Decoding Major Internet Outages in 2017

Nitin Nayar

Senior Solutions Engineer

AGENDA

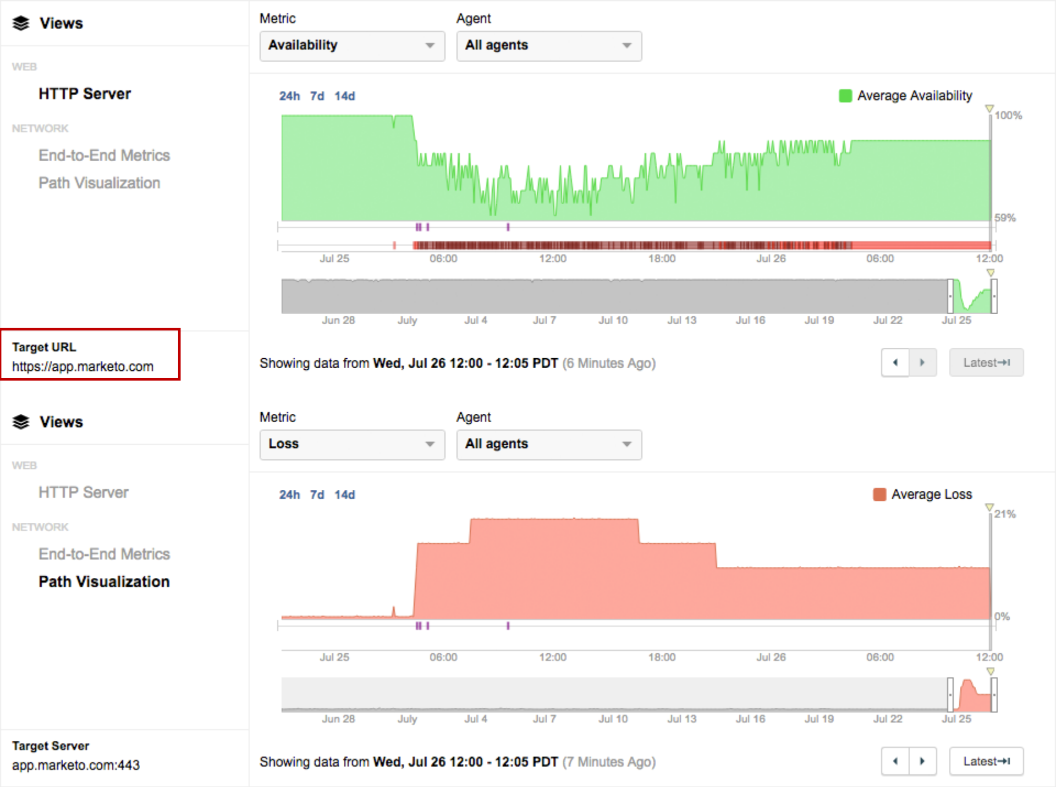
3 Major Outages from 2017:

- Marketo DNS
- AWS S3 outage
- Rostelecom Route Leak

What happens when Domain Name expires?

The Marketo Story

Marketo’s Domain Name Expiry



Target URL
https://app.marketo.com

Metric: Availability

Agent: All agents

Showing data from **Wed, Jul 26 12:00 - 12:05 PDT** (6 Minutes Ago)

Target Server
app.marketo.com:443

Metric: Loss

Agent: All agents

Showing data from **Wed, Jul 26 12:00 - 12:05 PDT** (7 Minutes Ago)

