Monitoring your prefixes with BGPmon

Andree Toonk

Andree@bgpmon.net

BGP mon

Where will we go today

1. BGPmon overview
2. Classifying alarms
3. Methods to detect hijacks
4. Using IRR data
5. Demo
6. Questions

Andree Toonk
andree@bgpmon.net

BGPmon: New kid on the block

Early 2008:

- Set of scripts intended for use in our (UBC/BCNET AS271 network)

Summer 2008:

- Requests to make available for peers

October 2008:

- Publicly available tool

Andree Toonk
andree@bgpmon.net

BGP mon

Feature overview

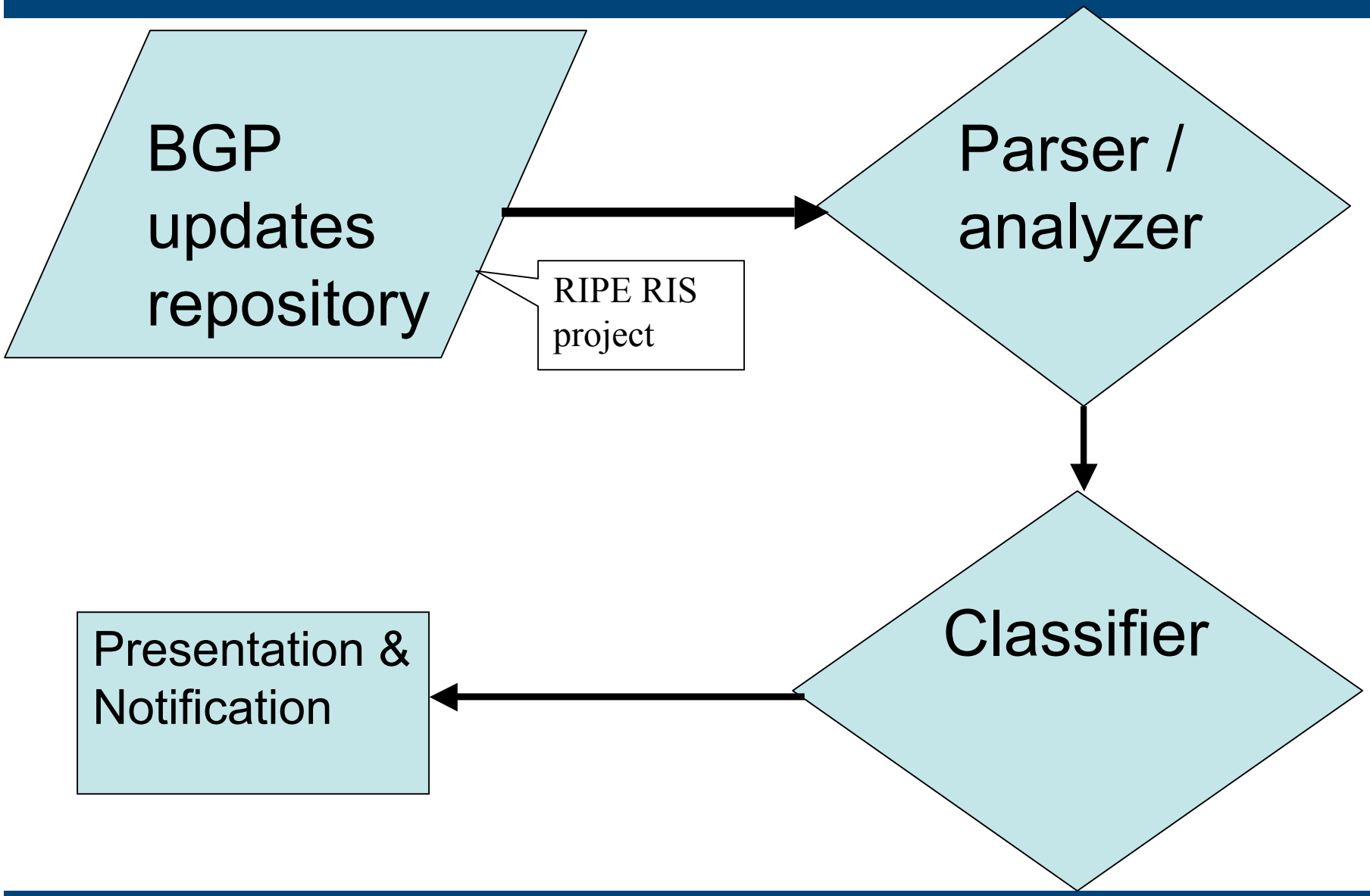
Feature rich:

- Alarm classifier
- IPv4 & IPv6 support
- 2 & 4 byte ASN support
- Fast notification time (~10min)
- Overview of historical alarms in web portal
- Regular expressions support
- Peer Threshold support
- IRR support
- Bogon detection
- And more…

Andree Toonk
andree@bgpmon.net

BGP mon

Architecture



Andree Toonk
andree@bgpmon.net

BGP mon

Event Classifier

Classifying event by type helps to determine the cause & impact

Three main event types:

1. Monitor your own network for configuration errors.
2. Monitor stability of your prefixes.
3. Monitor for hijacks by others.

