renesys

Detecting Attacks on Internet Infrastructure and Monitoring of Service Restoration in Real Time

Andy Ogielski

FCC Workshop on Cyber Security

30 September 2009

Threats to Internet Infrastructure

- Focus on threats to **Internet Infrastructure** – as opposed to threats to end systems (viruses, malware, fraud, data exfiltration, etc).
- The state of the Internet Infrastructure can be continuously measured – on the national and global scale.
- Response and restoration require accurate “who is who” directories and maps of network owners and operators.
- Objective metrics and scores can track compliance with policies and reliability goals.

renesys

Internet Connectivity Threats

Poorly understood by cyber security community

- **Physical problems**

  (Physical Infrastructure: Natural, accidental or intentional destruction)

  - Earthquakes, Anchors/Backhoes, Hurricanes, Bombs

- **Routing Vulnerabilities**

  (Logical Infrastructure: if routers do not direct traffic correctly, Internet is broken)

  - Insecure BGP Routing Protocol, Misconfigurations, Bugs, Exploits

- **Business Conflicts**

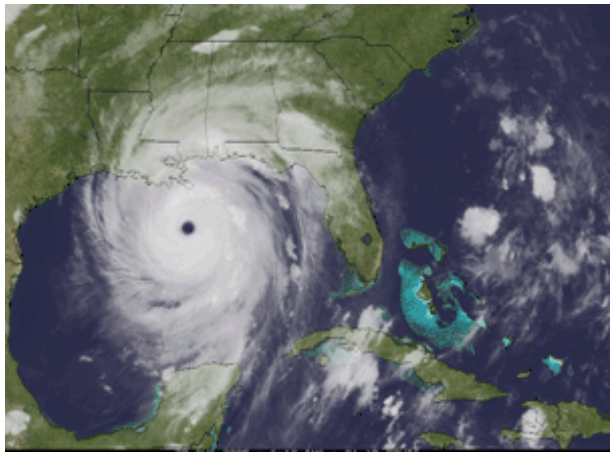
  (Competing providers can refuse to exchange their customers' traffic - depeerings)

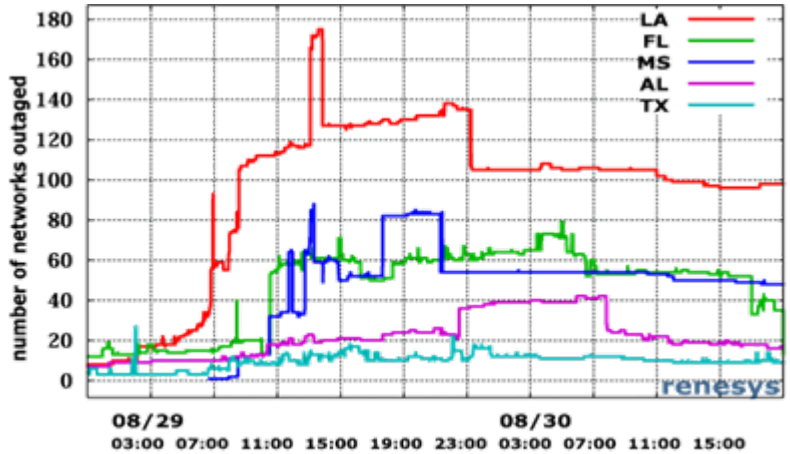
  - Recent depeerings between certain tier-1 providers left thousands of their "captive" customers without capability of connecting to one another – partitioning of the Internet.

renesys

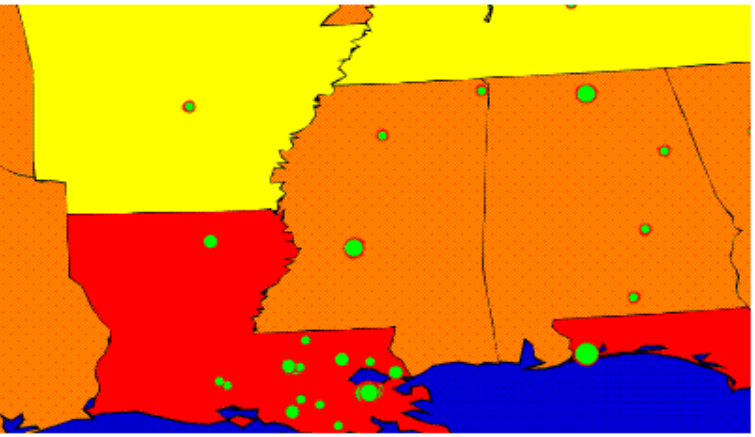
The state of the Internet can be monitored at all times