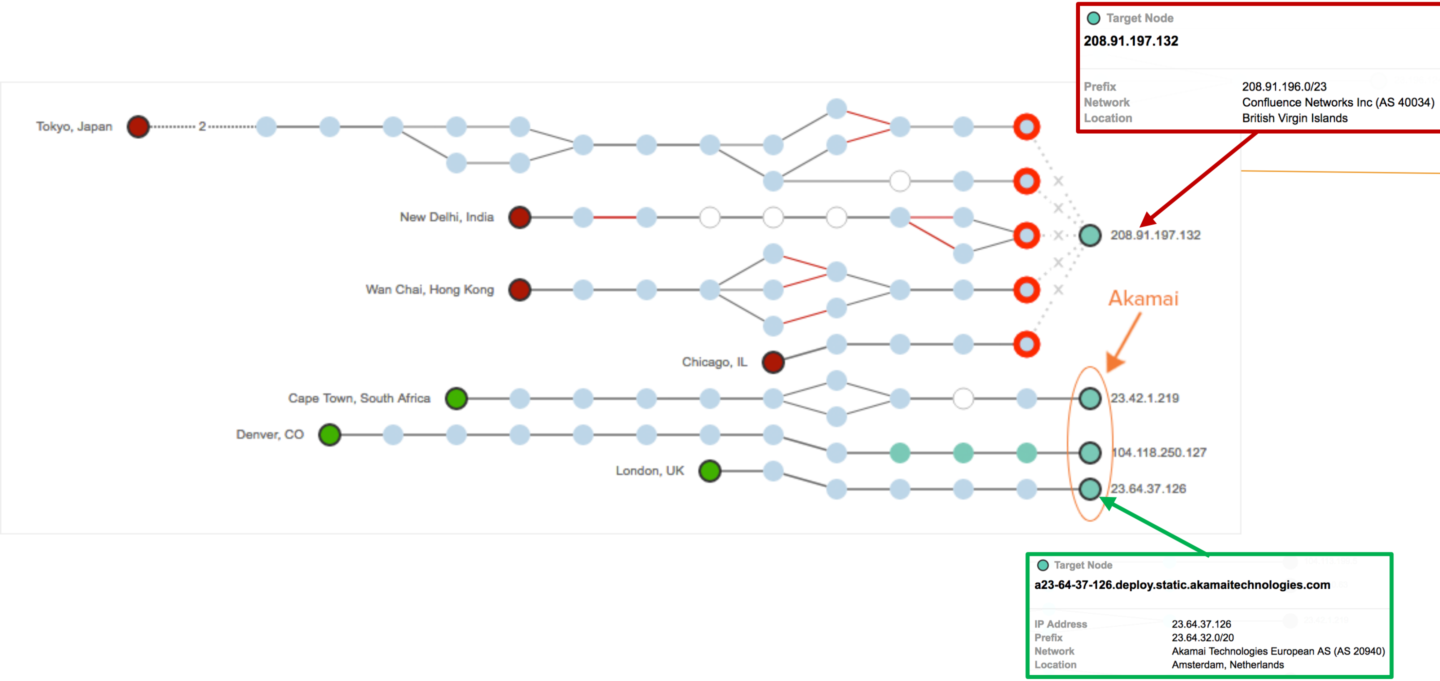
On July 25th at 4:25am PST, Marketo’s main domain started experiencing an outage

HTTP Availability dipped to 60-70%

Network packet loss ~20%

ShareLink: https://ciuvrxmw.share.thousandeyes.com

Marketo’s Domain Name Expiry



Target Node

208.91.197.132

Prefix	208.91.196.0/23
Network	Confluence Networks Inc (AS 40034)
Location	British Virgin Islands

