Network Explorations with Qrator Radar

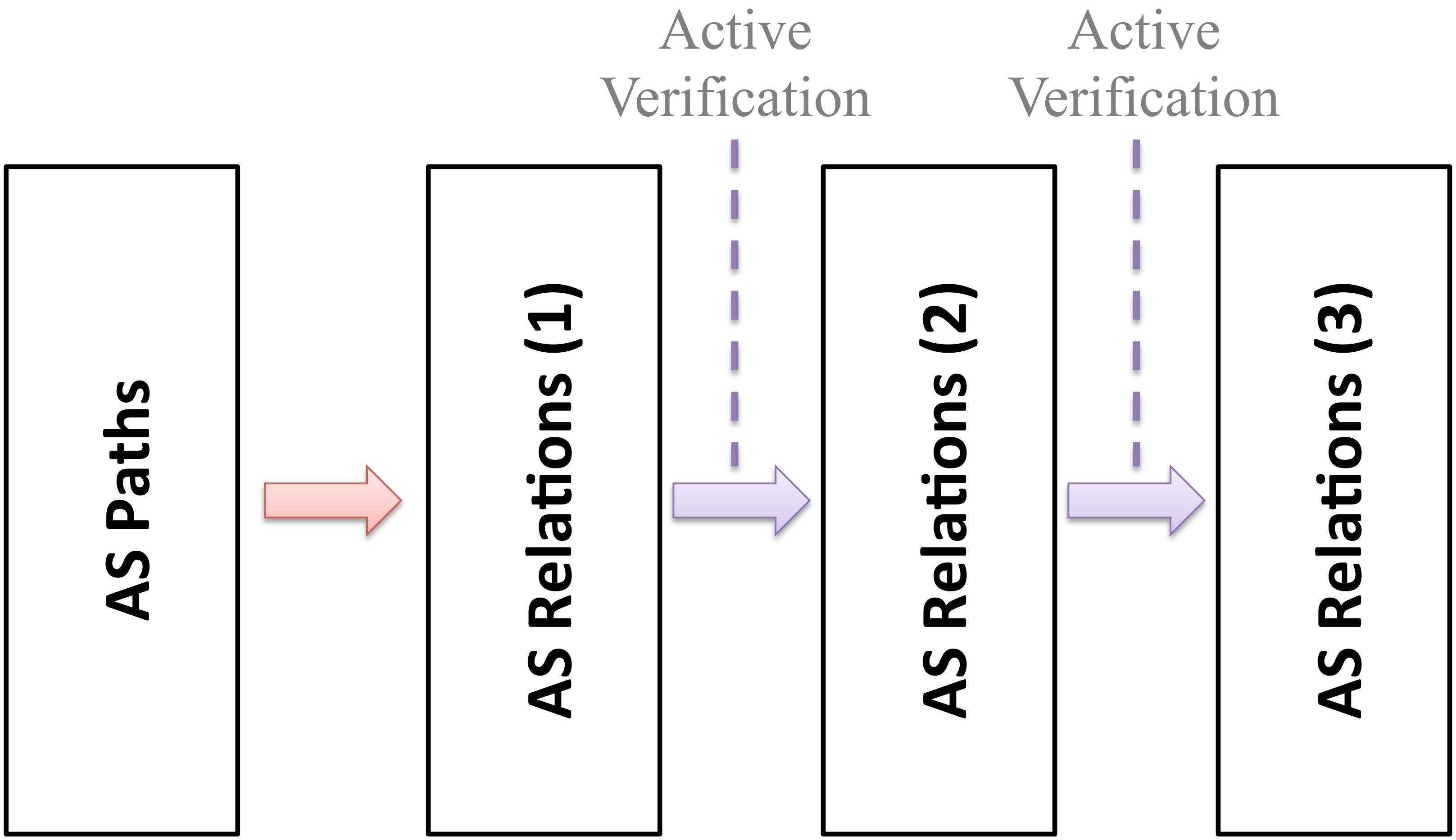
Alexnader Lyamin
<la@highloadlab.com>
Qrator Labs

Retrieving Route Policy

Common practices

1. Route Registries
   a. Outdated
   b. Incomplete
2. AS Paths
   a. Affected by route leaks
   b. No opportunity for paid peering detection

   Don’t cover lesser priorities



AS Paths

AS Relations (1)

