Meeting an SLA for 100% uptime without losing sleep
(Paranoia is pointless)

Jay Daley

p: (+64) (4) 931 6977 e: registry@nzrs.net.nz
f: (+64) (4) 931 6979 w: www.nzrs.net.nz
P.O. BOX 24361, WELLINGTON, NEW ZEALAND
NEW ZEALAND DOMAIN NAME REGISTRY LIMITED

It all begins with RISK

- Seriously. No, seriously:
  - STEP 1: Do a risk analysis
  - STEP 2: Implement it
  - STEP 3: Go to step 1

- Anything else is *paranoia*, *hand waving*, a *waste of time*, *pointless* … you get the picture

Yes, really!

- From the Risk Analysis comes
  - Priorities for work
  - Where to spend the money
  - What else you need to know
- There isn’t anything else.
  - Honest.

Simple risk

- Risk is quantifying a threat by
  - Likelihood
  - Impact
- To get a
  - Rating

Likelihood x Impact = Rating

Risk matrix

LIKELIHOOD	CONSEQUENCE				
	Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Almost certain	High	High	Critical	Critical	Critical
Likely	Medium	High	High	Critical	Critical
Possible	Low	Medium	High	High	Critical
Unlikely	Low	Low	Medium	High	Critical
Rare	Low	Low	Medium	High	High

Mega impact

- Meteor hits Wellington!
- Taupo caldera explodes!!
- Global depression!!!

- Only limited by your imagination. *sigh*

But

- Meteor hits Wellington!
  - 1 in every 65 million years
- Taupo caldera explodes!!
  - 1 in every 200 thousand years
- Global depression!!!
  - 1 in every 80 years

- Treat them very differently

Mega likelihood

- Someone will try to hack
  - Firewall
- Data corruption/loss
  - Backups
- Email to wrong person
  - Ah! – Depends on impact on your business

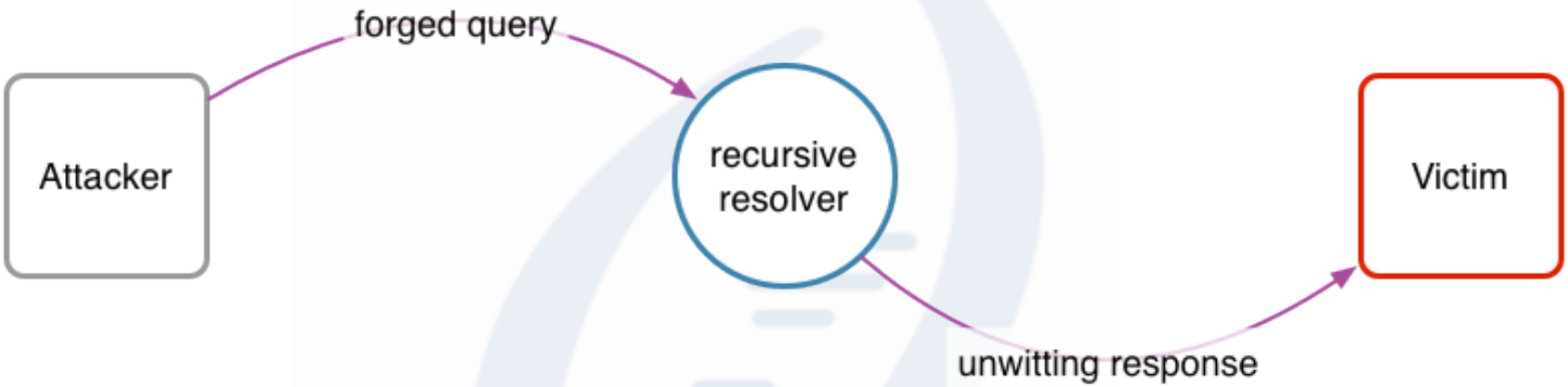
Internet threats

- Asymmetry
- Anonymity
- Speed of adaptation
- Zero cost transactions - arbitrage

