APNIC: Solving problems for our community

Sofía Silva Berenguer
Information Services Product Manager
sofia@apnic.net
A bit about me

• I started my journey in the RIR world working as a Hostmaster and Policy Officer at LACNIC in August 2010

• I then had some technical roles:
  – Networks and Security Engineer
  – Senior Security and Stability Engineer

• I started working with APNIC as a Data Scientist more than 2 years ago

• I’ve always suffered from Impostor Syndrome
Agenda

• Information Services Product family:
  – DASH (Dashboard for Autonomous System Health)
  – NetOX (Network Operators tool boX)
DASH (Dashboard for AS Health)

- Dashboard for resource holders that shows **information about malicious traffic** seen by our honeypots originated at IP addresses managed by the user.

- Currently just a prototype:
  - Only showing information about SSH attacks.
  - More features pending to be implemented.

- Short video available: [https://dash.apnic.net/about](https://dash.apnic.net/about)

- Preparing soft launch with set of Members who would find interesting info in the current version of the product.
My dashboard

My network
Total attacks in JUL 2.1K
Total attacks in JUN 2.1K

Compared to previous month 0.3%

VN
Total attacks in JUL 17.3K
Total attacks in JUN 24.1K

Compared to previous month 28.3%

South-Eastern Asia
Total attacks in JUL 23.3K
Total attacks in JUN 27.5K

Compared to previous month 15.0%

Number of attacks seen from my network compared to VN

<table>
<thead>
<tr>
<th>VN</th>
<th>South-Eastern Asia</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Daily totals of attacks seen coming from testASN compared to VN

<table>
<thead>
<tr>
<th>Date</th>
<th>My network</th>
<th>VN</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1K</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
My dashboard

Number of attacks seen from my network compared to VN

VN  South-Eastern Asia

Daily totals of attacks seen coming from testASN compared to VN
# My dashboard

My network top 10 offending prefixes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Attack types</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.51.100.0/24</td>
<td>SSH</td>
<td>1055</td>
</tr>
<tr>
<td>10.183.93.0/24</td>
<td>SSH</td>
<td>683</td>
</tr>
<tr>
<td>10.118.0.0/20</td>
<td>SSH</td>
<td>135</td>
</tr>
<tr>
<td>192.0.2/20</td>
<td>SSH</td>
<td>63</td>
</tr>
<tr>
<td>198.51.100.0/20</td>
<td>SSH</td>
<td>57</td>
</tr>
<tr>
<td>10.210.0.0/21</td>
<td>SSH</td>
<td>35</td>
</tr>
<tr>
<td>10.118.16.0/20</td>
<td>SSH</td>
<td>18</td>
</tr>
<tr>
<td>10.210.12.0/21</td>
<td>SSH</td>
<td>13</td>
</tr>
<tr>
<td>10.118.32.0/20</td>
<td>SSH</td>
<td>10</td>
</tr>
<tr>
<td>10.74.120.0/22</td>
<td>SSH</td>
<td>6</td>
</tr>
</tbody>
</table>
I’ve received an alert from APNIC DASH: 20% of my IPv4 addresses have been seen sending malicious traffic!

It seems two of the networks we use for corporate customers may have devices infected with malware. I’ll talk to them to get their networks checked.

I better check which prefixes may be compromised.

(Logs in to DASH)
NetOX (Network Operators ToolbOX)

• Set of tools that helps network operators interact with other networks
  – Solving routing issues
  – Deciding which other networks to connect to

• Working in collaboration with the RIPE NCC

• Currently RIPEstat with an APNIC ‘look & feel’

• Available at: https://netox.apnic.net
Search Internet Number Resources

This is APNIC’s Network Operators ToolbOX, powered by RIPE NCC’s RIPEstat. It is currently just a prototype. If you have any questions or comments, please reach out to us at feedback@apnic.net

Search...
AS Overview (AS4608)

Routing information (RIS)
✔️ Originates prefixes visible
✔️ Is seen in other routes

Name and holder of this ASN:
APNIC-SERVICES Asia Pacific Network Information Centre

<table>
<thead>
<tr>
<th>RIR</th>
<th>Status</th>
<th>Registration</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>APNIC</td>
<td>ALLOCATED</td>
<td>1995-05-30</td>
<td>AU</td>
</tr>
</tbody>
</table>

Show IANA Registry Information

Whois Matches (AS4608)

Whois results (1)

<table>
<thead>
<tr>
<th>aut-num</th>
<th>as-name</th>
<th>descr</th>
</tr>
</thead>
<tbody>
<tr>
<td>4608</td>
<td>APNIC-SERVICES</td>
<td>Asia Pacific Network Information Centre</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regional Internet Registry for the Asia-Pacific Region</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 Cordelia Street</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PO Box 3646</td>
</tr>
<tr>
<td></td>
<td></td>
<td>South Brisbane, QLD 4101</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Australia</td>
</tr>
<tr>
<td></td>
<td>country</td>
<td>AU</td>
</tr>
<tr>
<td></td>
<td>org</td>
<td>ORG-APNII-AP</td>
</tr>
<tr>
<td></td>
<td>mnt-by</td>
<td>APNIC-HM</td>
</tr>
</tbody>
</table>

Routing registries results (0)

Showing results for AS4608 as of 2019-05-19 16:00:00 UTC

Showing results for AS4608 as of 2019-05-20 01:35:00 UTC
NetOX in the future

• Exploring how to implement features to solve validated problems:
  – Bringing points of contact and other data (?) from PeeringDB
  – Easily visualizing upstream providers for a given ASN
  – Bringing data from IRRs, for automation of route filters

• Exploring idea of creating shared knowledge base for network operators
I’m considering hiring a new upstream provider. I wonder how well interconnected AS 4608 is??

They probably offer good robustness as they have three providers.
I’m having some routing issues. AS 4608 seems to be filtering one of my prefixes.

I’ve tried contacting the WHOIS PoC but they were not very responsive.

There must be a better contact for this type of issue.
I’m getting 27.100.7.0/24 transferred. I wonder if this prefix is clean.

It looks like this prefix is already in use!

And it has been routed for quite a long time!
NetOX – Use Case

Uhmmm It hasn’t been assigned by APNIC yet.

This prefix is a bogon!
NetOX – Use Case

And it’s in a blacklist!

This prefix is definitely not clean!

Yoshi

“I run the net”
Summary

• We are working on products to offer info to network operators
  – DASH (Dashboard for AS Health)
  – NetOX (Network Operators toolboX)

• We want to hear FROM YOU!
  – Do you see value in these products?
  – Do you want to provide any feedback?
  – Do you want to participate in interviews, testing sessions, etc.?
THANK YOU