Active Verification

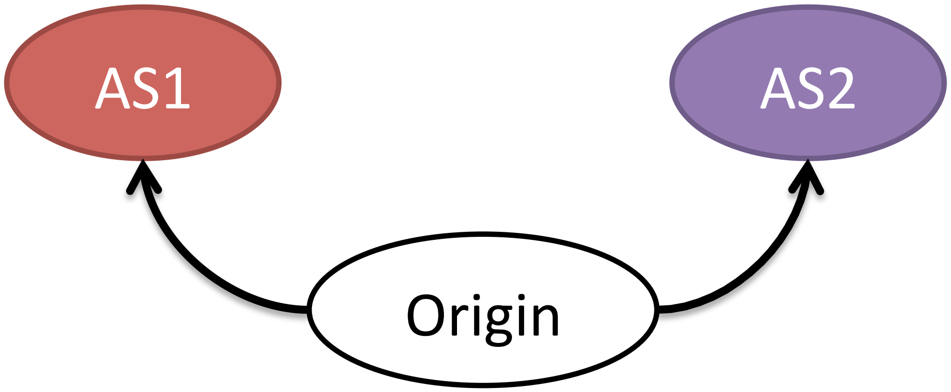
AS Relations (2)

Active Verification

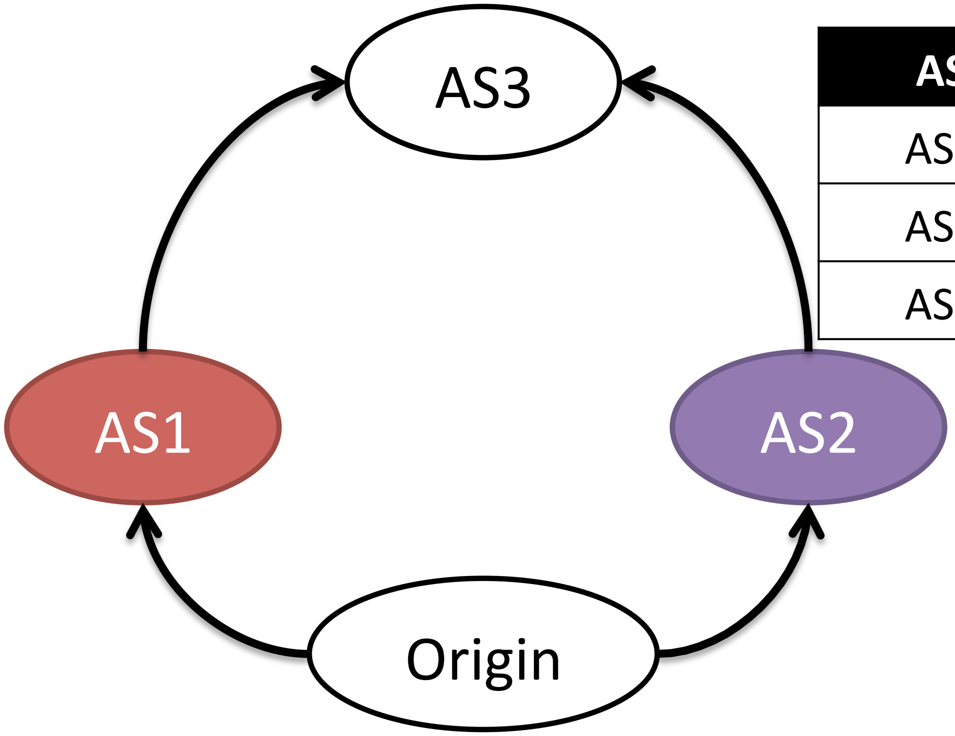
AS Relations (3)