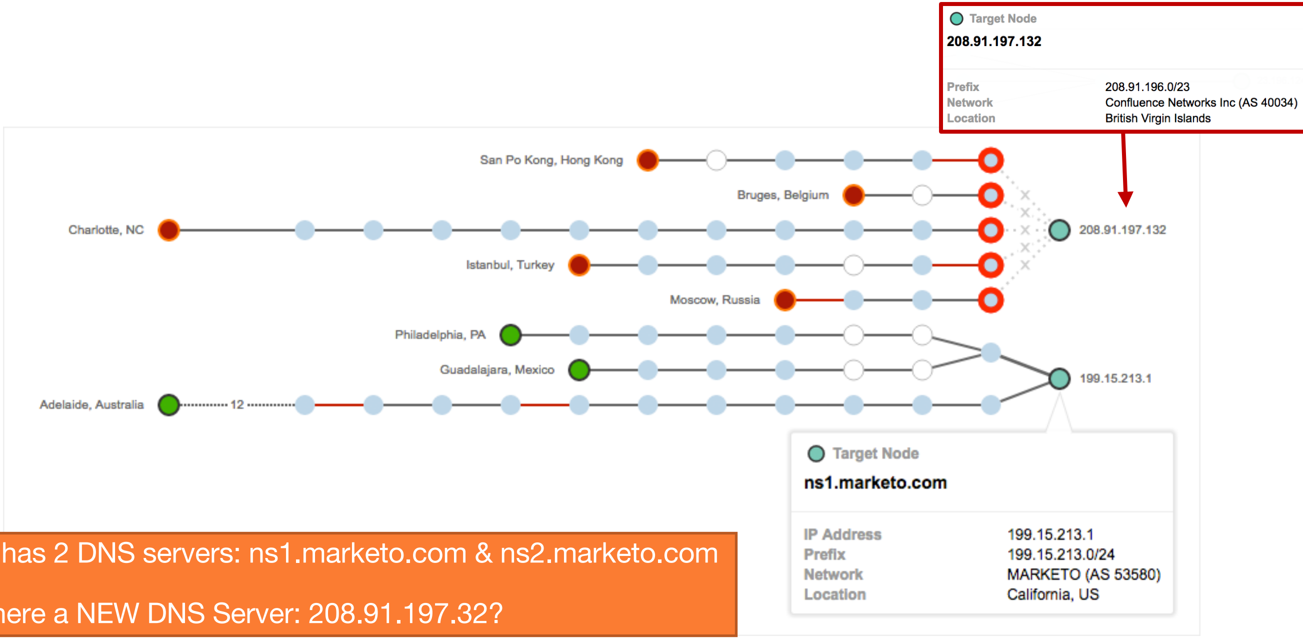
Target Node

a23-64-37-126.deploy.static.akamaitechnologies.com

IP Address	23.64.37.126
Prefix	23.64.32.0/20
Network	Akamai Technologies European AS (AS 20940)
Location	Amsterdam, Netherlands

Why is Traffic being sent to AS 40034- Confluence Networks?

Marketo's Domain Name Expiry
DNS Network Topology



Target Node

208.91.197.132

Prefix	208.91.196.0/23
Network	Confluence Networks Inc (AS 40034)
Location	British Virgin Islands

Target Node

ns1.marketo.com

IP Address	199.15.213.1
Prefix	199.15.213.0/24
Network	MARKETO (AS 53580)
Location	California, US

Marketo has 2 DNS servers: ns1.marketo.com & ns2.marketo.com

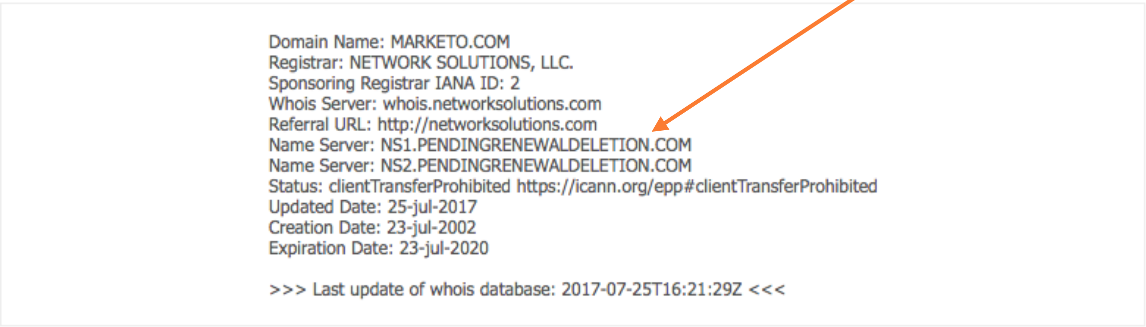
Why is there a NEW DNS Server: 208.91.197.32?

ShareLink: https://gmhux.share.thousandeyes.com

Marketo’s Domain Name Expiry

WHOIS Lookup

Nameservers used by “Network Solutions” for expired domains.



