

# Assessing DNS Vulnerability to Record Injection

Kyle Schomp<sup>†</sup>, Tom Callahan<sup>†</sup>, Michael Rabinovich<sup>†</sup>, Mark Allman<sup>†‡</sup>

<sup>†</sup>Case Western Reserve University

<sup>‡</sup>International Computer Science Institute

Passive and Active Measurement Conference 2014

Security training group EC-Council's website defaced

February 28, 2014 | By Paul Mah

In an ironic twist, the website of security certification website being defaced by a hacker who signed one of the characters in the movie Hackers. In the website, the hacker also claimed to have found to LE [Law Enforcement] (and .mil) officials."

As reported by Ars Technica the hacker also posted a passport on the defaced website as proof of his well as an email from Snowden to the council in were likely submitted to the EC-Council as proof courses or certifications.

This was not the first defacement suffered by the challenge that system administrators face to protect against security attacks. There was no mention of access, though a DNS hijacking was done using a DNS

For more: - check out this a

**Related Articles**

How a founder at Kaspersky: Anti-

Sign up for our

DNS attack writer a victim

www.networkworld.com/news/2008/073008-dns-attack-writer-a-victim.html

**NETWORKWORLD**

Security IANs & WANs UC / VoIP Cloud Infrastructure Mgmt Wireless Software Data Center SMB Careers Gearhead Tech Deb

Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SEM | White Papers | Webcasts | Tests

News

DNS attack writer a victim of his own creation

By Robert McMillan, DIG News Service July 28, 2008 09:50 PM ET

Latest News

- Is SDN your next security nightmare?
- Brocade's fabric strategy appears to be working
- IBM workforce cuts raise questions
- As Web's 25th anniversary approaches, 87% of U.S. is online

Security Fix - When Mon...

blog.washingtonpost.com/securityfix/2008/04/when\_monetizing\_isp\_traffic\_go.html

The Washington Post

washingtonpost.com > Technology > Security Fix

**Security Fix**  
Brian Krebs on Computer Security

About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Brian Krebs

SEARCH THIS BLOG

When Monetizing ISP Traffic Goes Horribly Wrong

RECENT POSTS

- Farewell 2009, and Washington Post
- Hackers exploit AOL Reader flaw via co-strip syndicate
- Twitter.com hijack by Iranian cyber a
- Group lba hotbeds Conficker worm outbreaks
- Hackers target unpatched Adobe

Widespread Hijacking of Search Traffic in the United States

https://www.eff.org/deeplinks/2011/07/widespread-search-hijacking-in-the-us

**ELECTRONIC FRONTIER FOUNDATION**  
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME ABOUT OUR WORK DEEPLINKS BLOG PRESS ROOM TAKE ACTION SHOP

AUGUST 4, 2011 | BY PETER ECKERSLEY

Widespread Hijacking of Search Traffic in the United States

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. Learn more about what the program is, how it works, and what you can do.

Follow EFF

Change the future of copyright in EU by sending your comments to the European Commission. Deadline is next week!  
https://eff.org/r/7zml  
FEB 28 @ 8:07AM

EFF membership packs include cam stickers to

First case of "drive-by pharming" identified in the wild

www.networkworld.com/news/2008/012208-drive-by-pharming.html

**NETWORKWORLD**

Security IANs & WANs UC / VoIP Cloud Infrastructure Mgmt Wireless Software Data Center SMB Careers Gearhead Tech Debate Tests Communities

Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SEM | White Papers | Webcasts | Tests

News

First case of "drive-by pharming" identified in the wild

Latest News

- Is SDN your next security nightmare?
- Who's hiring? Marketing lures more tech pros
- Brocade's fabric strategy appears to be working
- IBM workforce cuts raise questions
- As Web's 25th anniversary approaches, 87% of U.S. is online

View more Latest News

Massive DNS poisoning attacks in Brazil

www.securelist.com/en/blog/2008113214/Massive\_DNS\_poisoning\_attacks\_in\_Brazil

**SECURELIST**

Threats Analysis Blog Statistics Descriptions Glossary

Home > Blog > Incidents > November 07 2011 > Massive DNS poisoning attacks in Brazil

Fabio Assolini  
Kaspersky Lab Expert  
Posted November 07, 11:38 GMT  
Tags: DNS

In the past few days several Brazilian ISPs have fallen victim to a series of DNS cache poisoning attacks. These attacks see users being redirected to install malware before connecting to popular sites. Some incidents have also featured attacks on network devices, where routers or modems are compromised remotely.

Brazil has some big ISPs. Official statistics suggest the country has 73 million computers connected to the Internet, and the major ISPs average 3 or 4 million customers each. If a cybercriminal can change the DNS cache in just one server, the number of potential victims is huge.

Last week Brazil's web forums were alive with desperate cries for help from users who faced malicious redirections when trying to access websites such as YouTube, Gmail and Hotmail, as well as local market leaders including Uol, Terra and Globo. In all cases, users were asked to run a malicious file as soon as the website opened.

We monitored one attack which saw a clean machine displaying this warning when opening Google

Install Google Defence Para usar o novo Google.com

Widespread Hijacking of Search Traffic in the United States

with Peter Eckersley.

...which are marked

...range phenomena in the

...ks, some or all traffic to

...le, is being directed to

...routed through a

...teams that discovered the

...proxy servers that were

...ing Group and EFF have

...is interception. Paxfire's

...ue term that could be

...searches they conduct, or

...w if any of the affected ISP

...ed to this collection

...munications with search

...the ISPs using web

...d Cavalier, Cogent,

...d Paxfire in the past, but

Martirosian: Hacker attacks may continue for several days

www.washingtonpost.com/archive/local/2008/02/27/samvel-martirosian/

NEWSLINE

- 19/02 + 28/02: Georgian president visits his friend's family in Echmiadzin
- 19/01 + 28/02: G. Ohanian discusses issues of NATO new programs in Brussels
- 18/08 + 28/02: Report: UK agency spied on chats
- 18/09 + 28/02: G. Sahakian: Opposition does not need commission on March 1 events
- 18/03 + 28/02: Ukraine parliament is illegitimate - Yanukovich
- 18/14 + 28/02: Armenian police chief receives OSCE Yerevan Office head
- 18/12 + 28/02: Armed men seize Simferopol Airport in Crimea
- 17/08 + 28/02: Ukraine asks Russia to extradite Yanukovich
- 17/03 + 28/02: African migrants storm into Spanish enclave of Melilla
- 17/09 + 28/02: Presidents of Armenia and Georgia summarize results of talks
- 17/04 + 28/02: Peace talks still an option, Syrian opposition says
- 17/08 + 28/02: Tevan Poghosian: No need to dream of Maidan in Armenia
- 15/08 + 28/02: Iskandarian: Ukraine today is divided into twelve, not two
- 15/13 + 28/02: Psaki: There cannot be a military solution to Karabakh conflict

27.02.2014, 19:27  
Aysor.am

drive-by pharming attacks.

reported Tuesday that drive-by on a customer's broadband router

Web site, has been observed in

against a Mexican bank. "It's mate Spanish-language e-greeting

y Response principal researcher g but instead of displaying images,

de seeks to change 2Wire DSL bank site that mimics the site of one

the specific bank.

3 of the real one, you'd get the

ale signs that it's occurring," he

University School of Informatics e JavaScript-based security threat

padband users.

ipment is often left configured with

ged. "The attacks know what the

make sure home routers of any

able to drive-by pharming "because

# DNS Recording Injection

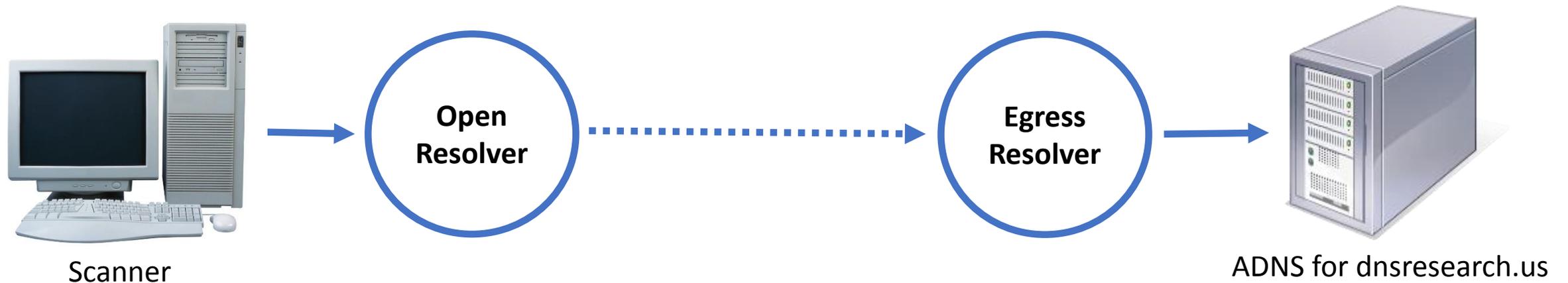
- Subverting the DNS name to address bindings can result in:
  - Redirection to a malicious webserver
  - Privacy issues
  - Denial of service
  - Phishing attacks
  - Malware installation

