DNS Security

New cache-poisoning attacks & why it matters

Sam Sargeant - Modica Group

APNIC 26 - Christchurch - August 2008

What I'll cover

1. Simplified version of how DNS works and cache poisoning
2. What is the impact of a poisoned cache?

About me

- I am not
  - A security professional
  - nor a vendor of DNS software
- I am
  - an operator of DNS servers
  - from New Zealand

Part I

How DNS & Cache Poisoning work

Query:
www.apnic.net

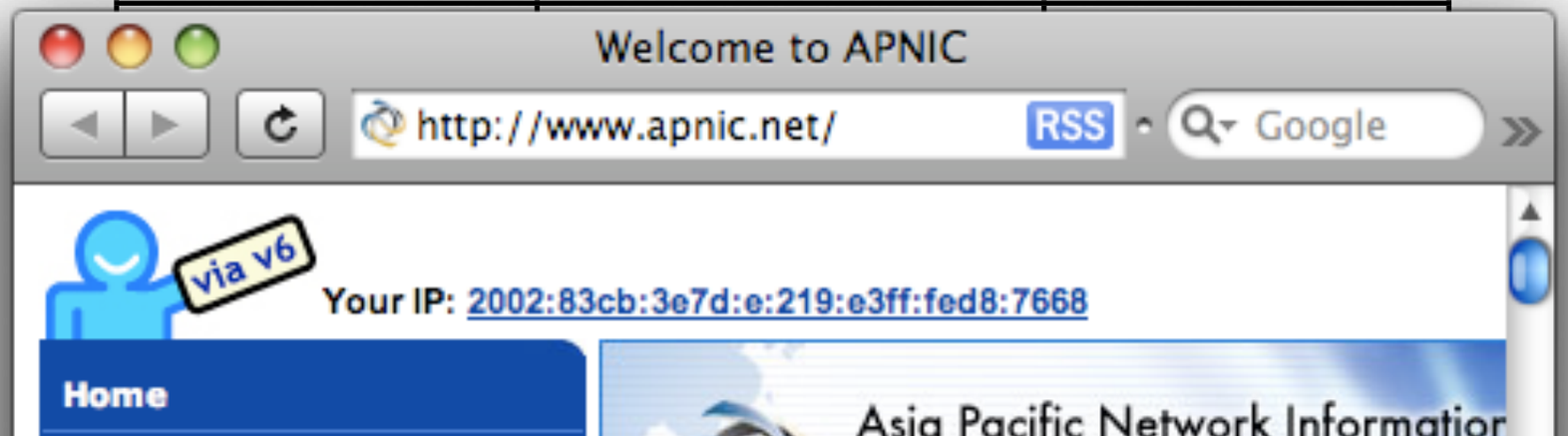
Answer:
2001:dc0:2001:0:4608:20::

My Laptop

Conference
DNS Server

APNIC's
DNS Server

Query	Answer	Cache Lifetime
www.wlug.org.nz	2002:3cea:4275::1	600
www.apnic.net	2001:dc0:2001:0:4608:20::	3600
www.google.com	2001:4860:0:2001::68	300
www.paradise.gen.nz	2001:4400:0:81::1	86400
ns1.dns.net.nz	2001:dce:2000:2::130	86400



Cache Poisoning: Spoofing

- First get the server to ask the right question
- Then spoof the answer packet and match:
  - Source IP address
  - Destination port
  - Query ID - 16 bit number

Query:
www.apnic.net

Query (0x3F8):
www.apnic.net

Answer (0x3F8):
2001:dc0:2001:0:4608:20::

Attacker Laptop

Conference
DNS Server

APNIC's
DNS Server

Answer (0x2E3):
2001:cafe:0f:dead:beef::2

Query	Answer	Cache Lifetime
www.apnic.net	2001:cafe:0f:dead:beef::2	1,000,000,000

Answer (0x72C):
2001:cafe:0f:dead:beef::2

Answer (0xD2C):
2001:cafe:0f:dead:beef::2

Answer (0x3F8):
2001:cafe:0f:dead:beef::2

Mitigating spoofing

- Transaction IDs are a 16 bit number
- In the mid-90s, this was sequential & easy to spoof
- Resolvers now use pseudo-random numbers
- Window of opportunity is small enough that attacks aren't practical

Cache Poisoning: RRSet

- First get the server to ask you a question
- Then respond with a set of records, including the poisoning record for your target

Query:
www.evil.com

Answer:
www.evil.com is
2001:dc0:2001:0:4608:20::
Oh, and www.apnic.net is
2001:cafe:0f:dead:beef::2

Attacker

Conference
DNS Server

Attacker's
DNS Server

Query	Answer	Cache Lifetime
www.apnic.net	2001:cafe:0f:dead:beef::2	1,000,000,000
www.evil.com	2001:dc0:2001:0:4608:20::	3600

Mitigating RRSet

- Your additional records must be relevant to the question
- It's okay to supply "ns2.apnic.net" along with the answer for "www.apnic.net"
- Your answer will be dropped if you reply for "www.evil.com" and include the record for "www.apnic.net"

Summary thus far:

- Spoofing - requires a lot of luck to get it right during the small window of opportunity - Guess the right number between 1 in 65535
- RRSet - Checking for relevance eliminates this as a useful means to poison a cache

Kaminsky Attack

- Early 2008: Kaminsky discovers new exploit, DNS vendors notified
- 8th July: New exploit is publicly announced however details are kept secret. Updated software released
- 21st July: Details of exploit are leaked, exploit code is available within days
- Early August: Full details released

Are you vulnerable?