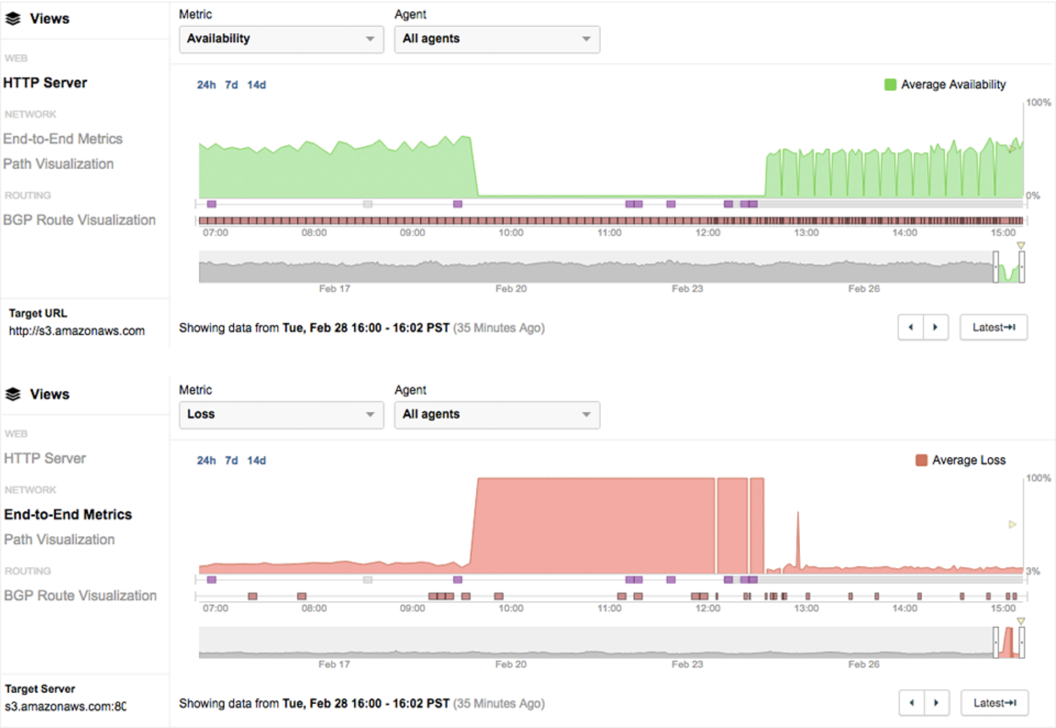
```
Domain Name: MARKETO.COM
Registrar: NETWORK SOLUTIONS, LLC.
Sponsoring Registrar IANA ID: 2
Whois Server: whois.networksolutions.com
Referral URL: http://networksolutions.com
Name Server: NS1.PENDINGRENEWALDELETION.COM
Name Server: NS2.PENDINGRENEWALDELETION.COM
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 25-jul-2017
Creation Date: 23-jul-2002
Expiration Date: 23-jul-2020

>>> Last update of whois database: 2017-07-25T16:21:29Z <<<
```

Marketo Outage Root Cause Summary

- Outage was a direct result of “marketo.com” domain name expiry
- On expiry, traffic to Marketo was black-holed in a new network belonging to “Confluence Networks”

AWS S3 Outage

AWS S3 Outage



Metric: Availability

Agent: All agents

Target URL
http://s3.amazonaws.com

Showing data from **Tue, Feb 28 16:00 - 16:02 PST** (35 Minutes Ago)

Metric: Loss

Agent: All agents

Target Server
s3.amazonaws.com:8C

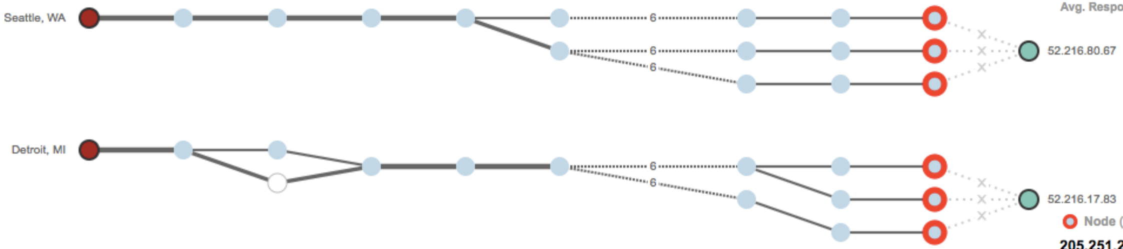
Showing data from **Tue, Feb 28 16:00 - 16:02 PST** (35 Minutes Ago)

- AWS S3 (US-East Region) experienced a massive outage on Feb 28th between 9:40am – 12:36am PST
- Impact of the outage was widespread disrupting multiple services like Quora, Coursera, Docker and Down Detector
- The outage highlighted the dependency across various AWS services

ShareLink: https://gokahptkc.share.thousandeyes.com

AWS S3 Outage Root Cause Analysis

100% Packet Loss / Complete loss of TCP connectivity



● Node (with loss)

205.251.245.232

Error: 1 trace terminates here

Prefix	205.251.244.0/23
Network	Amazon.com, Inc. (AS 16509)
Location	Ashburn, VA, US
DSCP	Best Effort (DSCP 0)
Forwarding Loss	100% (11 of 11 packets)
Loss Frequency	Noisy
Avg. Response	26 ms

● Node (with loss)

205.251.245.123

Error: 1 trace terminates here

Prefix	205.251.244.0/23
Network	Amazon.com, Inc. (AS 16509)
Location	Ashburn, VA, US
DSCP	Best Effort (DSCP 0)
Forwarding Loss	100% (27 of 27 packets)
Loss Frequency	Noisy
Avg. Response	68 ms