Scale

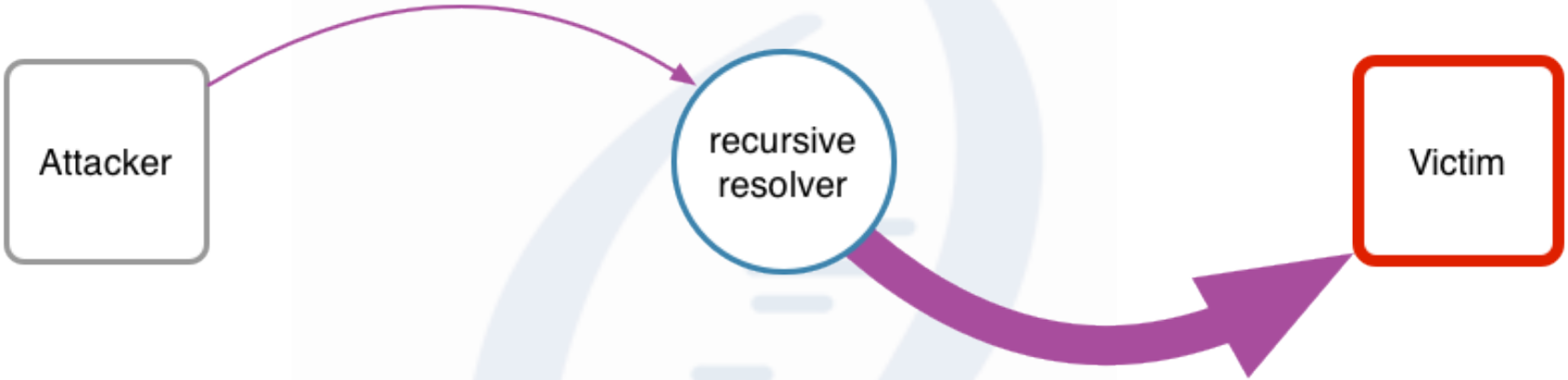
- Huge server farms – commodity hardware
- DNS bit flips
  - Artem Dinaburg estimates:
    - 120 failures in test per billion operating hours per megabit of DRAM (using Google hardware data)
    - Globally 614,400 errors/hour are generated
  - At least 1 trillion DNS lookups per day
  - Makes bit squatting a reality
    - See bit flipped version of microsoft.com

Illustrated Internet threat - 1



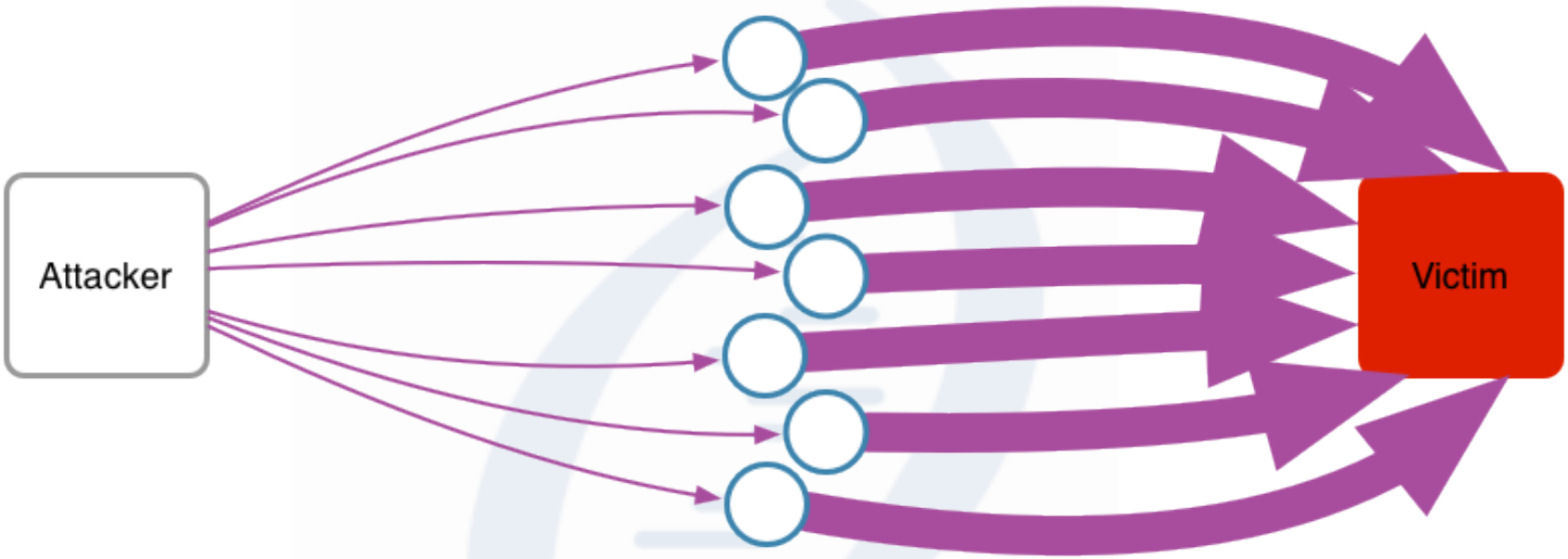
- Queries can have fake source address
- Resolver responds to that fake address