Andree Toonk
andree@bgpmon.net

BGP mon

Your own announcements

Detect configuration errors ASAP

Stable situation:

142.231.0.0/16 Originated by AS271

Configuration change, causing you to leak:

142.231.0.0/17 Originated by AS271

Andree Toonk
andree@bgpmon.net

Your own announcements

```
From: BGPmon Alert <info@bgpmon.net>
To: andree.toonk@bc.net
Subject: BGPmon.net Notification

<..>
====================
More Specific with known ASpath (Code: 22)
32 number of peer(s) detected this updates for your prefix
     142.231.0.0/16:
Update details: 2009-01-03 02:10 (UTC)
Detected prefix: 142.231.0.0/17
Announced by: AS271 (BCNET-AS - BCnet)
Transit AS: 6509 (CANARIE-NTN - Canarie Inc)
ASpath: 1103 20965 6509 271
====================
```


Andree Toonk
andree@bgpmon.net

BGP mon

Monitor Prefix stability

Large number of withdraws for your prefix means reachability issues

Possible cause could be problem with:

- your border router
- your upstream
- large IX somewhere
- …..

Andree Toonk
andree@bgpmon.net

Monitor Prefix stability

BGPmon notification

```
From: BGPmon Alert <info@bgpmon.net>
To: andree.toonk@bc.net
Subject: BGPmon.net Notification

<..>
=====================================
Withdraw of Prefix (Code: 97)
=====================================
43 peer(s) detected this updates for your prefix 142.231.0.0/16
Update details: 2009-01-19 09:41 (UTC)
Detected prefix: 142.231.0.0/16
```


Andree Toonk
andree@bgpmon.net

BGP mon

ASpath monitoring

Flexible monitoring using regular expressions

- Useful for if you have many peers
- Useful when monitoring some specific traffic engineering situations.

  Example: $prefix may show behind ANY of my peers except $AS_Expensive

- Regular expression generator available

Andree Toonk
andree@bgpmon.net

BGP mon

Detecting Hijacks

Obvious hijacks

- Your prefix, but origin AS is not yours.
- YouTube hijack last year

```
========================================
Possible Prefix Hijack (Code: 10)
========================================
44 peer(s) detected this updates for your prefix 208.65.152.0/22:
Update details: 2008-02-24 18:48 (UTC)
Detected prefix: 208.65.153.0/24
Announced by: AS17557 (PKTELECOM-AS-AP Pakistan Telecom)
Transit AS: 3491 (PCCWGlobal-ASN)
ASpath:  26943 23352 3491 17557
```


