Global Routing Instabilities
during Code Red 2 and Nimda Worm Propagation

Jim Cowie and Andy Ogielski
Renesys Corporation

17 December 2001
Abstract

We review our recent discovery of the unexpected impact of Microsoft worm propagation (Code Red II and Nimda) on the stability of the global routing system.

Joint analysis of the archived BGP message streams from 150+ BGP routers (from the RIPE-NCC Routing Information Service) and of the worm attack packet traces shows large and long-lasting “BGP storms" induced by worm propagation.

We present preliminary results concerning the mechanisms by which the worm traffic may cause multiple router failures and destabilize the BGP routing system.

We also present another kind of global routing instabilities triggered by common router misconfigurations.

Outline

Catastrophic instabilities are an expected behavior of large engineered systems (John Doyle, Caltech)

1. **Define** global routing instability

2. **Analyze** raw BGP message traffic from 150+ peers (all RIPE RRCs).

3. **Paint** a picture of instabilities caused by:

   - Microsoft worms
   - router misconfigurations
   - .....?
**Focus: RIPE rrc00 collection point**

EBGP peers from around the world

<table>
<thead>
<tr>
<th>AS</th>
<th>peer IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>13129</td>
<td>Global Access</td>
</tr>
<tr>
<td>1103</td>
<td>SURFnet</td>
</tr>
<tr>
<td>513</td>
<td>CERN</td>
</tr>
<tr>
<td>3333</td>
<td>RIPE NCC</td>
</tr>
<tr>
<td>286</td>
<td>KPN Qwest</td>
</tr>
<tr>
<td>4777</td>
<td>APNIC Tokyo Servers</td>
</tr>
<tr>
<td>9177</td>
<td>Nextra</td>
</tr>
<tr>
<td>4608</td>
<td>Telstra</td>
</tr>
<tr>
<td>3257</td>
<td>Tiscali</td>
</tr>
<tr>
<td>3549</td>
<td>Global Crossing UK</td>
</tr>
<tr>
<td>3549</td>
<td>Global Crossing USA</td>
</tr>
<tr>
<td>2914</td>
<td>Verio</td>
</tr>
<tr>
<td>7018</td>
<td>AT&amp;T Internet4</td>
</tr>
</tbody>
</table>
Errors & anomalies in raw zebra BGP data (RIPE, Oregon):

prefiltering needed

- decreasing timestamps – clock shifts
- corrupted MRT headers
- truncated BGP messages
- peers opening/closing sessions
Errors & anomalies in raw zebra data:
Periodic update logging failures

Eight Hour Prefix Withdrawal History at Oregon Routeviews

13 December 2001
BGP message traffic rate

received by a single BGP router from 12 major peers.

Analysis at message level does not reveal very much.

Must analyze content.
A view on content of the same messages

Number of prefix announcements in 30 sec intervals

September 18:
Notice over 20-fold exponential growth
returning back to baseline after 4 days!
Analysis exposes correlations:

Behavior across...

- peers
- peering points
- origin ASs
- prefixes
- prefix length
- route lifetimes
Prefix announcements by peer

RIPE NCC, September 10 - 22, 15-min intervals

September 18:

Long-tail wave of routing instabilities in BGP message streams from major Internet providers

Each row = time series of # of prefixes announced by one rrc00 peer
September 18 Nimda worm attack

exponential spread

port 80 SYNs

unique attacker IPs
Nimda probes burn routers’ CPU cycles...

Inset plot shows highly correlated router cpu utilization ... in a different net
September 18 BGP event correlates in time with Nimda worm attack

Smaller events: leakage of reserved AS numbers
# Global Internet Routing Instabilities

## Qualitative definition

<table>
<thead>
<tr>
<th>rate</th>
<th>duration</th>
<th>diversity</th>
</tr>
</thead>
<tbody>
<tr>
<td>High rates of route changes:</td>
<td>Very long times:</td>
<td>Seen at many observation points:</td>
</tr>
<tr>
<td>• magnitude</td>
<td>• long relative to baseline noise</td>
<td>• many external BGP peers</td>
</tr>
<tr>
<td>• acceleration</td>
<td>• long relative to expected routing table convergence time</td>
<td>• many exchanges</td>
</tr>
<tr>
<td>• variance</td>
<td></td>
<td>• Intra-AS networks</td>
</tr>
</tbody>
</table>

Seen in high diversity of routing traffic content:
- number of prefixes
- number of routes
One peer unstable: not a global instability

October 20 rrc00 announcements– AS 1103 unstable
## Global Internet Routing Instabilities

**operational definition**

<table>
<thead>
<tr>
<th>rate</th>
<th>duration</th>
<th>diversity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exponential growth of rate of prefix announcements and withdrawals</td>
<td>Hours to days</td>
<td>• almost all prefixes churning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• from most large ISP peers</td>
</tr>
</tbody>
</table>
Worm story # 2:
Code Red v2 attack
prefix announcement rate in 30 sec intervals