# Our Contribution

- Assess vulnerability to extraneous record injection
  - Bailiwick violations
- Examine the incidence rate of intentional response rewriting by resolvers
  - Negative response rewriting
  - Search engine hijacking (Paxfire)
- Survey use of established mitigations to the *Kaminsky* vulnerability
- Demonstrate a new record injection attack (the *Preplay* vulnerability)

# Dataset Collection Methodology

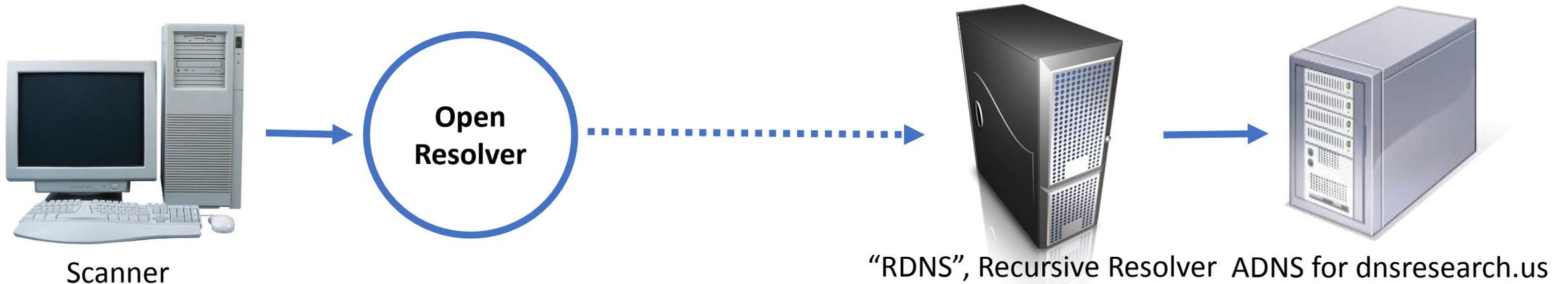
- Discover open resolvers by sampling randomly from the Internet
- Deploy our own authoritative DNS server (*ADNS*)
- DNS request probes target our own domain



- Test open and egress resolvers for vulnerability to record injection

# Dataset Collection Methodology

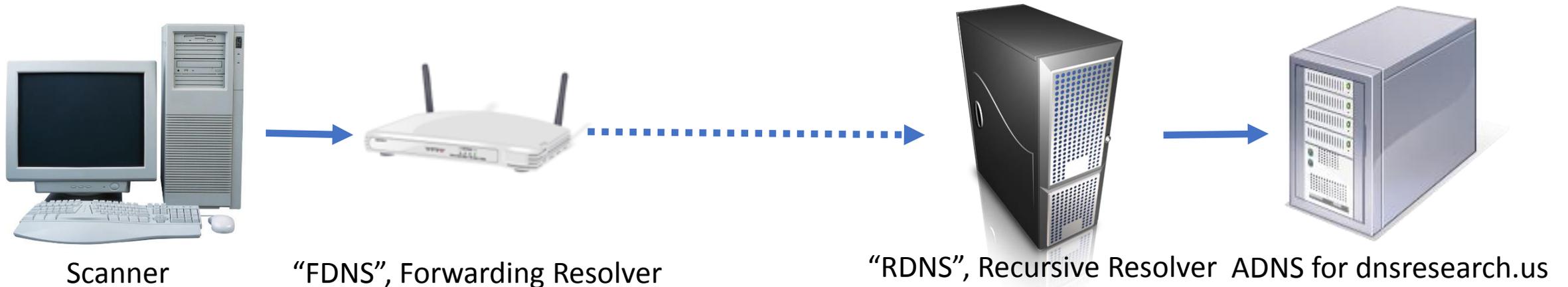
- Discover open resolvers by sampling randomly from the Internet
- Deploy our own authoritative DNS server (*ADNS*)
- DNS request probes target our own domain



- Test open and egress resolvers for vulnerability to record injection

# Dataset Collection Methodology

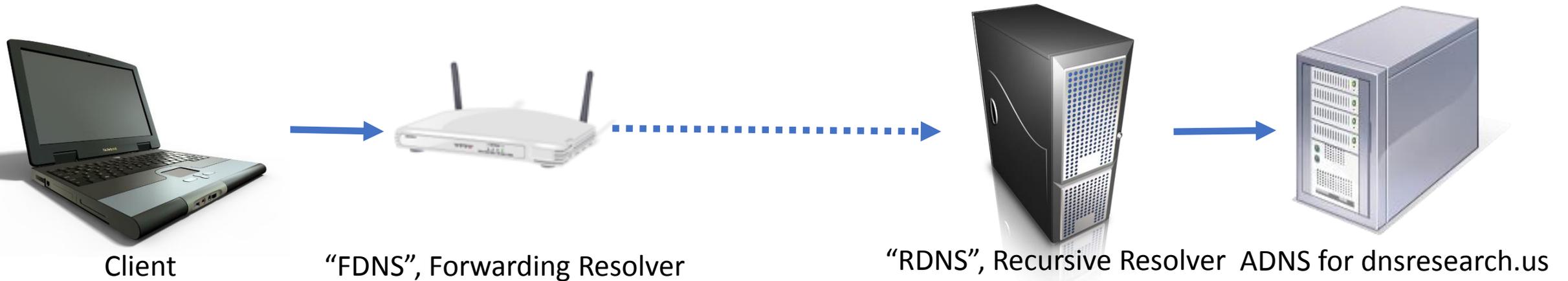
- Discover open resolvers by sampling randomly from the Internet
- Deploy our own authoritative DNS server (*ADNS*)
- DNS request probes target our own domain



- Test open and egress resolvers for vulnerability to record injection

# Dataset Collection Methodology

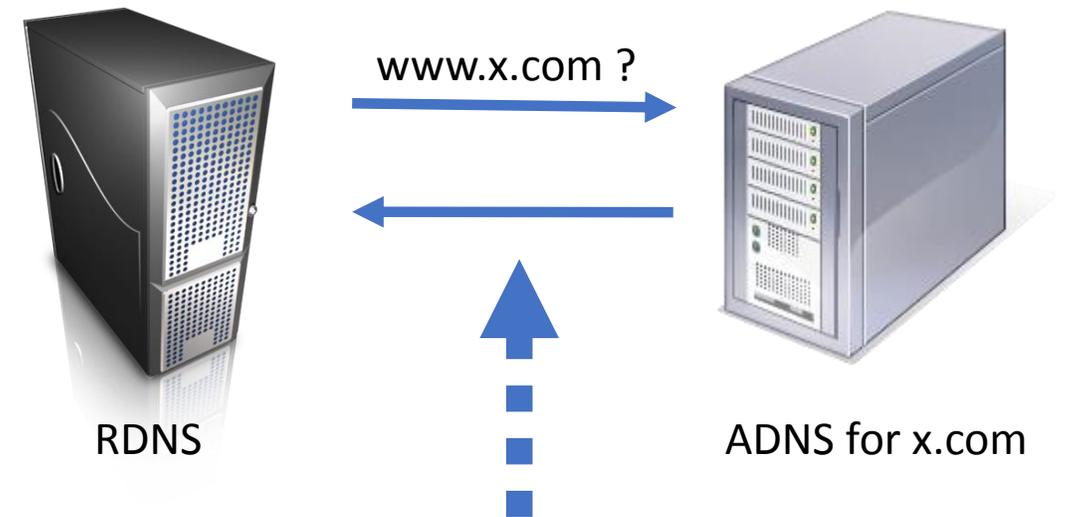
- Discover open resolvers by sampling randomly from the Internet
- Deploy our own authoritative DNS server (*ADNS*)
- DNS request probes target our own domain



- Test open and egress resolvers for vulnerability to record injection

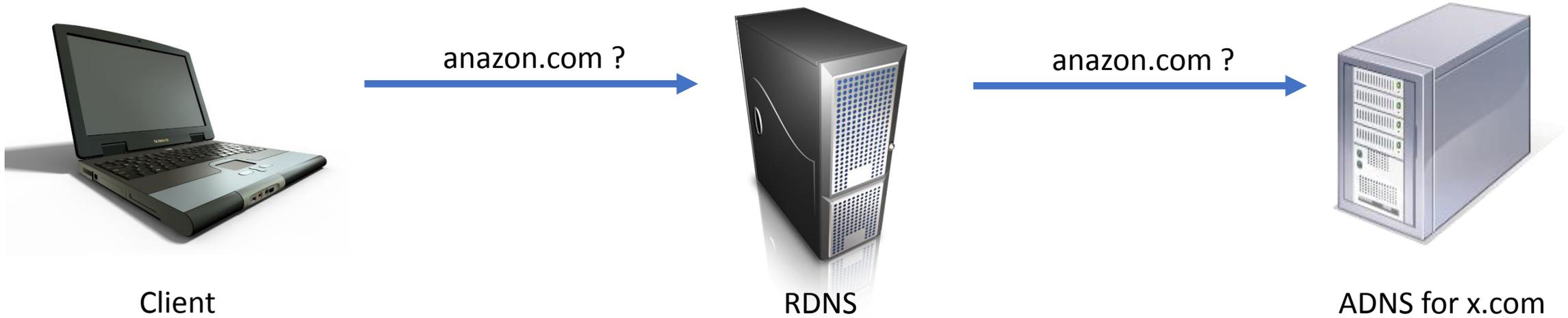
# Bailiwick Violations

- Over 10 years old
- Mitigated via the bailiwick rules
- 749 violations found in 1.09M open resolvers tested
- Some resolvers *still* vulnerable to this very old attack!