Outages and restoration data can be tracked with precision





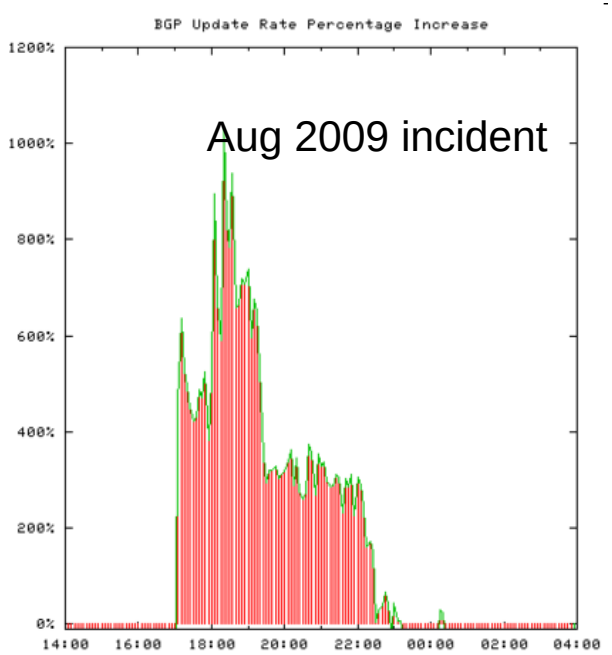
Mississippi Report: Network Outages over the past 2 hours

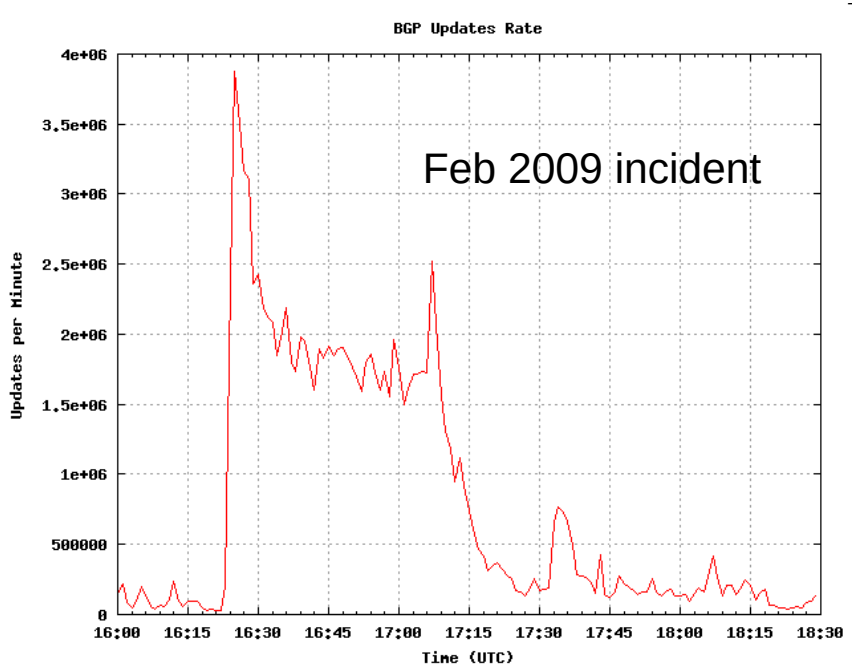


19:33:53 UTC 08 Sep 2005

Country	Network	State	Zip
	CommuniGroup of Jackson MS MS 39201 (65.183.96.0/20)	MS	39201
	WATER VALLEY INTERCHANGE MS 38965 (64.49.18.0/24)	MS	38965
	TriState Education initiative MS 38852-4375 (192.149.138.0/24)	MS	38852-4375
	Arch Communications MS 39157 (208.251.18.0/24)	MS	39157
	AIR2LAN Inc MS 39216 (216.212.214.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.215.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.216.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.217.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.218.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.219.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.220.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.221.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.222.0/24)	MS	39216
	AIR2LAN Inc MS 39216 (216.212.223.0/24)	MS	39216

