, now())
 peerasn    | bigint               | not null
 peeraddr   | inet                 | not null
 route      | inet                 | not null
 aspath     | text                 |
 category   | text                 | default 'utrs'::text
 withdrawn  | boolean              | not null default false
```

ExaBGP hooked processes (logging)

```
process receive-routes {
    encoder json;
    receive-routes;
    run /path/to/receive-routes.pl;
}

process receive-keepalives {
    receive {
        parsed;
        keepalive;
    }
    run /path/to/receive-keepalives.pl;
    encoder json;
}
```

syslog-ng hooked processes (processing)

```
destination d_keepalive {
    program("/path/to/process-keepalives.pl");
};

destination d_update {
    program("/path/to/process-updates.pl -m");
};
```

process-updates.pl

```
next if $route !~ m{ \A \d{1,3}
    (?: [.] \d{1,3} ){3} [/] 32 \z }xms;

next if !valid_peer(...);
next if $pt_bogon->match_string($route);

if ( $type eq 'announcement' ) {
    next if !historic_route(...);
    next if !blacklisted(...);
    next if num_of_announcements(...) >= $MAXPREFIX;
}
else {
    next if !announced(...);
}

add_to_database_rib(...);
send_update(...);
if ($opts{m}) { email_alert(...); }
```

Parting Thoughts

- Convincing people to use/setup the service
- Thanks for all your routes, not!
- Relaying peer's customer routes needed
- Could've used a web-based interface
- Some interest in flow-spec, but not enough
- Seems do-able, not sure if TC will continue it :-/
- If not, should we try re-implementing/deploying?