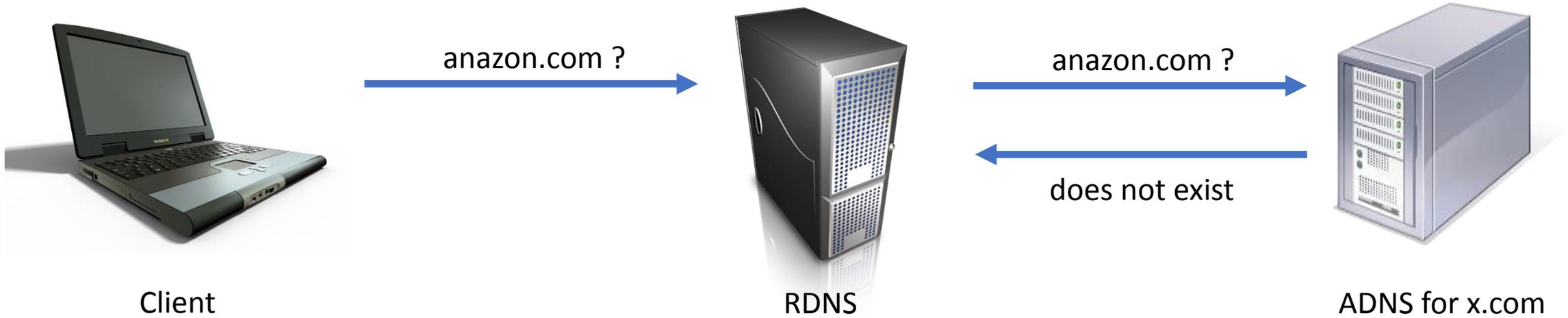


Query	www.x.com ?
Answer	1.2.3.4
Additional	www.hsbc.com A 2.3.4.5

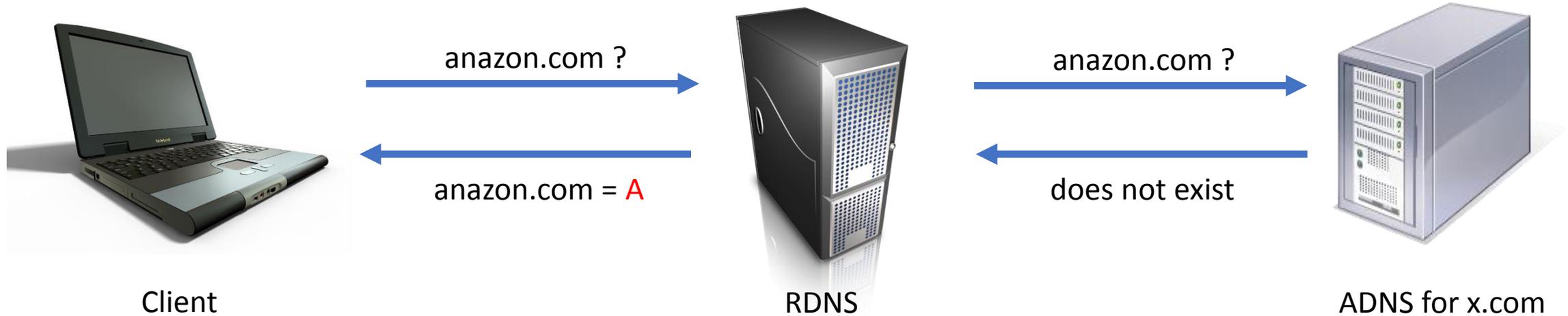
# Negative Response Rewriting



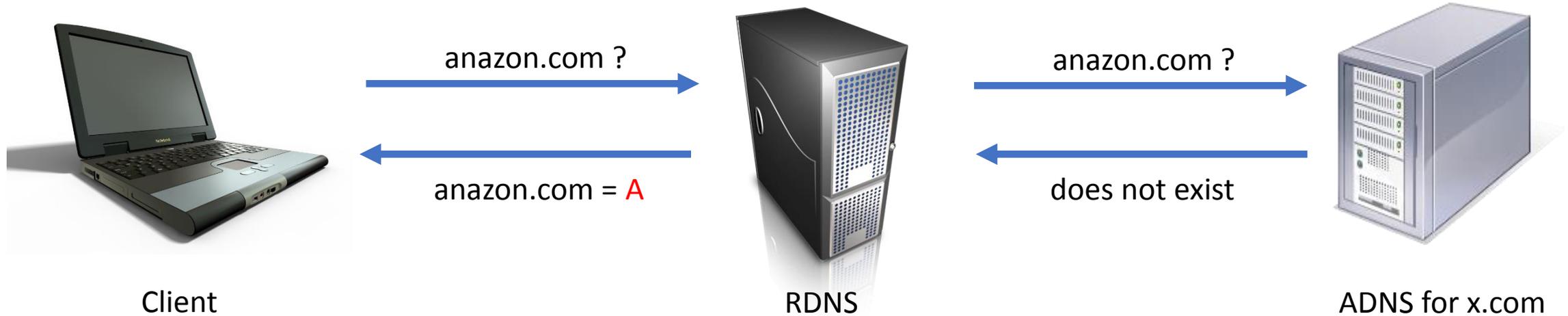
# Negative Response Rewriting



# Negative Response Rewriting

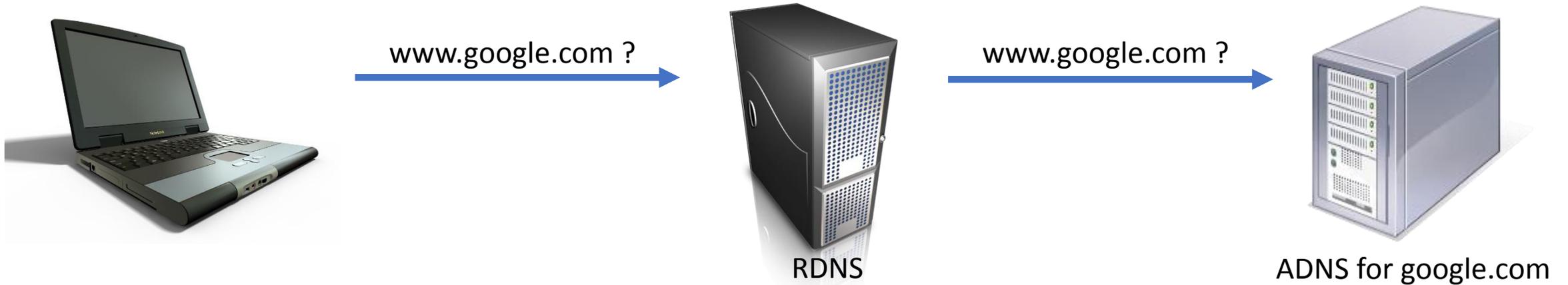


# Negative Response Rewriting

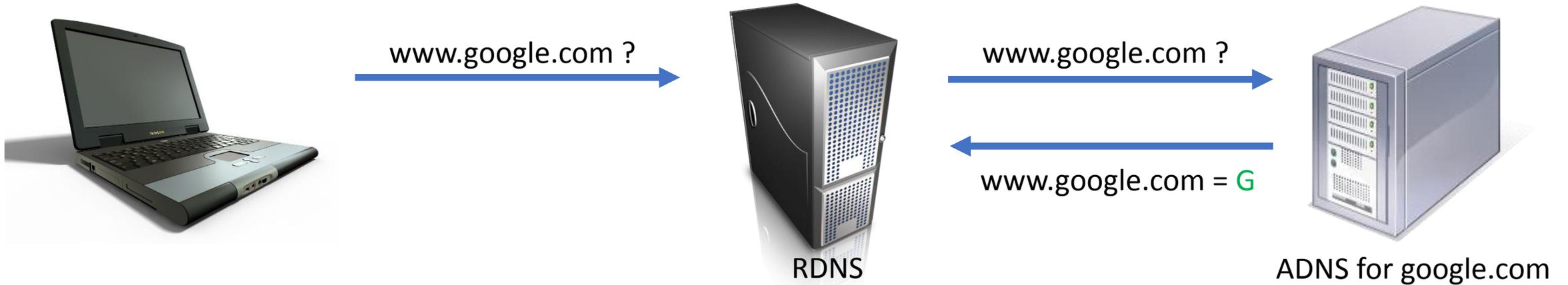


- Why? DNS provider profits from advertising at A
- Happens to 24% of open resolvers