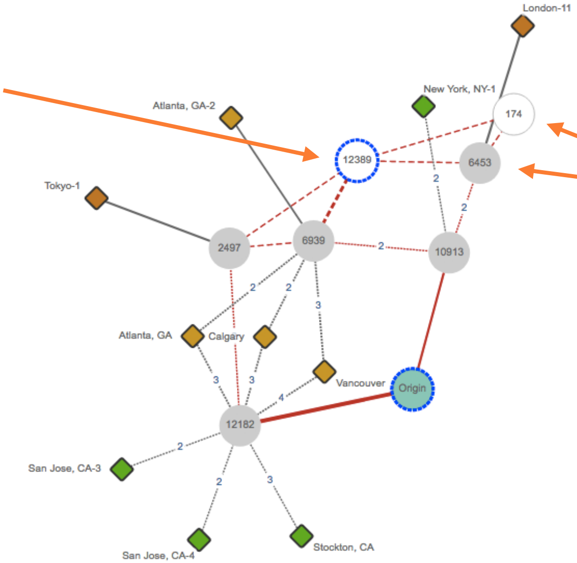
Root Cause: Human error that mistakenly took down more servers than intended.

Rostelecom BGP Route Leak

Rostelecom BGP Route Leak

- On April 26th between 22:36-22:43 UTC, Rostelecom, (Russia's largest ISP) leaked dozens of routes
- The affected IP prefixes belonged to financial services firms, e-commerce and payment services
  - 136 prefixes affected (36 belonged to financial companies)
  - Mastercard SecureCode, Smart Data and MasterPass
  - Verified by Visa and Visa-owned CardinalCommerce
  - Symantec WebSecurity and Geotrust
  - RSA's email servers
  - Online banking sites for French banks BNP Paribas and CIT, and Polish Bank Zachodni owned by Santander
- Traffic to indented destinations was steered through Rostelcom's network

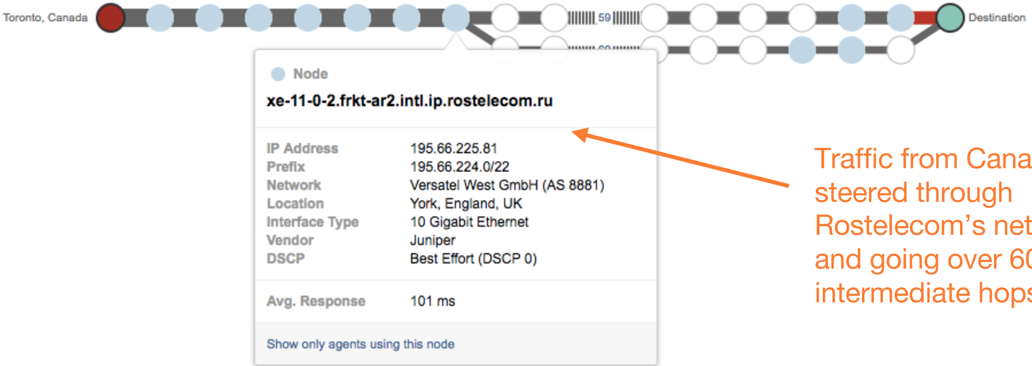
Rostelecom BGP Route Leak



Rostelecom (AS 12389) advertised and withdrew routes to its neighbors

Peers such as Cogent (AS 174), Hurricane Electric (AS 6939) and Tata (AS 6453) accepted these routes and propagated them across the Internet.

Rostelecom BGP Route Leak



Node

xe-11-0-2.frkt-ar2.intl.ip.rostelecom.ru

IP Address	195.66.225.81
Prefix	195.66.224.0/22
Network	Versatel West GmbH (AS 8881)
Location	York, England, UK
Interface Type	10 Gigabit Ethernet
Vendor	Juniper
DSCP	Best Effort (DSCP 0)
Avg. Response	101 ms

Show only agents using this node

Traffic from Canada steered through Rostelecom’s network, and going over 60+ intermediate hops!

References

- AWS S3 Outage
  - ShareLink: https://gokahptkc.share.thousandeyes.com
  - **AWS Root** Cause Analysis- ThousandEyes Blog: https://blog.thousandeyes.com/aws-s3-outage-likely-caused-by-internal-network-issue/

- Marketo:
  - ShareLink-HTTP: https://ciuvrxmw.share.thousandeyes.com
  - ShareLink-DNS: https://gmhux.share.thousandeyes.com
  - **Marketo Root** Cause Analysis- ThousandEyes Blog: https://blog.thousandeyes.com/what-happened-when-marketos-domain-name-expired/

Thank You