Active Verification

AS	Next
AS1	Origin
AS2	Origin



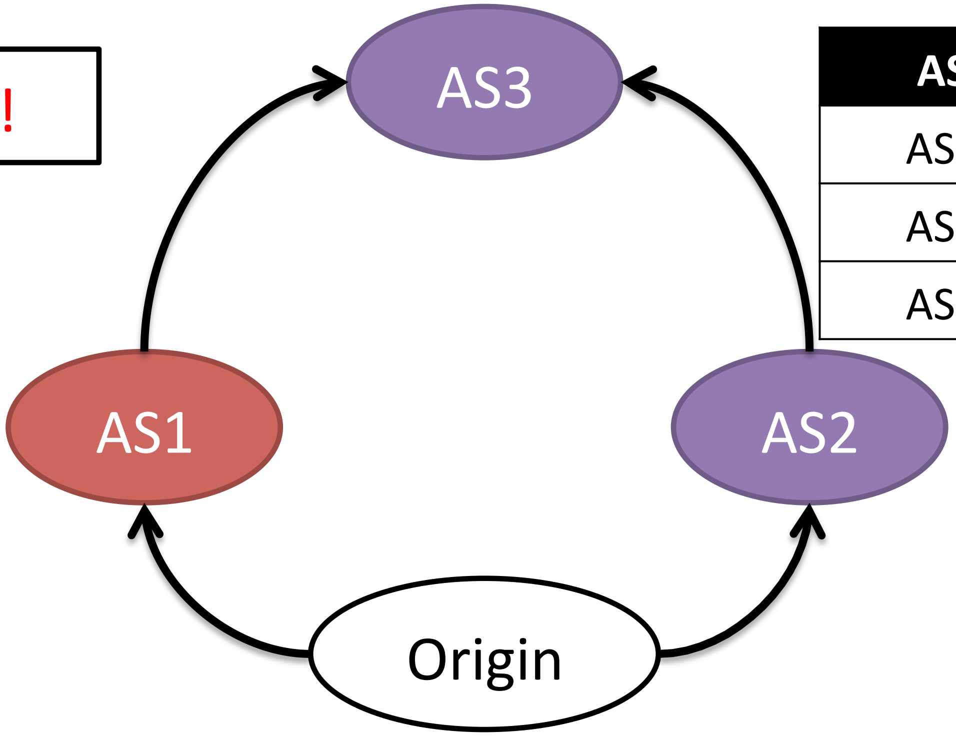
Active Verification



AS	Next
AS1	Origin
AS2	Origin
AS3	?

Active Verification

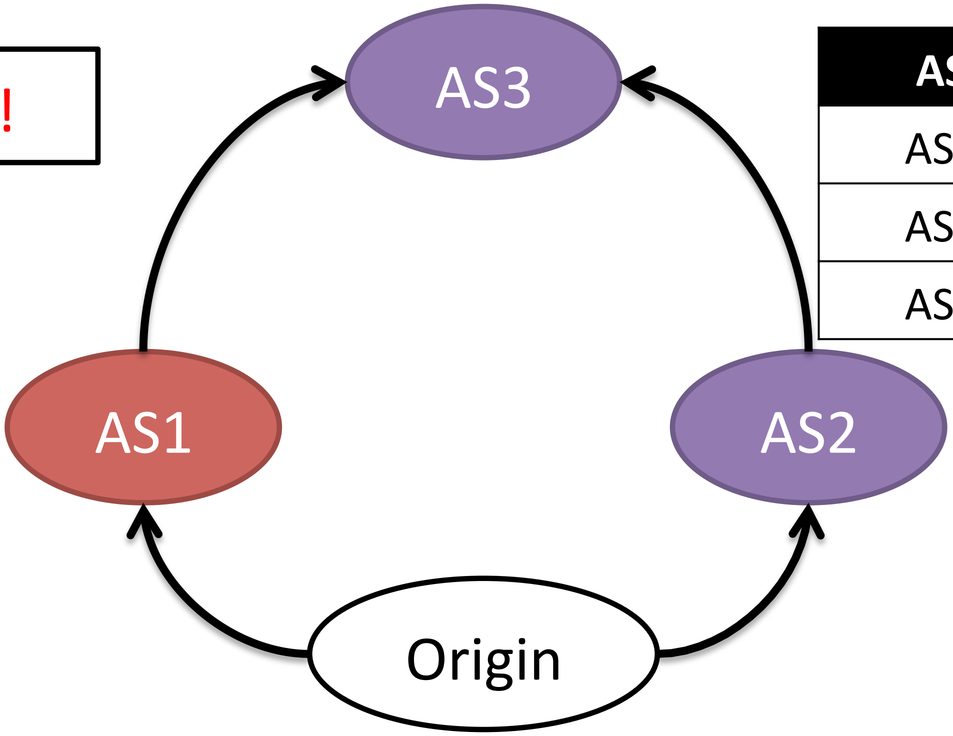
Ping it!



AS	Next
AS1	Origin
AS2	Origin
AS3	AS2

Active Verification

Ping it!



AS	Next
AS1	Origin
AS2	Origin
AS3	AS2

1. Cover AS graph Using Dijcstra algorithm;
2. Changing route policies at origin helps to detect more policies.

What is Qrator Radar?