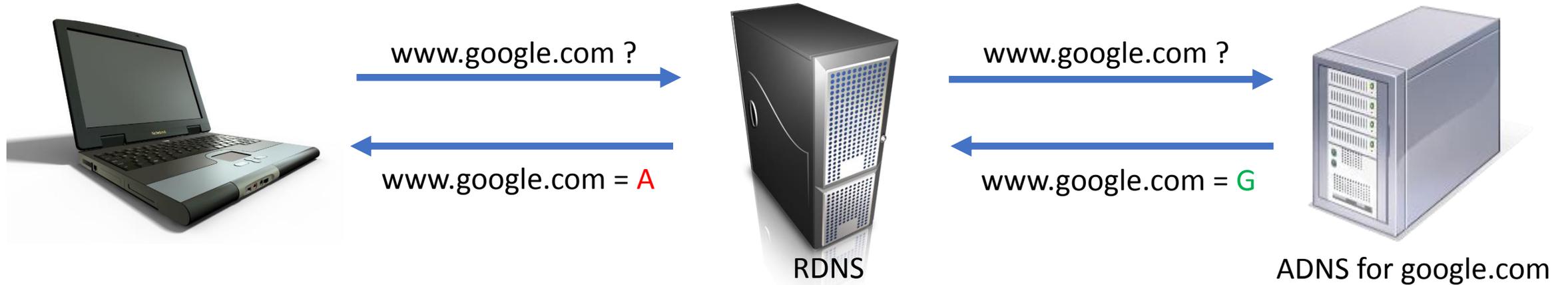
# Search Engine Hijacking (Paxfire)



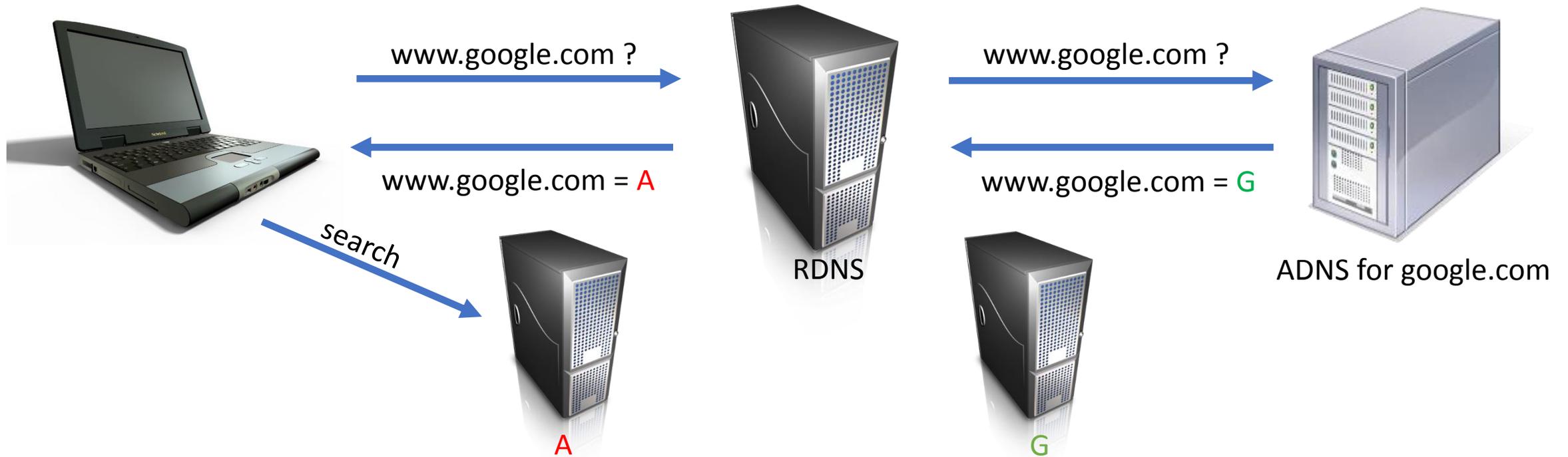
# Search Engine Hijacking (Paxfire)



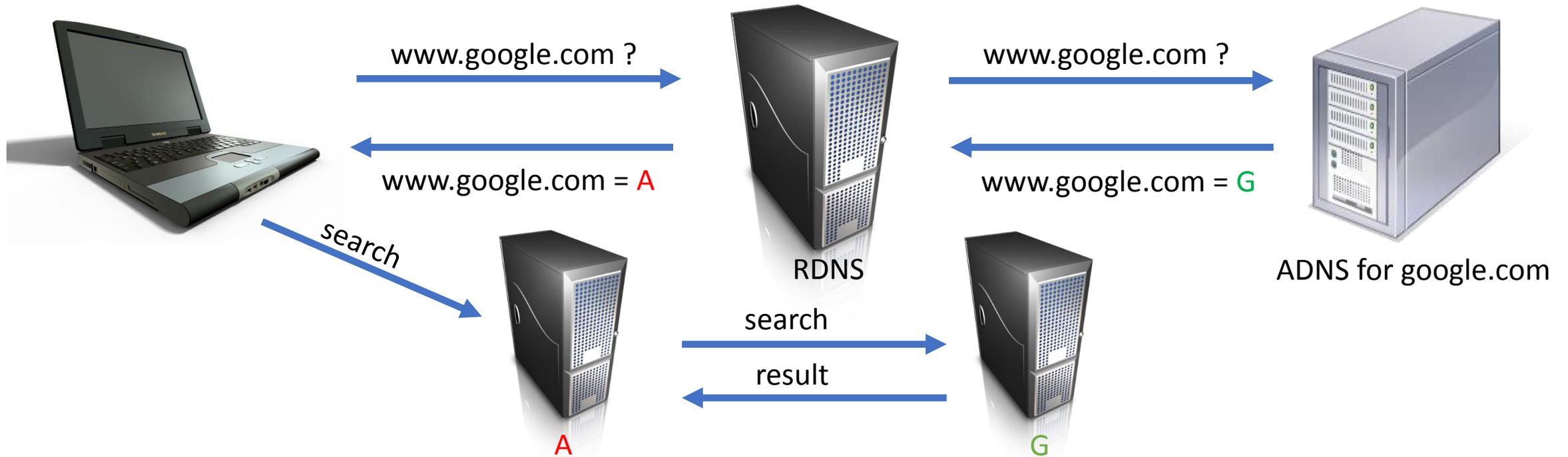
# Search Engine Hijacking (Paxfire)



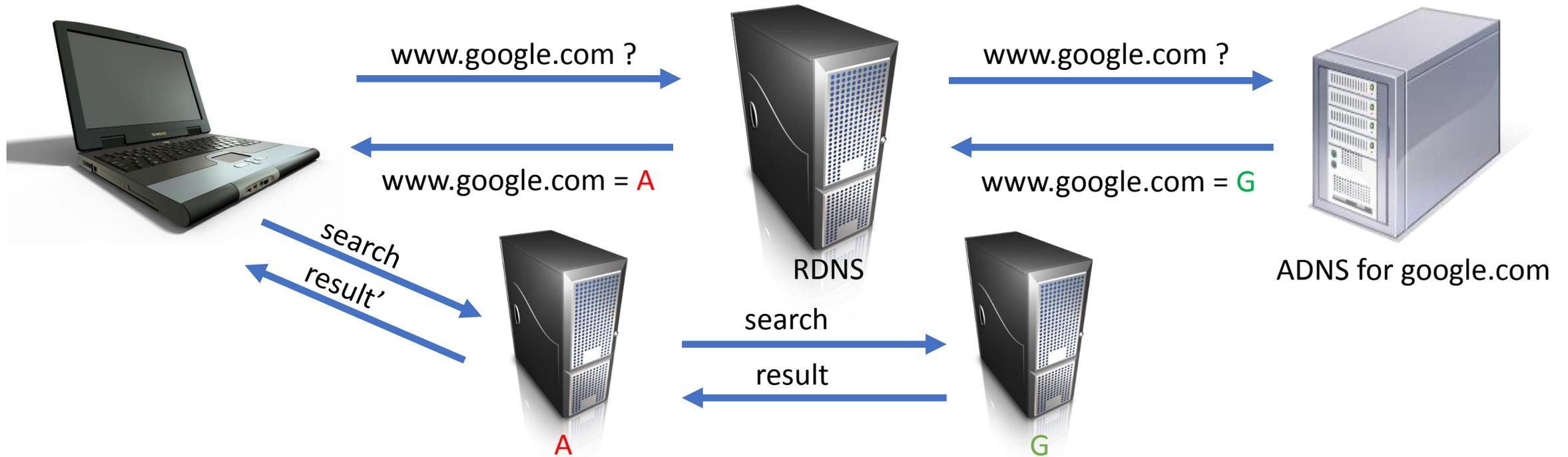
# Search Engine Hijacking (Paxfire)