Recorded incidents illustrate the potential of cyber attacks





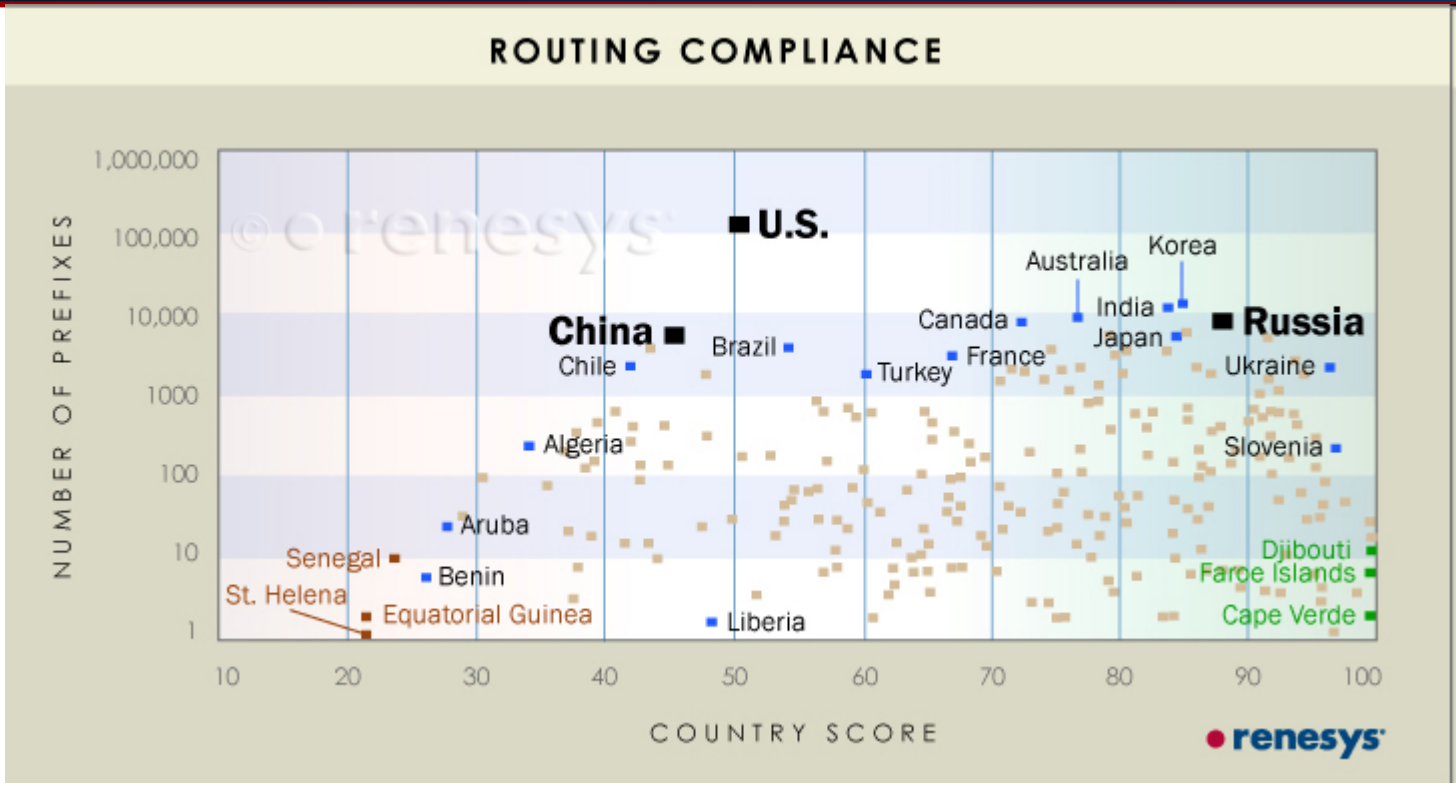
Spread of malformed router-to-router messages triggers worldwide failures of certain router models until the culprits recognize their error & turn the box off.

A single “bad” router can cause 10-fold routing instability increase, globally, in minutes...

Many worse incidents on record: False routes can be injected, traffic hijacked.

renesys

Objective metrics can measure compliance with policies



Example metric - based on continuous measurements - for quantifying the agreement between officially registered routing policies and actually observed routing for every network prefix in every country.

renesys

Internet Connectivity Threats

Trends & Prognosis

- **Physical problems**

  (Physical Infrastructure: Natural, accidental or intentional destruction)

  - Earthquakes, Anchors/Backhoes, Hurricanes, Bombs
  - **Prognosis is improving. Need bandwidth & constant attention.**

- **Routing Vulnerabilities**

  (Logical Infrastructure: if routers do not direct traffic correctly, Internet is broken)

  - Insecure BGP Routing Protocol, Misconfigurations, Bugs, Exploits
  - **Best we can do now is monitor and respond quickly.**
  - **Prognosis is dismal. Need a manageable path to secure routing.**

- **Business Conflicts**

  (Competing providers can refuse to exchange traffic - depeerings)

  - **Prognosis is improving. Measure diversity within Internet provider markets. Consider defining "too big to fail."**

renesys

Additional Information

More examples of infrastructure vulnerabilities and ways to address them at **www.renesys.com**