AS Relations

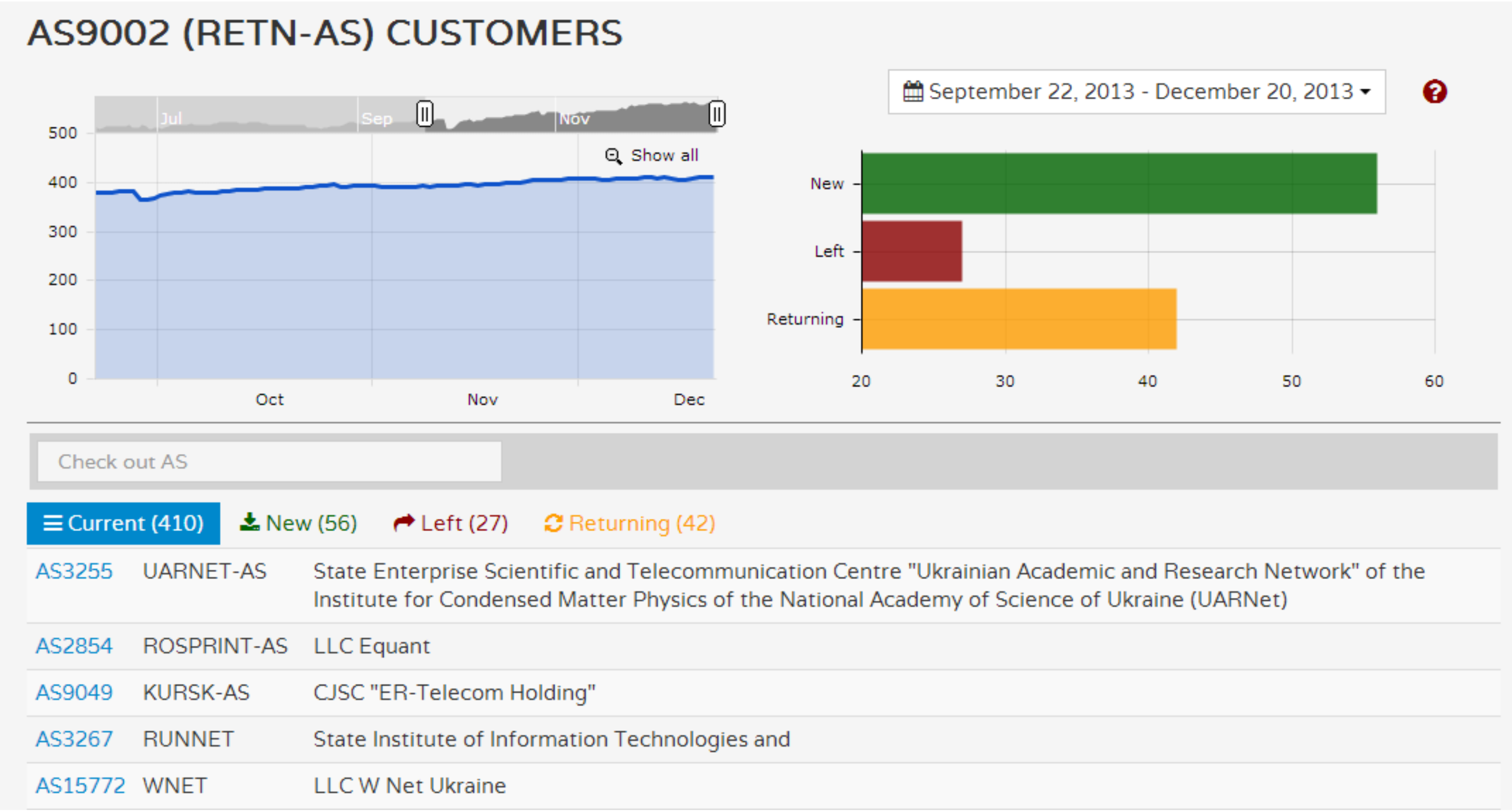
AS Design

Radar Monitor

AS Relations

1. AS Relations typing
2. Prepend policy prediction
3. Active verification
4. Priority at every level of BGP decision process

AS Relations



AS9002 (RETN-AS) CUSTOMERS

September 22, 2013 - December 20, 2013

Check out AS

☰ Current (410) | New (56) | Left (27) | Returning (42)