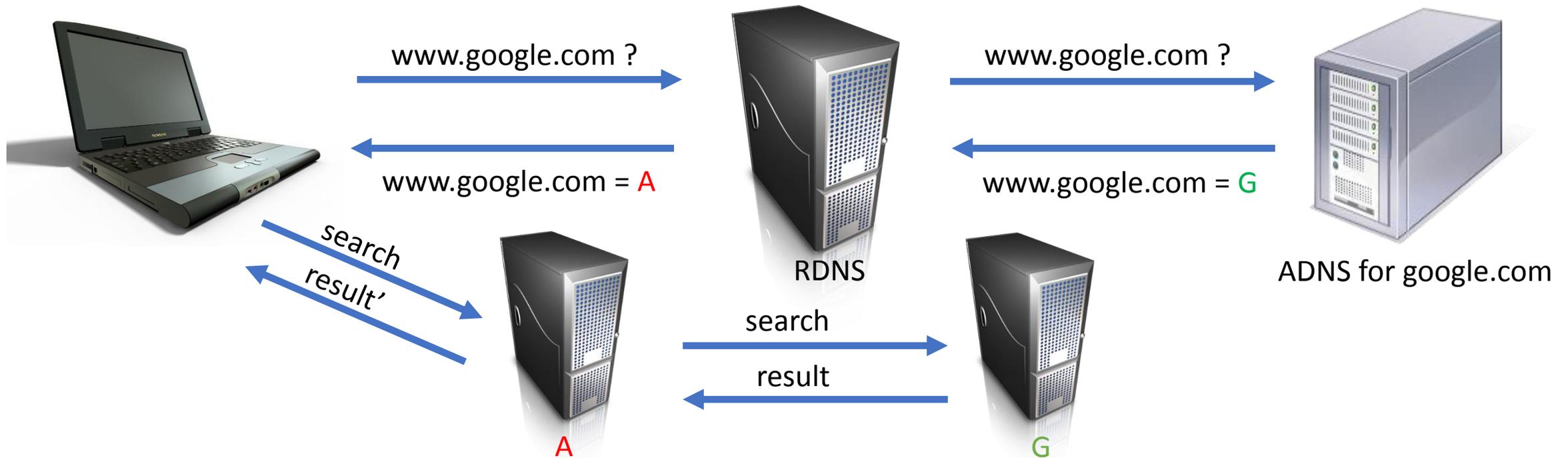
# Search Engine Hijacking (Paxfire)



# Search Engine Hijacking (Paxfire)



# Search Engine Hijacking (Paxfire)



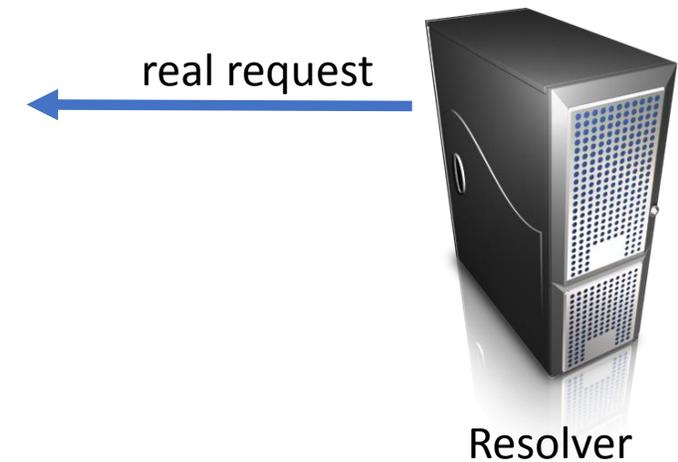
- Again, the primary reason is to monetize user's search traffic
- While once common, this is no longer a widespread practice

# Off-path Attacks

- Craft an acceptable DNS response to squeeze between the real DNS request and response

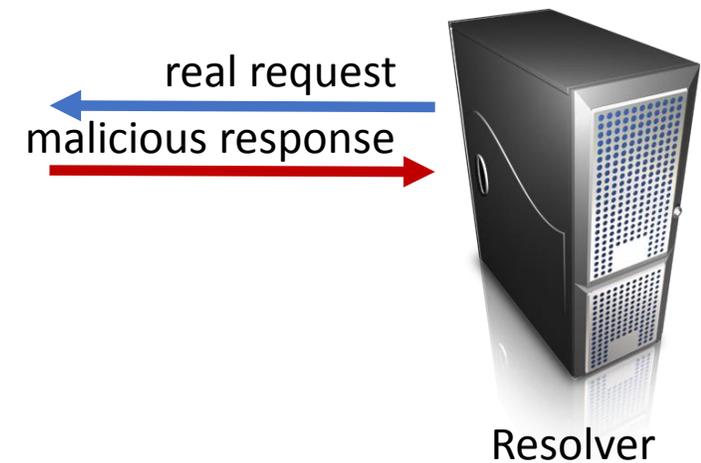
# Off-path Attacks

- Craft an acceptable DNS response to squeeze between the real DNS request and response



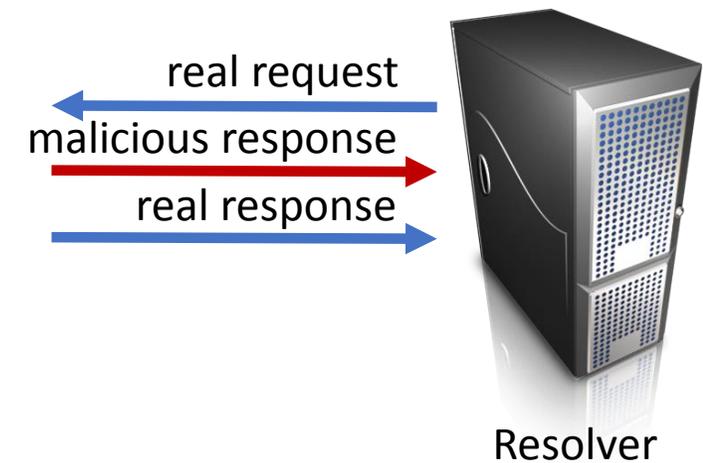
# Off-path Attacks

- Craft an acceptable DNS response to squeeze between the real DNS request and response



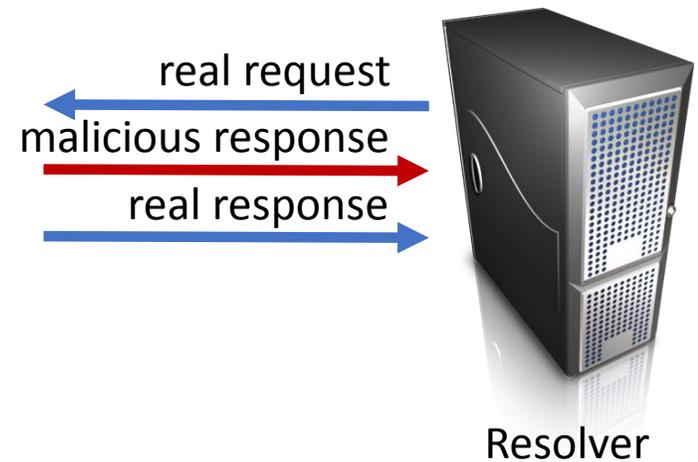
# Off-path Attacks

- Craft an acceptable DNS response to squeeze between the real DNS request and response



# Off-path Attacks

- Craft an acceptable DNS response to squeeze between the real DNS request and response
- Fields to match:
  - IP addresses: source and destination
  - Port numbers: source and destination
  - Query string and transaction ID



# Kaminsky Vulnerability

- In 2008, Dan Kaminsky discovered a new vulnerability
- 2 keys to Kaminsky
  - Transaction ID is the only field the attacker needs to guess
  - Simple way to attempt multiple guesses
- Kaminsky showed that a cache could be poisoned in under 10 minutes!