Andree Toonk
andree@bgpmon.net

BGP mon

BGP MITM attacks

Not so obvious hijacks

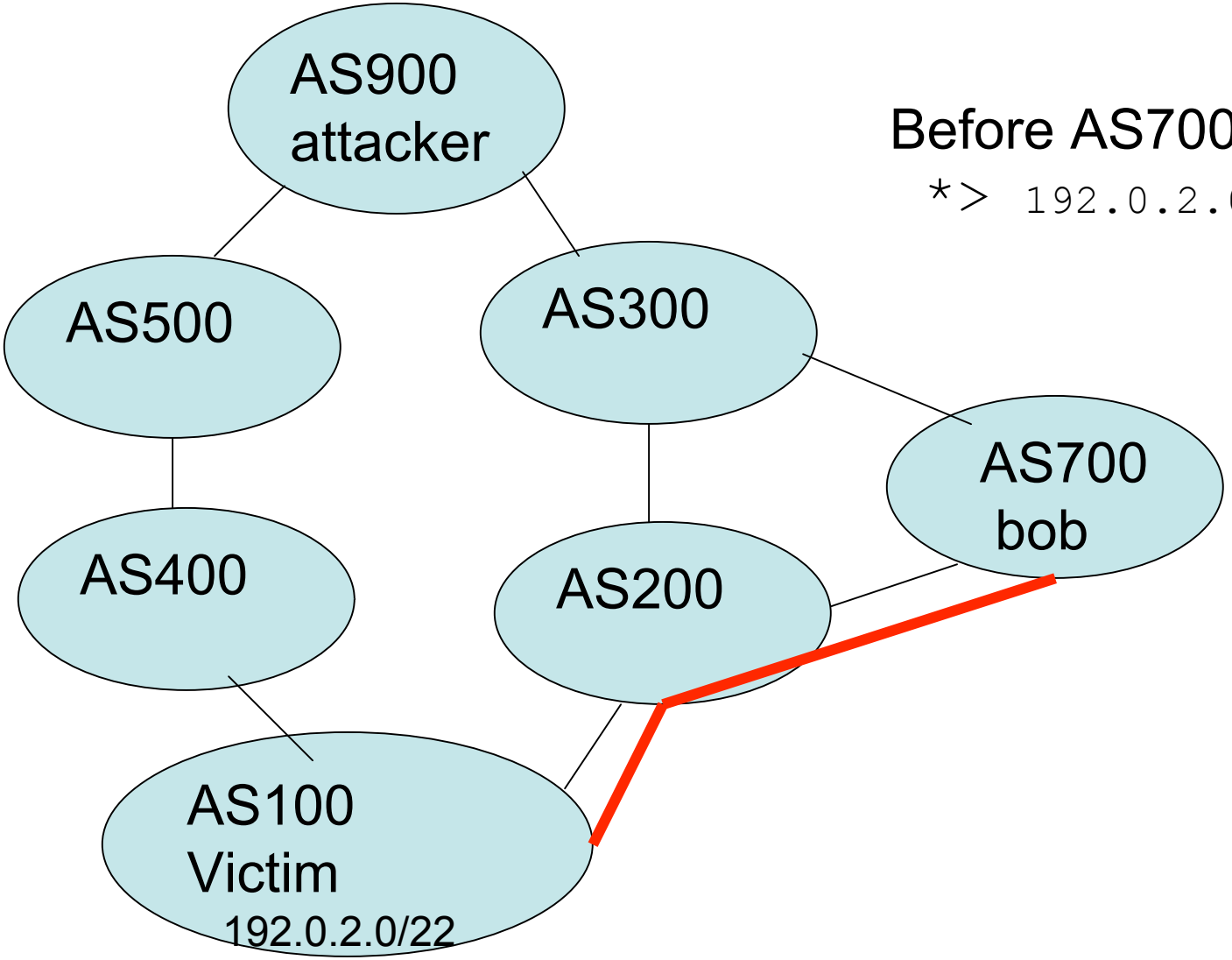
- As demonstrated at Defcon last summer ("Stealing the Internet")

Looks like:

- A more specific of your prefix.
- Looks like it's originated by your AS
- Result: looks like a 'regular' leak by my AS