Illustrated Internet threat - 2



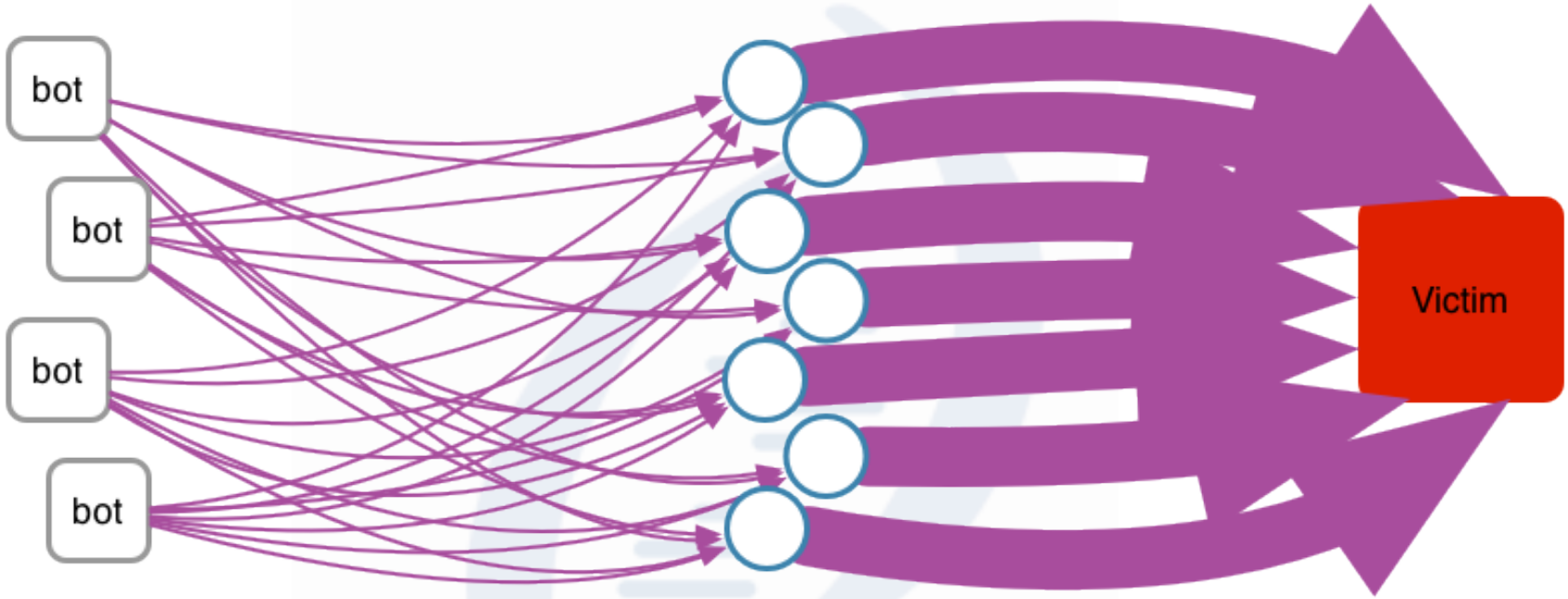
- Traffic can be amplified by factor of 80
  - Query is normally 52 to 64 bytes
  - Response can be over 4000 bytes

Illustrated Internet threat - 3



- Use multiple resolvers
  - Over 25 million to use
  - Limits detection by individual resolvers

Illustrated Internet threat - 4



- If the attacker controls a botnet
  - Could by 100,000 strong or more

Mitigation strategies

- Genetic diversity
- Remove ~~unnecessary~~ stuff
- Never assume – look and see
- Steal every good idea
- Compartmentalise
- Two pairs of eyes

Some of our risks

#	Risk	Categories	er	L'hood	Impact	Rating	/ Man
1l	Loss of Wellington including all staff and primary site	Strategic Financial Service Reputation Legal External People	CE	Rare	Extreme	High	• BCP • Direc of W to re • Cont on m busir • Insur

	Controls / Risk Mitigation / Management Strategies	Time frame	Target L'hood	Target Impact	Target Risk Rating	Additional controls to consider / further action proposed?
	• BCP • Directors based outside of Wellington with ability to restart business. • Contract with company on mirror site to restart business. • Insurance	Mitigated as much as possible				None
	• Multiple, geographically					

Business Continuity Plan

- For when it all goes wrong (and it will)
- Our chapter headings:
  - First 2 hours emergency response plan checklist
  - Overview
  - Emergency response plan
  - Emergency roles and responsibilities
  - Business recovery checklist and business recovery plan
  - Appendices:

Contacts (us, suppliers, banks, media, customers)
Emergency team roles and procedures
Emergency kits
Insurance documents
Risk register

IT disaster recovery plan
IT risk matrix
Security incident detection and response
Emergency operator activation plan
All key supplier contracts
Instructions for emergency comms kit

And finally

- So you can tweet in any disaster

Any questions?

p: (+64) (4) 931 6977 e: registry@nzrs.net.nz
f: (+64) (4) 931 6979 w: www.nzrs.net.nz
P.O. BOX 24361, WELLINGTON, NEW ZEALAND
NEW ZEALAND DOMAIN NAME REGISTRY LIMITED