# Kaminsky Vulnerability (cont.)



Attacker

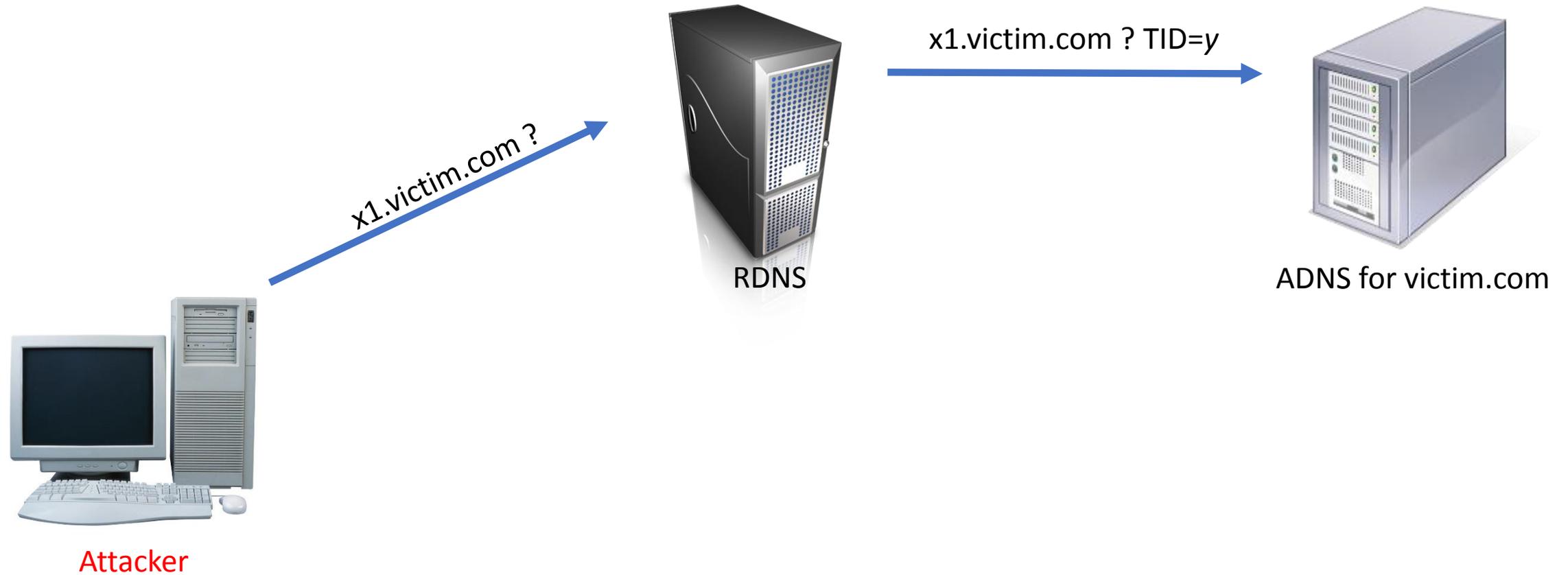


RDNS

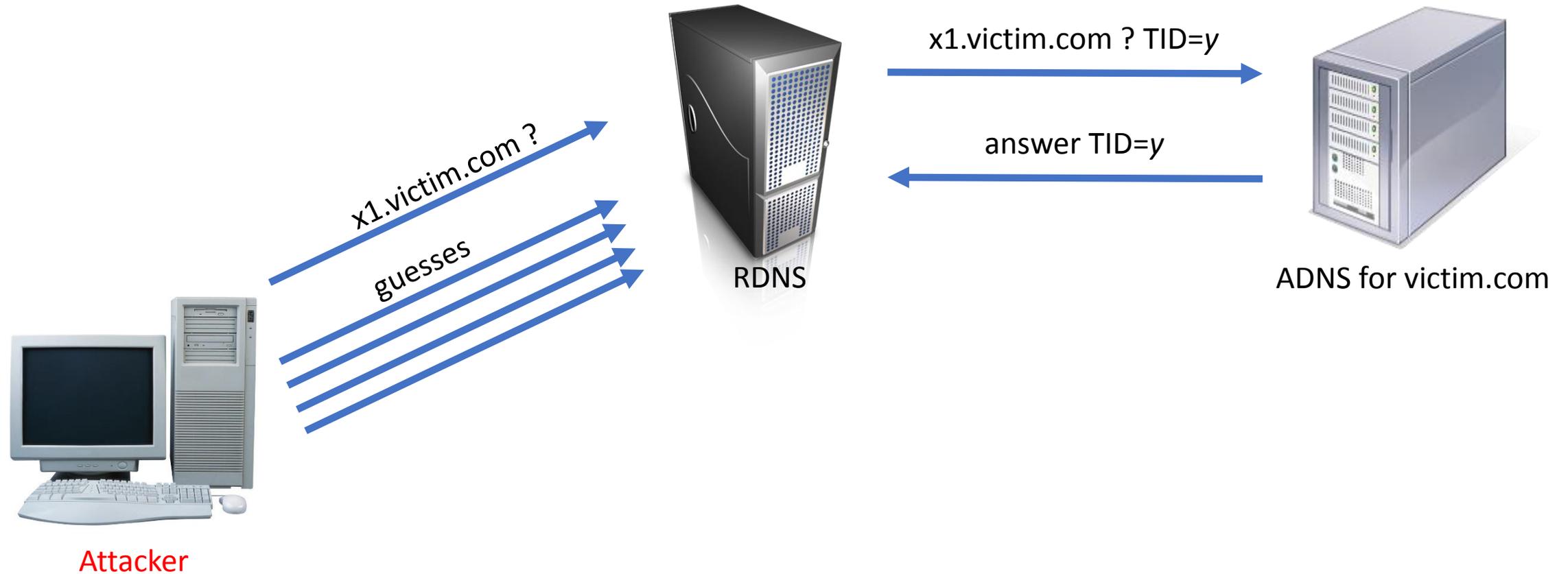


ADNS for victim.com

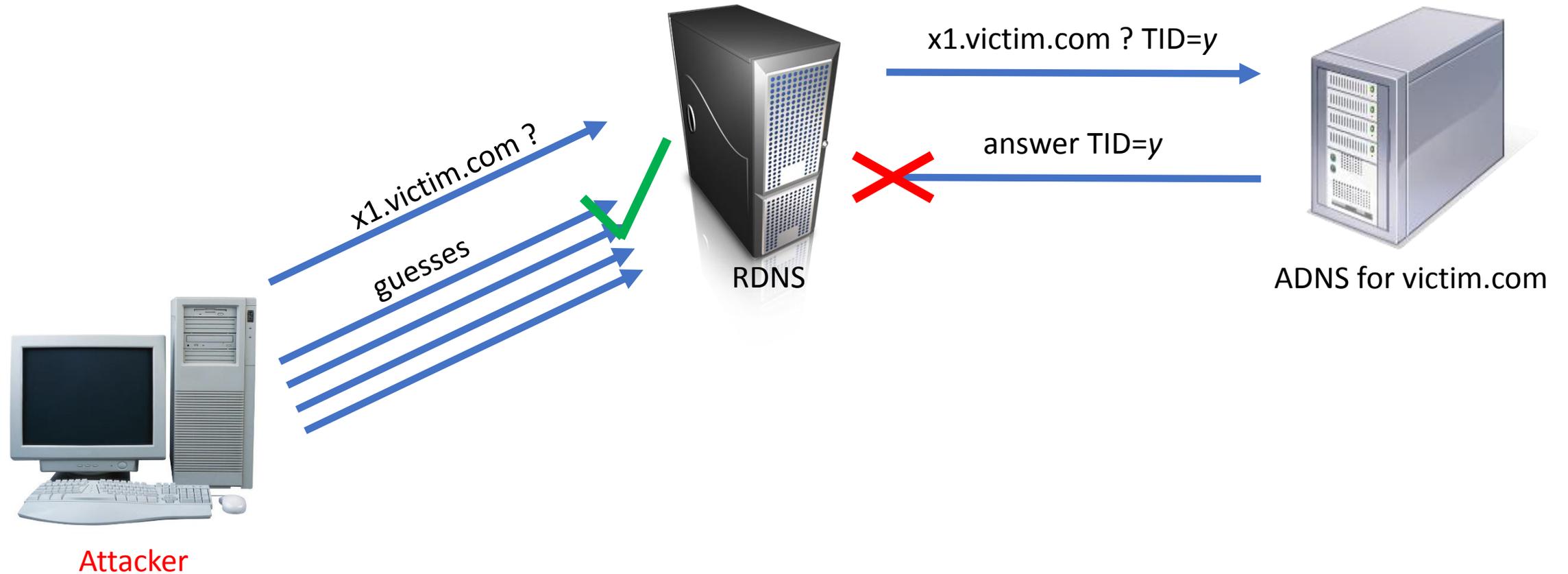
# Kaminsky Vulnerability (cont.)



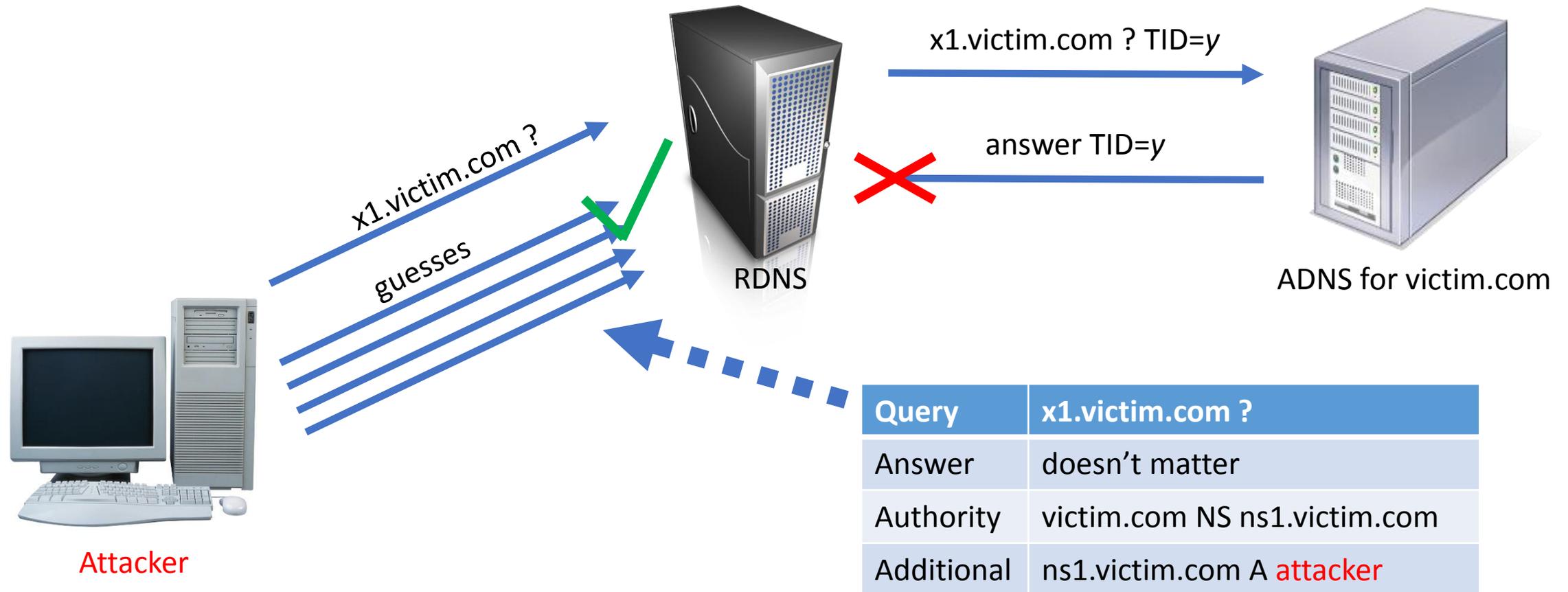
# Kaminsky Vulnerability (cont.)