July 19:
Notice 10-fold exponential growth
returning back to baseline after 16 hours
July 19 Code Red II worm attack

Worm attack on a /16
exponential spread
port 80 SYNs
unique attacker IPs
July 19 BGP storm correlates in time with Code Red II worm attack
Results of detailed analysis:

Nimda and Code Red triggered long-term BGP instabilities unlike any localized network failure:

- **no suspect peers** – all major peers
- **no suspect prefixes** – most prefixes churn
- **no suspect routes** – most routes churn
Look for behavior across prefixes
Prefixes seen for A’dam IX July 19 busiest hour
Prefixes seen for A’dam IX July 7 slow hour
Polar coordinates for IP prefixes

"bulls-eye" view of the distribution of prefixes:
graphically represents the fragmentation of the entire IP address space (2^32 addresses) into BGP-announced networks.

In the plot the prefix a.b.c.d/p is represented by a small arc.
The polar coordinates of the arc are:

radius = prefix length p

\[
\text{start angle } \phi_1 = \frac{\text{int value of the lowest IP address in prefix}}{2^{32}} \times 360 \text{ deg}
\]

\[
\text{end angle } \phi_2 = \frac{\text{int value of the highest IP address in prefix}}{2^{32}} \times 360 \text{ deg}
\]
167k legit prefixes seen at RIPE RRC in July ‘01
Prefix counts: July 19 busiest hour  AMS-IX RRC
Prefix counts: July 7 slow hour  AMS-IX RRC
Look for route withdrawals by prefix length
Hourly prefix withdrawals, Code Red: July 19-20, rrc00
Hourly prefix withdrawals, Nimda: September 18-19, rrc00
Look for route lifetimes
July 19: Histogram of route lifetimes
Red: July 19 heavy BGP traffic, updates from each peer come every 30 sec (MRAI).

Blue: July 7 slow BGP traffic – often no updates to send for over 30 sec.

However, **qualitative distribution of route lifetimes is similar.**
worm-induced BGP instabilities

Do not look like effects of link failures between multiply-connected major Internet providers (Internet core).

Cable cuts, Baltimore tunnel fire, September 11 did not create global instabilities.

Cable cuts between core providers affect route changes that are localized between affected providers.

Worm-induced BGP events seem to arise from BGP connectivity failures at very many locations: edge? core?
Nimda probes burn routers’ CPU cycles...

Inset plot shows highly correlated router cpu utilization ... in a different net
Possible causes of BGP session failures

Why BGP routers can fail:
- router CPU overload
- router out of memory, cache overflows
- router software bugs

Possible worm traffic causes: thanks for emails!
- traffic intensity
- traffic diversity (# flows)
- HTTP servers in routers (mngmt interfaces)
- failures in network gear (DSL routers,...)
- IGP (Intra-AS) flapping and routing failures
- proactive disconnection of networks
Preliminary analysis - summary

Worm traffic diversity causes: most likely?

- extreme scan rate -> extremely many flows -> router CPU/memory, NAT problems, ARP storms.

Routing traffic causes: likely?

- -- extremely high rate of BGP updates – router CPU/memory

Worm traffic intensity causes:

- -- loss of BGP messages (presumably at the edge)
  congestion unlikely
Misconfiguration instabilities

common BGP events in the Internet core

0. Misconfigured AS starts announcing a private (confederation) ASpath:

```
%BGP-6-ASPATH: Invalid AS path xxx 3300 (64603) 2008 received from x.x.x.x: Confederation AS-path found in the middle
```

1. Certain routers **ignore** but **propagate** the malformed route
2. Other, RFC-compliant routers **close** & **reopen** the BGP sessions.
3. The combination may propagate wildly
4. Instability ends only when the original leak is plugged.

“... we have the stick now. unfortunately, we also have a vendor who ignores sticks.”
(Randy Bush)
Smaller BGP events: cascading router failures

Initiated by local leakage of malformed route announcements (ASPATH)
June 20 – 30 BGP instabilities

Responsible ASPATH segment: 523 - 64520 - 721
October 6 - 15 BGP instabilities, rrc00
We barely scratched the surface...

1. Globally correlated BGP instabilities are common
2. Some causes are understood a bit – ASPATH oddities
3. Others are unexpected & disturbing (Microsoft worms)
Credits

• Early analysis with BJ Premore and Yougu Yuan at Renesys.

• Raw BGP msg data courtesy of RIPE RIS. Special thanks to Henk Uijterwaal (RIPE).

• Worm traffic data from several /16 networks courtesy of Vicki Irwin (SANS Institute), Ken Eichman (CAS), Vern Paxson (ACIRI).

• Thanks to many network operators and administrators for detailed case stories and observations on Major Vendors’ router misbehaviors.

• Thanks to Tim Griffin (AT&T) and Dave Donoho (Stanford) for discussions.