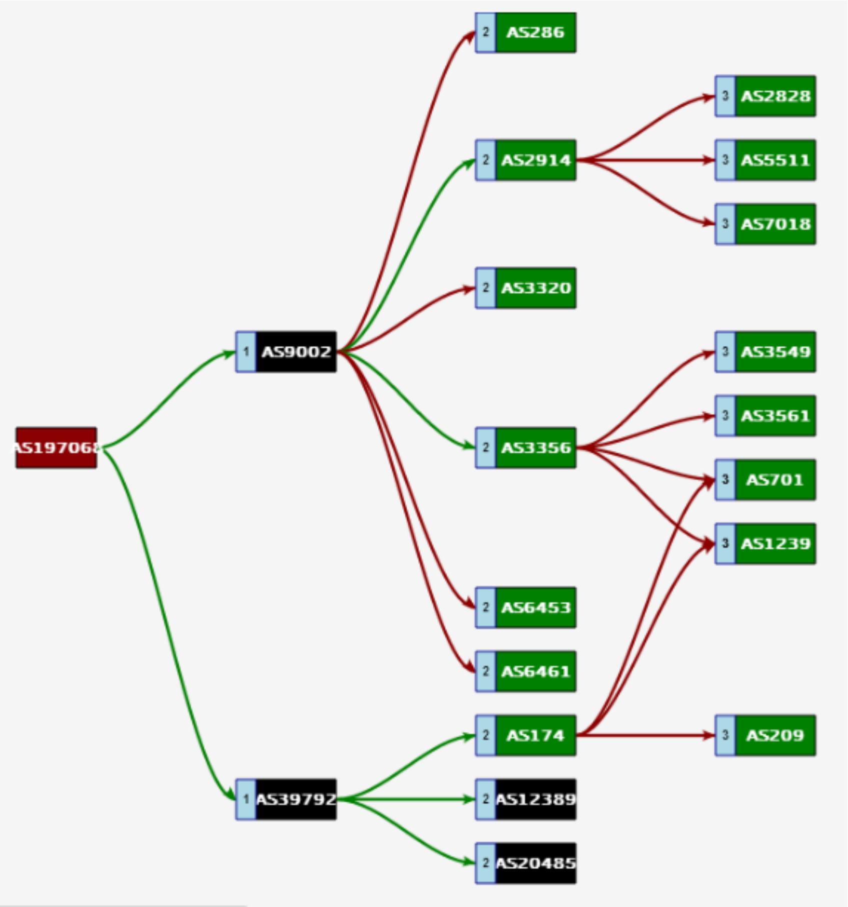
AS3255	UARNET-AS	State Enterprise Scientific and Telecommunication Centre "Ukrainian Academic and Research Network" of the Institute for Condensed Matter Physics of the National Academy of Science of Ukraine (UARNet)
AS2854	ROSPRINT-AS	LLC Equant
AS9049	KURSK-AS	CJSC "ER-Telecom Holding"
AS3267	RUNNET	State Institute of Information Technologies and
AS15772	WNET	LLC W Net Ukraine

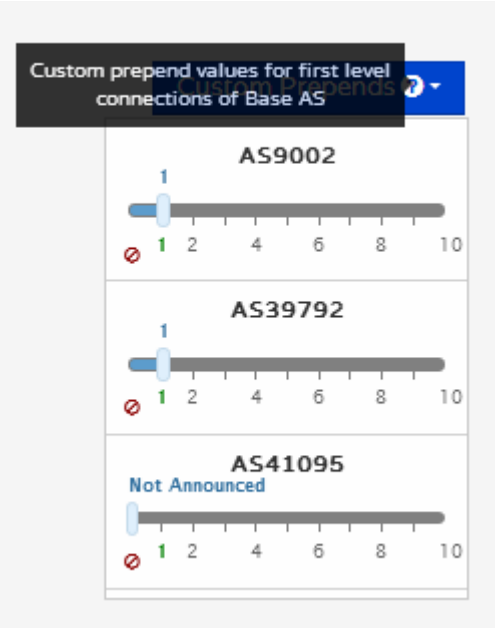
Peering, Customers, Providers

Qrator AS Graph

Path prediction instead of AS Path visualization.