Andree Toonk
andree@bgpmon.net

BGP MITM attacks

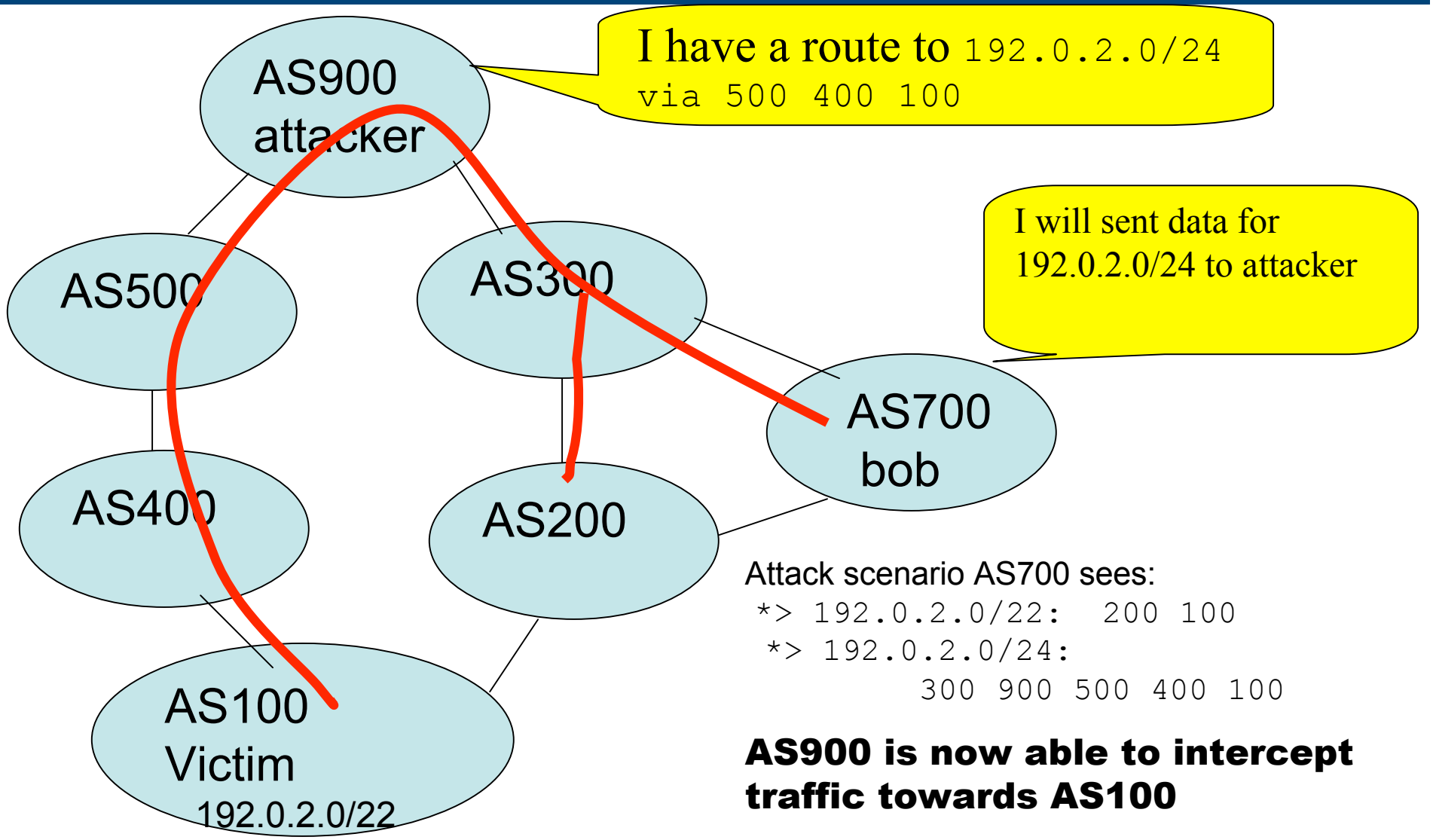


Before AS700 sees:

```
*>  192.0.2.0/22:   200 100
```


Andree Toonk
andree@bgpmon.net

BGP MITM attacks



Attack scenario AS700 sees:

```
*> 192.0.2.0/22:   200 100
 *> 192.0.2.0/24:
          300 900 500 400 100
```

AS900 is now able to intercept traffic towards AS100

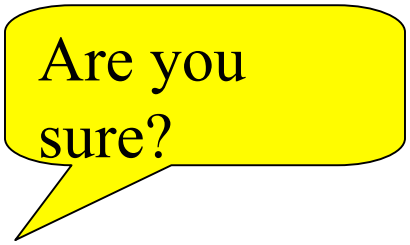
Andree Toonk
andree@bgpmon.net

BGP MITM attacks

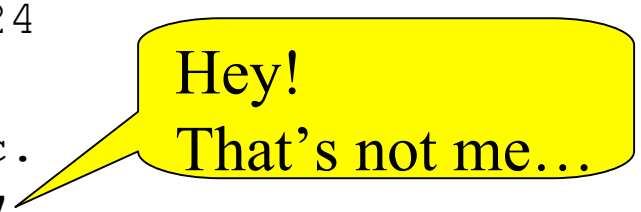
How can we detect an attack like this?

- More specific route
- New AS path

- Probably not a valid route object




```
whois -h whois.altdb.net  24.120.56.0/24
        route:      24.120.56.0/24
        origin:     AS26627
        descr:      Pilosoft, Inc.
        mnt-by:     MAINT-AS26627
        changed:    alex@pilosoft.com 20080425
        source:     ALTDB
```



Andree Toonk
andree@bgpmon.net

BGP MITM attacks

How can we detect an attack like this?