# Kaminsky Vulnerability (cont.)



# Kaminsky Vulnerability (cont.)



# Kaminsky Vulnerability (cont.)



www.victim.com ?



RDNS

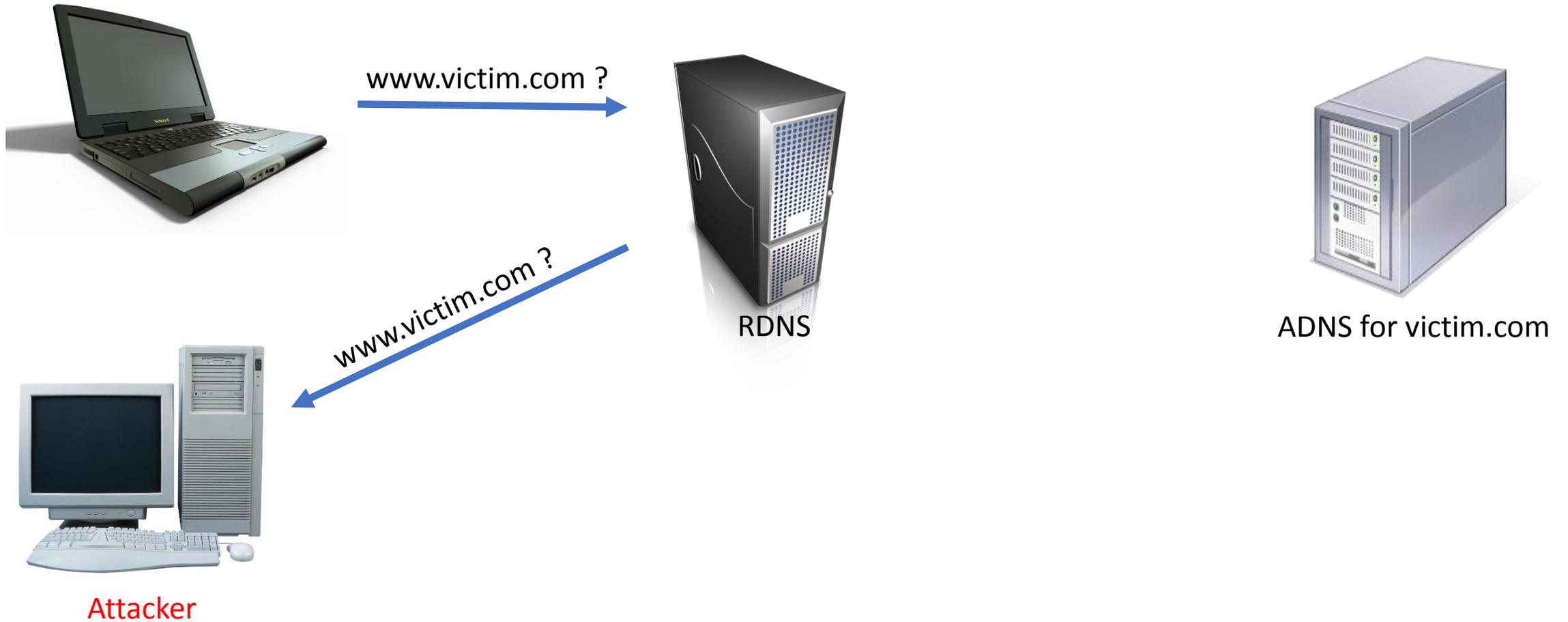


ADNS for victim.com



Attacker

# Kaminsky Vulnerability (cont.)



# Kaminsky Vulnerability (cont.)

- 65K possible transaction IDs
- First attempt likely unsuccessful, so repeat with:
  - x2.victim.com
  - x3.victim.com
  - etc...
- Since none of these names will be in the resolver's cache, can retry *immediately*
- Eventually, the attacker will guess correctly

# Mitigating the Kaminsky Vulnerability

- Add entropy to response beyond just a random transaction ID
- Randomized ephemeral port
- 0x20 encoding
  - Random capitalization of query string, i.e. X1.VicTIm.Com
  - ADNS echoes the capitalization back
  - Attacker must guess capitalization
  - 1 bit of entropy per letter in query string
- DNSSEC and ingress filtering defeat the Kaminsky Attack
  - Slow progress means mitigation is needed

# Survey of Mitigations to Kaminsky

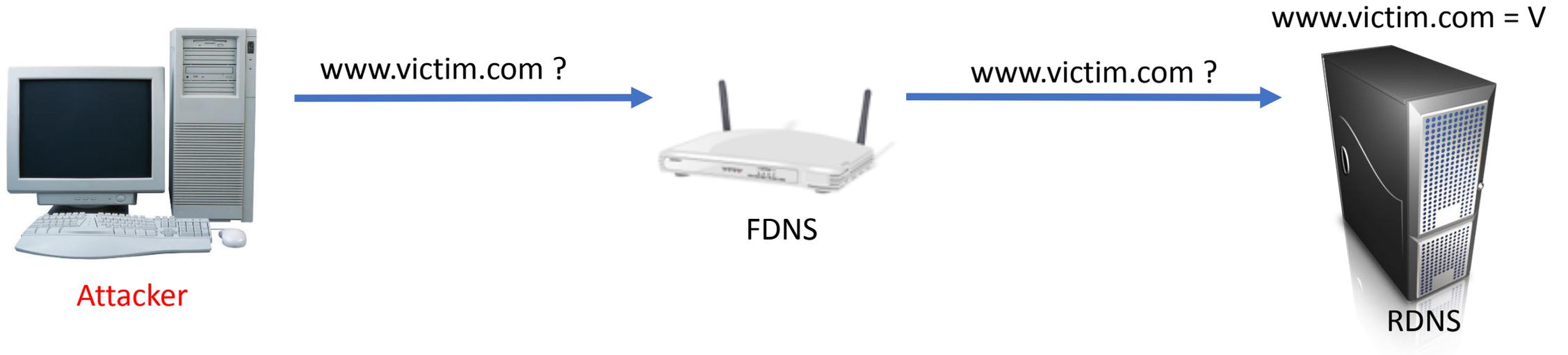
- Send multiple DNS requests through each RDNS
  - Classify RDNS where 10 or more DNS requests arrive at our ADNS
- Nearly all classified resolvers appear to use random transaction IDs
- 16% of classified resolvers use *static* ephemeral ports!
- 0x20 encoding rare
  - (lower bound)

Observation	RDNS	
	Number	Percentage
Total Classified	57K	100%
Complex Transaction ID Sequence	57K	100%
Variable Ephemeral Port	48K	84%
0x20 Encoding	195	0.3%

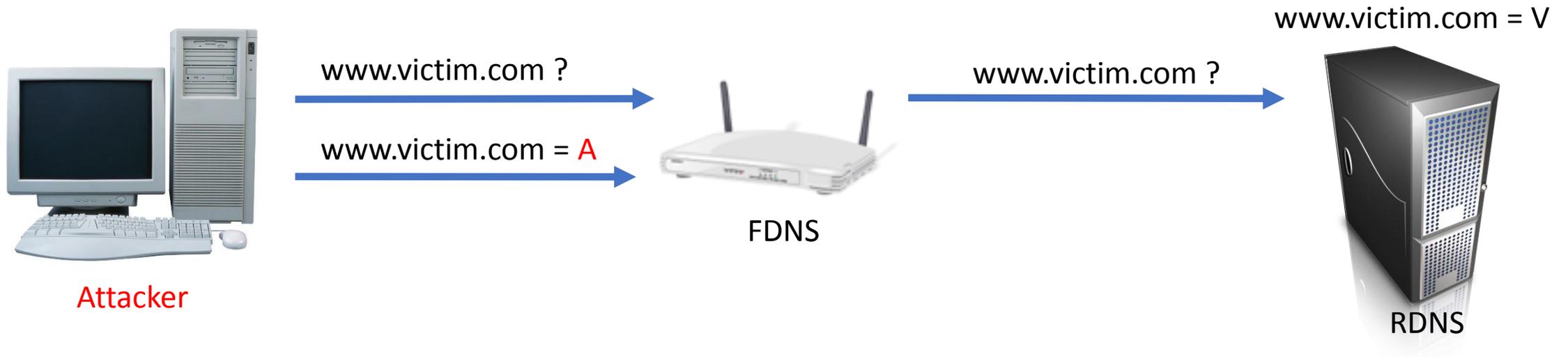
# Preplay Vulnerability

- If RDNS are vulnerable, what about FDNS?
- FDNS:
  - Residential locations
  - Most likely home wifi routers
  - Little attention paid to security
- We found that FDNS have a vulnerability that is much easier to exploit than the Kaminsky vulnerability