BGP Route Prediction



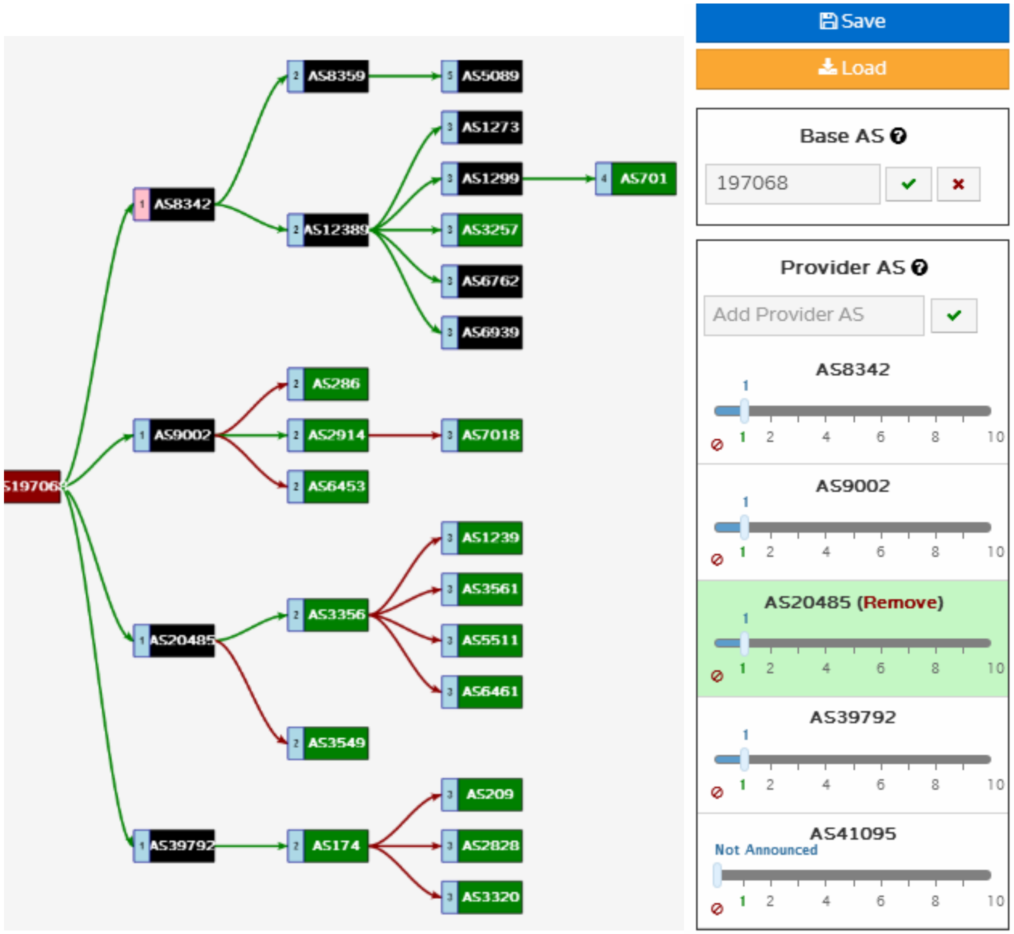

Custom prepend values for first level connections of Base AS

AS9002
1

AS39792
1

AS41095
Not Announced

AS Design



Base AS

197068 ✓ ✗

Provider AS

Add Provider AS ✓

AS8342

1

1 2 4 6 8 10

AS9002

1

1 2 4 6 8 10

AS20485 (Remove)