Let's rephrase that:

- More specific route
- New AS path
- No route object with me as maintainer and me as originAS

Andree Toonk
andree@bgpmon.net

BGP MITM attacks

```
========================================
More Specific with unknown ASpath (Code: 21)
========================================
16 peer(s) detected this updates for your prefix 24.120.56.0/22:
Update details: 2008-08-10 19:33 (UTC)
Detected prefix: 24.120.56.0/24
Announced by: AS20195 (SPARKLV-1 - Sparkplug Las Vegas, Inc.)
Transit AS: 23005 (SWITCH-COMMUNICATIONS)
ASpath: 24875 6461 3561 26627 4436 22822 23005 20195
```


Andree Toonk
andree@bgpmon.net

Resource Certification

To make sure that we can trust IRR data

- Resource Public Key Infrastructure Initiative (RPKI)
- Actively worked on by RIRs

  Beta implementation: certtest.ripe.net
- Digitally sign IRR data, such as route object:
  - Route Origination Authorization (ROA)

Andree Toonk
andree@bgpmon.net

BGP mon

Summary Alarm Classifications

Different alarm codes, for different events:

- 10 & 11 Origin AS change (hijack, private AS leak)
- 21 More specific with unknown AS path (Possible BGP MITM Attack)
- 22 more specific with known AS path (prefix leak)
- 31 change of upstream AS (filter failure)
- 41 regular expression mismatch (very flexible)
- 97 withdraw of prefix (instability)

Andree Toonk
andree@bgpmon.net

BGP mon

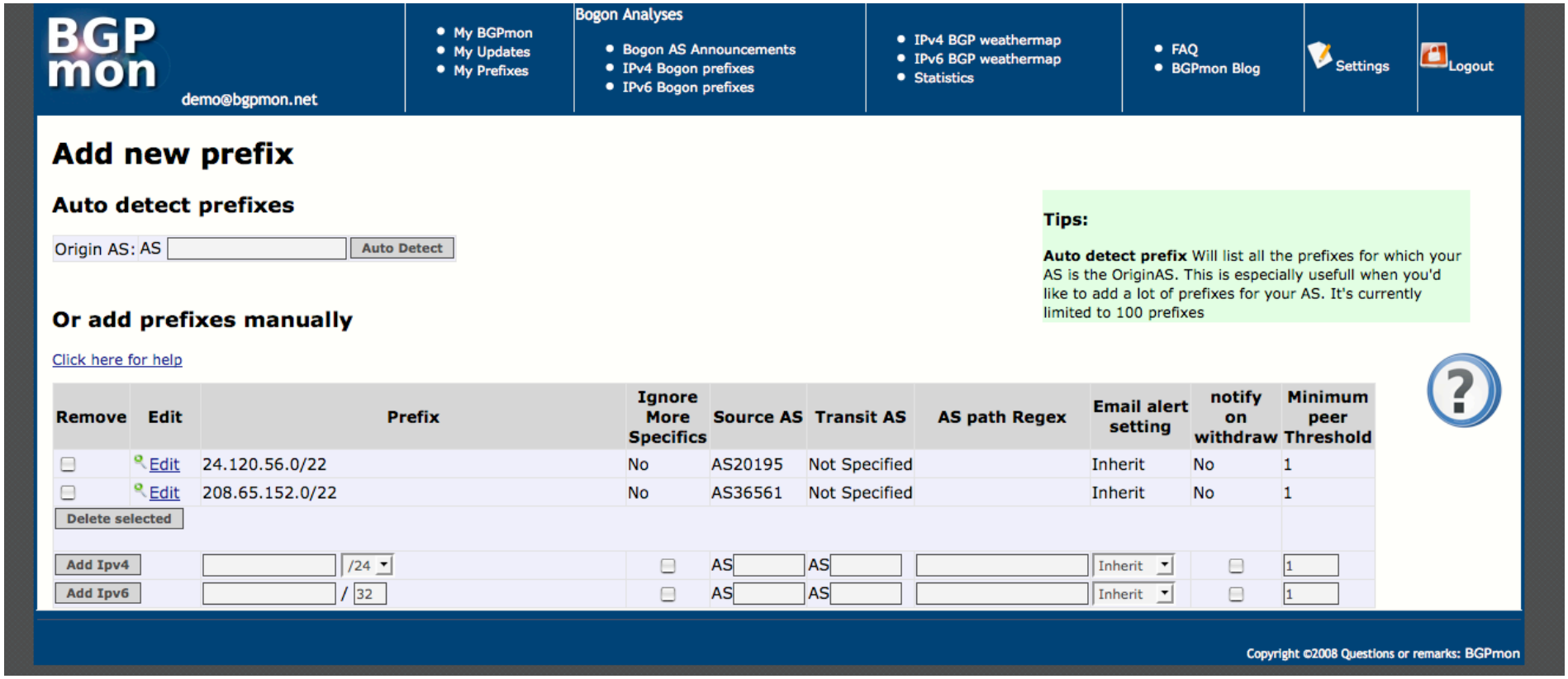
Customize notification

Per prefix settings for:

- Notification settings
- Peer threshold for updates
- Peer threshold for withdraws
- Ignore more specifics
- Regular expression
- Notify on withdraw

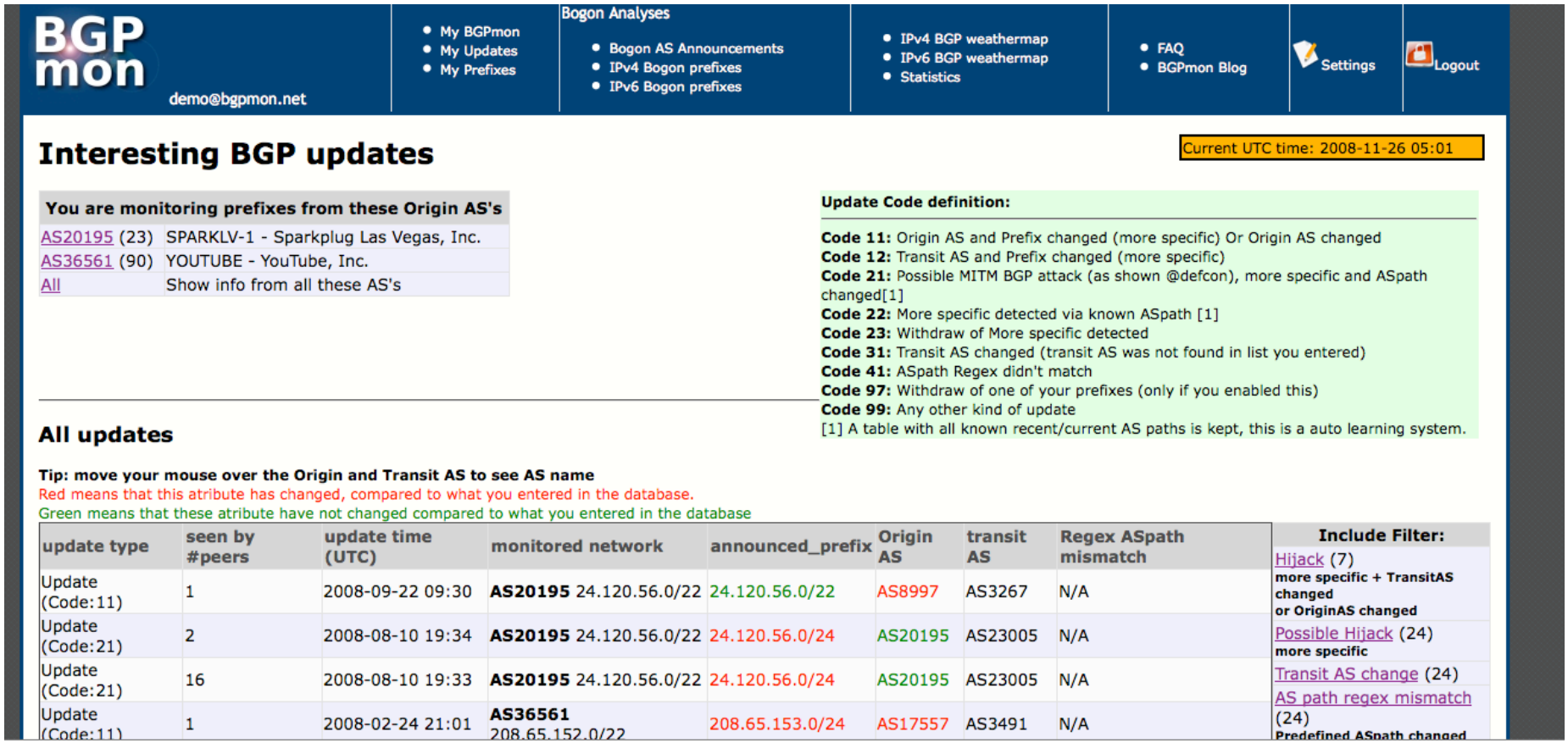
Andree Toonk
andree@bgpmon.net

My Prefixes



Andree Toonk
andree@bgpmon.net

My Updates



BGP mon

demo@bgpmon.net

- My BGPmon
- My Updates
- My Prefixes

Bogon Analyses

- Bogon AS Announcements
- IPv4 Bogon prefixes
- IPv6 Bogon prefixes

- IPv4 BGP weathermap
- IPv6 BGP weathermap
- Statistics

- FAQ
- BGPmon Blog

Settings Logout

Interesting BGP updates

Current UTC time: 2008-11-26 05:01

You are monitoring prefixes from these Origin AS's	
AS20195 (23)	SPARKLV-1 - Sparkplug Las Vegas, Inc.
AS36561 (90)	YOUTUBE - YouTube, Inc.
All	Show info from all these AS's