- Under Linux or Mac OS X run this command:

```
dig +short porttest.dns-oarc.net TXT
```

- On Windows, visit www.doxpara.com

Query:
aab.apnic.net

Attacker

Conference
DNS Server

Answer:
NXDOMAIN

APNIC's
DNS Server

Answer:
aab.apnic.net is
NXDOMAIN
Oh, and www.apnic.net is
2001:cafe:0f:dead:beef::2

Query	Answer	Cache Lifetime
www.apnic.net	2001:cafe:0f:dead:beef::2	1,000,000,000

How do we fix this?

- Source port randomisation in DNS software
- Increases difficulty for attackers from 16-bits to around 32-bits
- Patches have been available from most vendors since July
- NAT changes the source port of outgoing packets and maybe predictable

Vectors

- Customers of service providers can keep generating queries against their ISPs DNS server
- Some service providers have open DNS resolvers; anyone on the planet can start the race
- Phishing can trigger a flurry of DNS queries

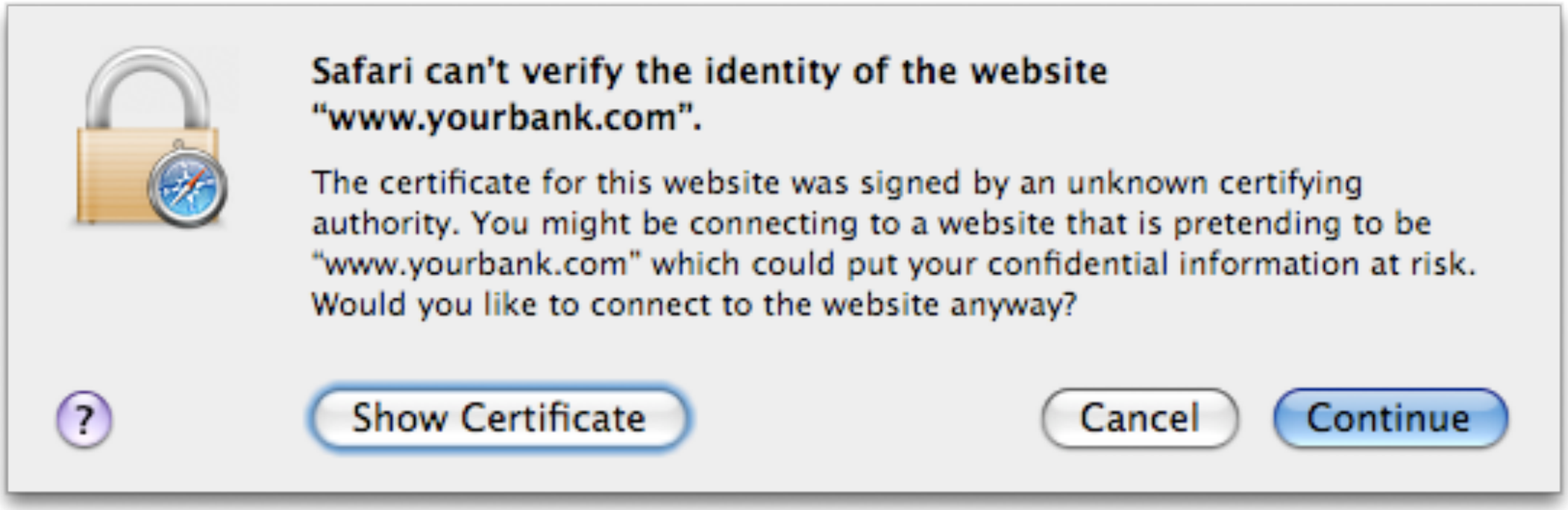
Part 3

Why should you care?

Attacker in the middle

- Poison a DNS cache so www.YourBank.com resolves to a server controlled by you
- When users arrive at the site, ask them for their username & password or credit card. They'll give it to you
- Sites that use two-factor authentication are more resilient, but a smart attacker can still get access to your bank

Doesn't HTTPS fix it?