1

1 2 4 6 8 10

AS39792

1

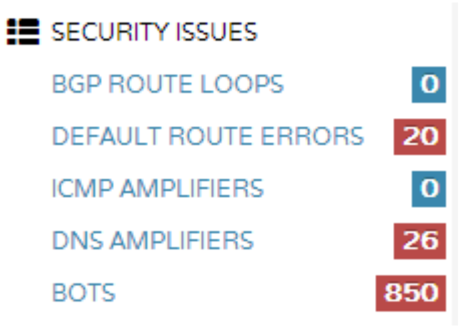
1 2 4 6 8 10

AS41095

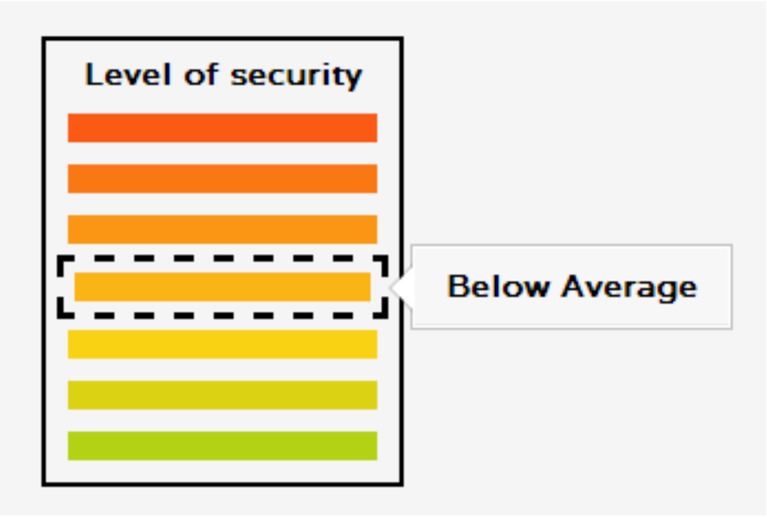
Not Announced

1 2 4 6 8 10

Security Issues

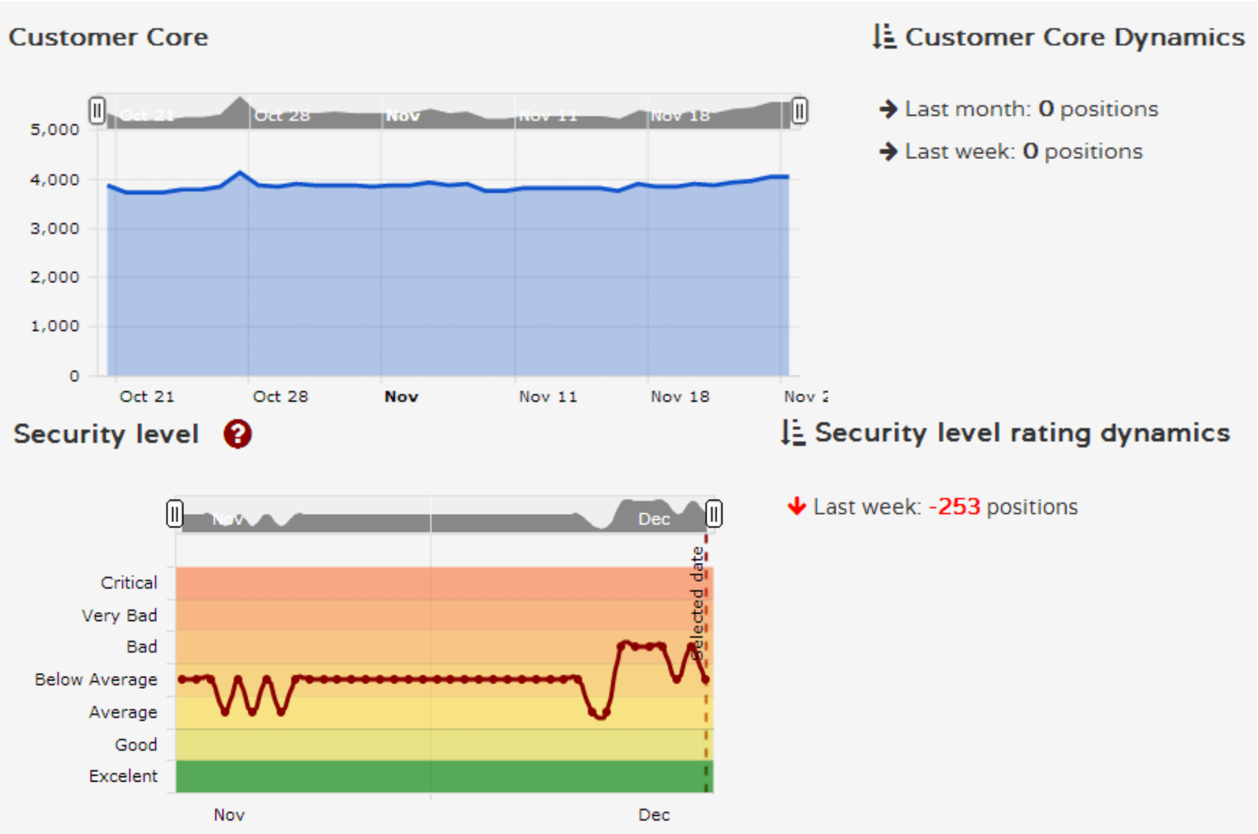


SECURITY ISSUES	
BGP ROUTE LOOPS	0
DEFAULT ROUTE ERRORS	20
ICMP AMPLIFIERS	0
DNS AMPLIFIERS	26
BOTS	850



Full disclosure is available after verification

Rates



Customer Core

Customer Core Dynamics

Last month: **0** positions

Last week: **0** positions

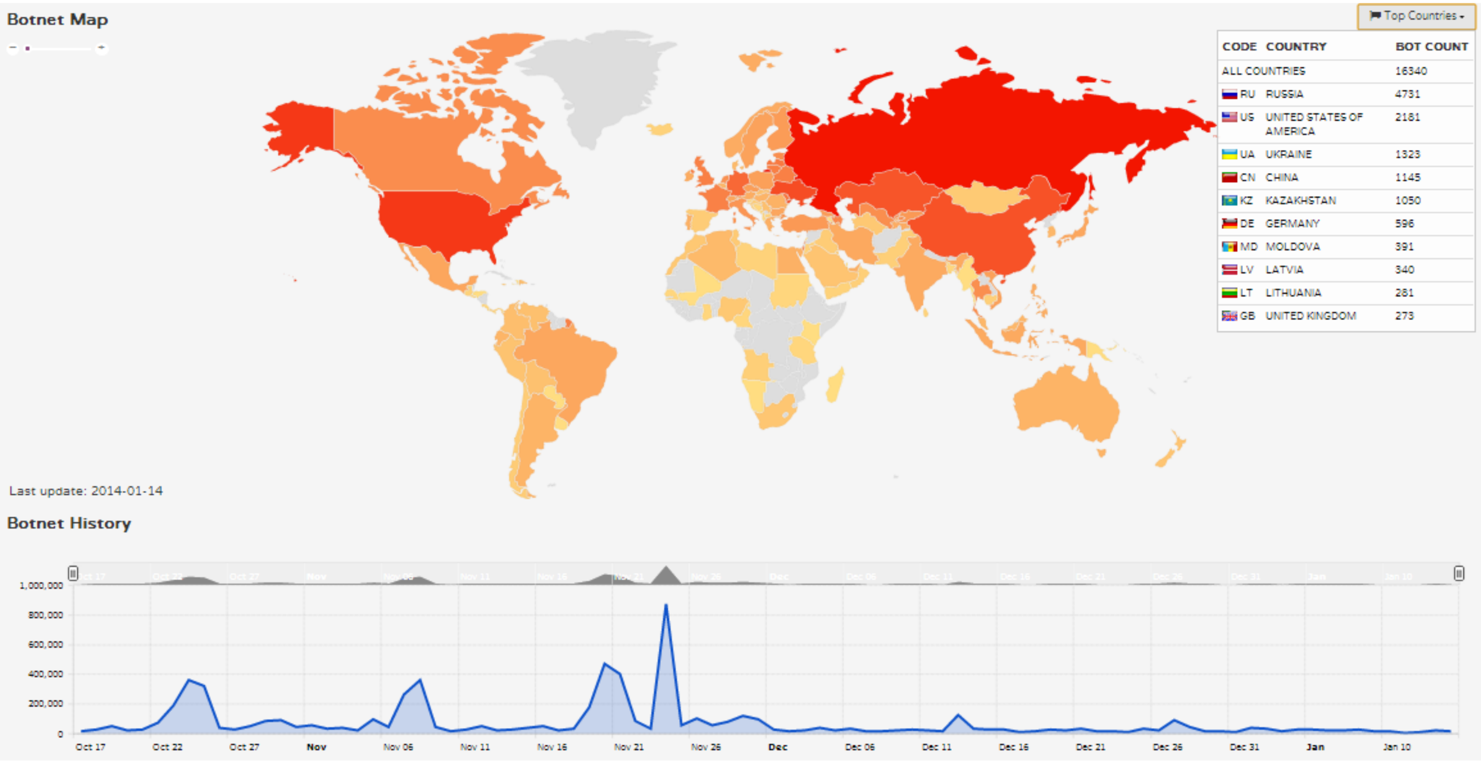
Security level

Security level rating dynamics

Last week: -253 positions

Daily updated

Botnet Activity Map



Botnet Map

CODE	COUNTRY	BOT COUNT
ALL COUNTRIES		16340
RU	RUSSIA	4731
US	UNITED STATES OF AMERICA	2181
UA	UKRAINE	1323
CN	CHINA	1145
KZ	KAZAKHSTAN	1050
DE	GERMANY	596
MD	MOLDOVA	391
LV	LATVIA	340
LT	LITHUANIA	281
GB	UNITED KINGDOM	273

Last update: 2014-01-14

Botnet History

We are looking forward…

1. Your feedbacks!
2. Your feature requests
3. BGP sessions with our reflector

We are planning…

1. Reverse Looking Glass
2. Notification for security issues
3. API

Questions?

https://radar.qrator.net