Update Code definition:

Code 11: Origin AS and Prefix changed (more specific) Or Origin AS changed
Code 12: Transit AS and Prefix changed (more specific)
Code 21: Possible MITM BGP attack (as shown @defcon), more specific and ASpath changed[1]
Code 22: More specific detected via known ASpath [1]
Code 23: Withdraw of More specific detected
Code 31: Transit AS changed (transit AS was not found in list you entered)
Code 41: ASpath Regex didn't match
Code 97: Withdraw of one of your prefixes (only if you enabled this)
Code 99: Any other kind of update
[1] A table with all known recent/current AS paths is kept, this is a auto learning system.

All updates

Tip: move your mouse over the Origin and Transit AS to see AS name
Red means that this atribute has changed, compared to what you entered in the database.
Green means that these atribute have not changed compared to what you entered in the database

update type	seen by #peers	update time (UTC)	monitored network	announced_prefix	Origin AS	transit AS	Regex ASpath mismatch	Include Filter:
Update (Code:11)	1	2008-09-22 09:30	**AS20195** 24.120.56.0/22	24.120.56.0/22	AS8997	AS3267	N/A	Hijack (7) **more specific + TransitAS changed or OriginAS changed**
Update (Code:21)	2	2008-08-10 19:34	**AS20195** 24.120.56.0/22	24.120.56.0/24	AS20195	AS23005	N/A	Possible Hijack (24) **more specific**
Update (Code:21)	16	2008-08-10 19:33	**AS20195** 24.120.56.0/22	24.120.56.0/24	AS20195	AS23005	N/A	Transit AS change (24)
Update (Code:11)	1	2008-02-24 21:01	**AS36561** 208.65.152.0/22	208.65.153.0/24	AS17557	AS3491	N/A	AS path regex mismatch (24) **Predefined ASpath changed**

Andree Toonk
andree@bgpmon.net

Customize

BGP mon

demo@bgpmon.net

- My BGPmon
- My Updates
- My Prefixes

Return to My Prefixes

Edit prefix 208.65.152.0/22

prefix	208.65.152.0/22
Ignore more specifics?	
Origin AS	AS 36561
Transit AS	AS Not Specified
Regular expression	
Email Level	Inherit
Notify on Withdraw	
Minimum peer Threshold (for updates)	1
Minimum peer Withdraw Threshold	3

Update

BGPmon.net Monitoring your prefixes

http://www.bgpmon.net/autoregex.php?prefix=208.65.152.0&length=22&originas=36561

Results for prefix 208.65.152.0/22

Your regex is:

```
(^|\s)(3549|9002|16150|174|15169|3356|19151|14361|6939|13030|7018|4589|7575|8359) 36561$
```

Your prefix:

208.65.152.0/22
OriginAS AS36561
YOUTUBE - YouTube, Inc.