Redirect to malware site

- Happened to an ISP in China last week
- Users who mistyped a domain were sent to a site that infected their computer

Denial of Service attack

- Take a competitor's web site down by sending their traffic elsewhere
- Create fake SPF records to restrict outbound email
- Create a poisoned entry for google.com and direct huge numbers of users to the target

Not just email and web

- FTP: Gather login details
- OpenSSH: Does a great job of warning about potential attacker-in-the-middle and refuses to continue
- VPN: If your client doesn't validate the server

Targets at risk

- Resolvers used by service provider customers
- Enterprise resolvers

Targets that are safe

- Authoritative servers

Would DNSSEC help?

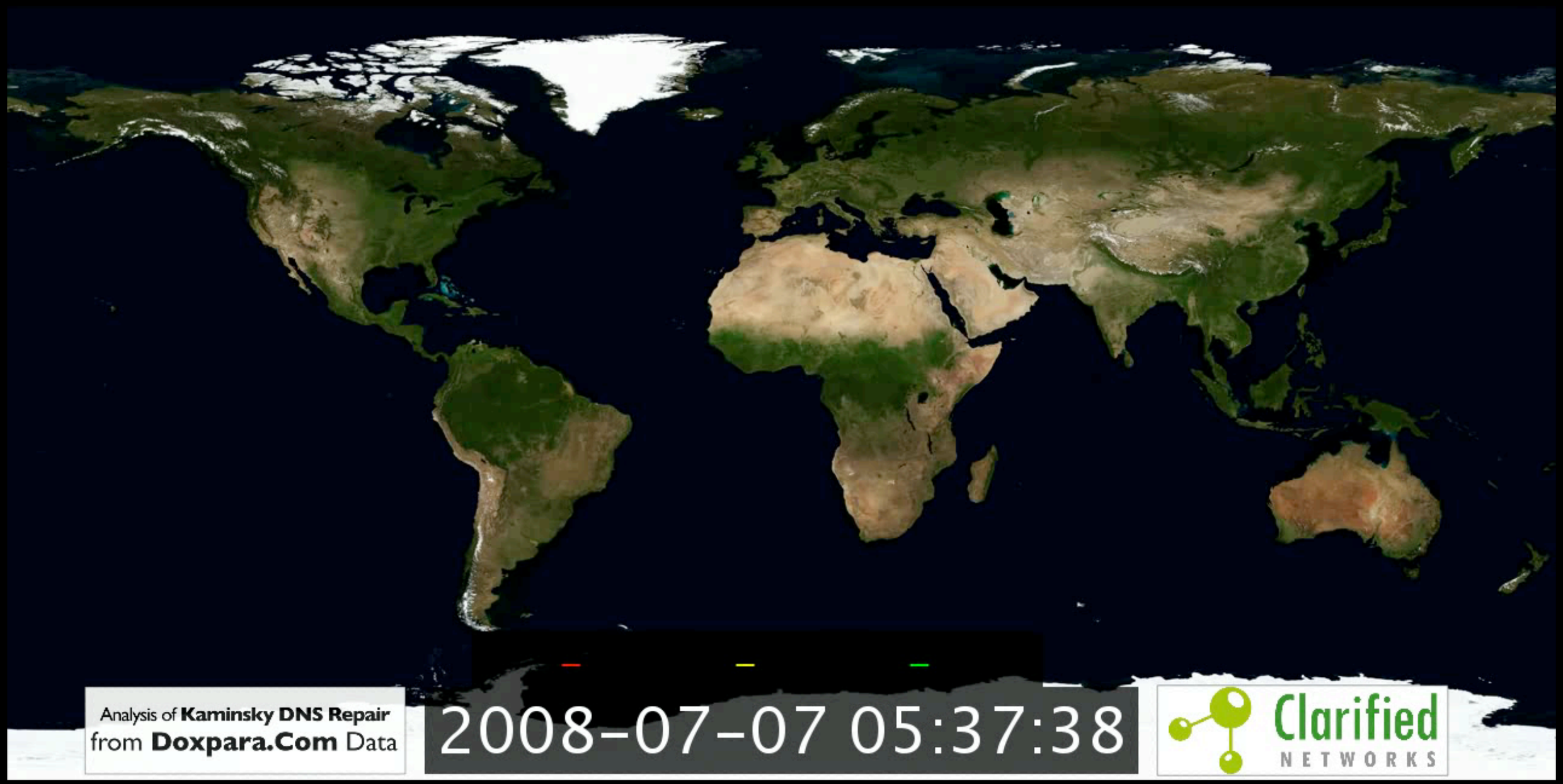
- Sure, but you need ICANN to sign the root
- You also need a resolver that validates signed responses
- DNSSEC will not solve the problem without other deployment - You can’t do it on your own

How can we solve this?

- Upgrade your DNS server software
- Limit the exposure by ensuring your servers only answer queries from your customers
- Protocol design needs some attention

Summary

- It sounds like the old problems we had in the 1990s
- It's really a new problem based on combining old ones
- Exploits have been used in the wild
- DNSSEC will help, when it works
- Defence in depth is best



Unpatched

Patched (NAT)

Patched

Queries?