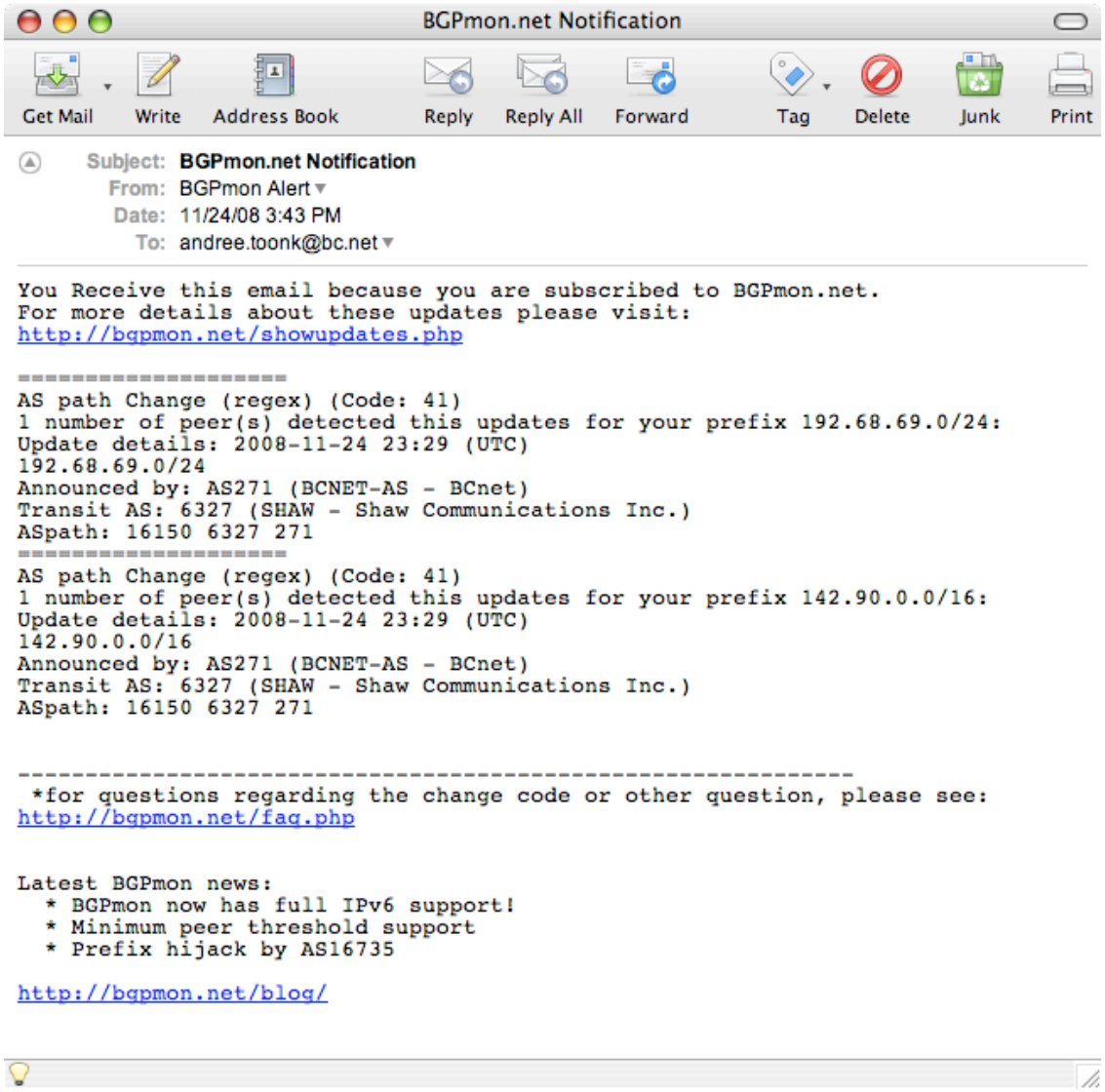
Your Upstream / Peering AS's (found 14):

Peering/upstream AS: AS3549 GBLX Global Crossing Ltd.
Peering/upstream AS: AS9002 RETN-AS ReTN.net Autonomous System
Peering/upstream AS: AS16150 PORT80-GLOBALTRANSIT Port80
Peering/upstream AS: AS174 COGENT Cogent/PSI
Peering/upstream AS: AS15169 GOOGLE - Google Inc.
Peering/upstream AS: AS3356 LEVEL3 Level 3 Communications
Peering/upstream AS: AS19151 WVFIBER-1 - WV FIBER LLC
Peering/upstream AS: AS14361 HOPONE-GLOBAL - HopOne Internet Corporation
Peering/upstream AS: AS6939 HURRICANE - Hurricane Electric, Inc.
Peering/upstream AS: AS13030 INIT7 Init Seven AG, Zurich, Switzerland
Peering/upstream AS: AS7018 ATT-INTERNET4 - AT&T WorldNet Services
Peering/upstream AS: AS4589 EASYNET Easynet Group Plc
Peering/upstream AS: AS7575 AARNET-AS-AP Australian Academic and Reasearch Network (AARNet)
Peering/upstream AS: AS8359 COMSTAR COMSTAR-Direct Moscow regior network

Done

Andree Toonk
andree@bgpmon.net

Alarm message



Andree Toonk
andree@bgpmon.net

BGP mon

Feedback!

- Thanks for all the feedback, bug reports and feature requests!
- Keep it coming, always looking to improve the system.
  - What else do you think is useful
  - How would you like to be notified?
    - RSS? SNMP traps? Syslog?

Andree Toonk
andree@bgpmon.net

BGP mon

Questions?

Andree@bgpmon.net

Try the demo @

http://BGPmon.net

Thanks *BCNET* & *University of British Columbia* for your support!

BCNET
The Backbone of Research, Education and Innovation

UBC