# Preplay Vulnerability (cont.)



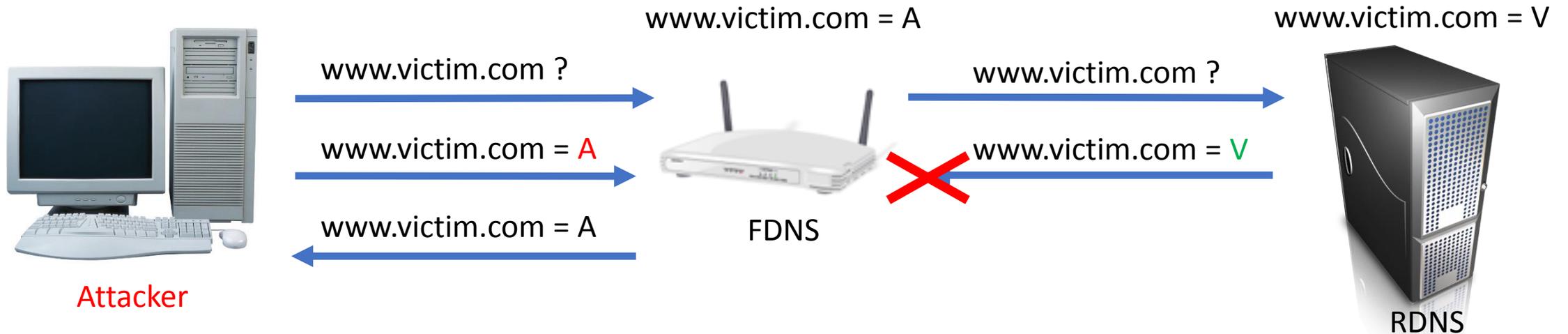
# Preplay Vulnerability (cont.)



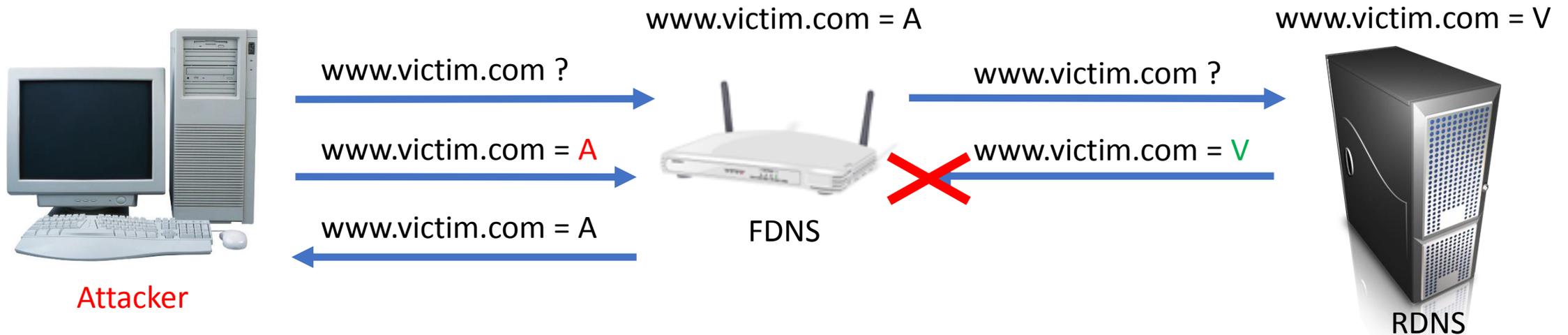
# Preplay Vulnerability (cont.)



# Preplay Vulnerability (cont.)



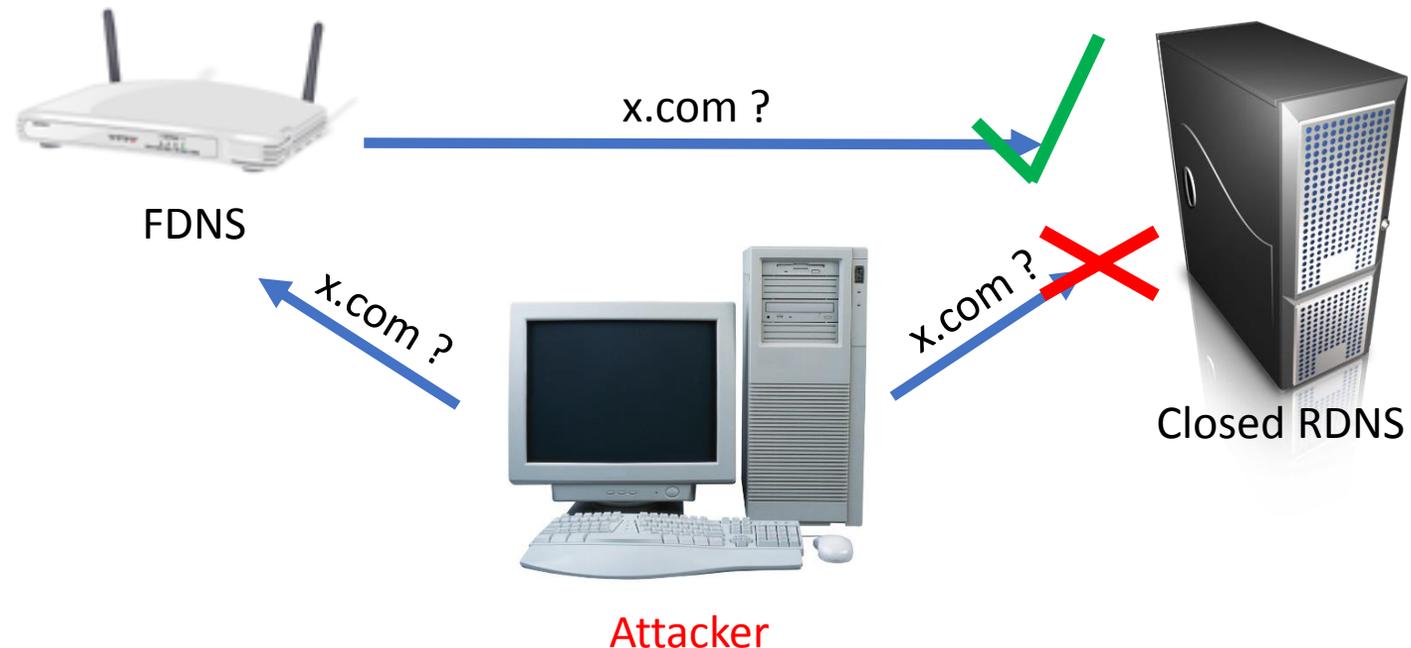
# Preplay Vulnerability (cont.)



- RDNS IP address, transaction ID, and port numbers are not validated!
- 7-9% FDNS are vulnerable
- 2-3 million out of the ~32 million open resolvers on the Internet

# Implication: Indirect Attacks

- 62% of RDNS are closed, yet still accessible through FDNS
- FDNS are an avenue to detect and attack closed resolvers



# Implication: Phantom DDoS Attacks



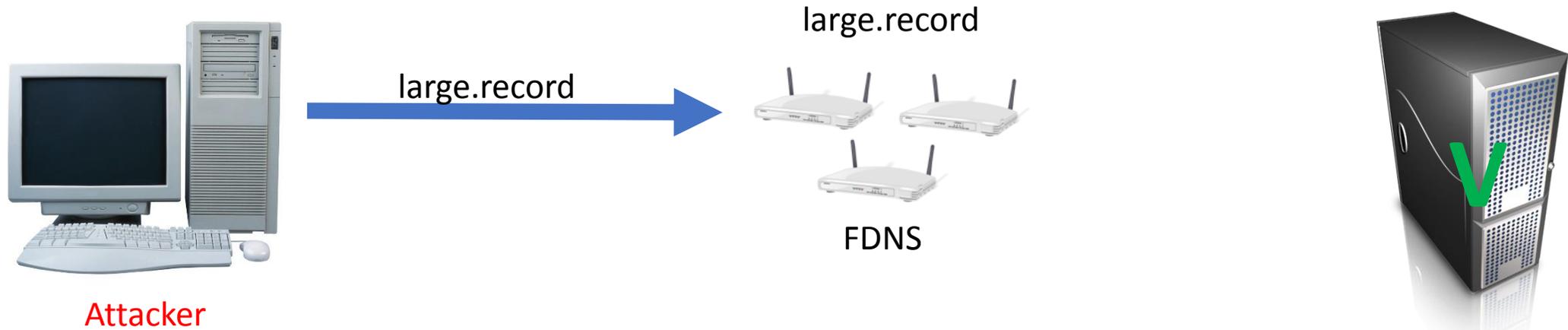
Attacker



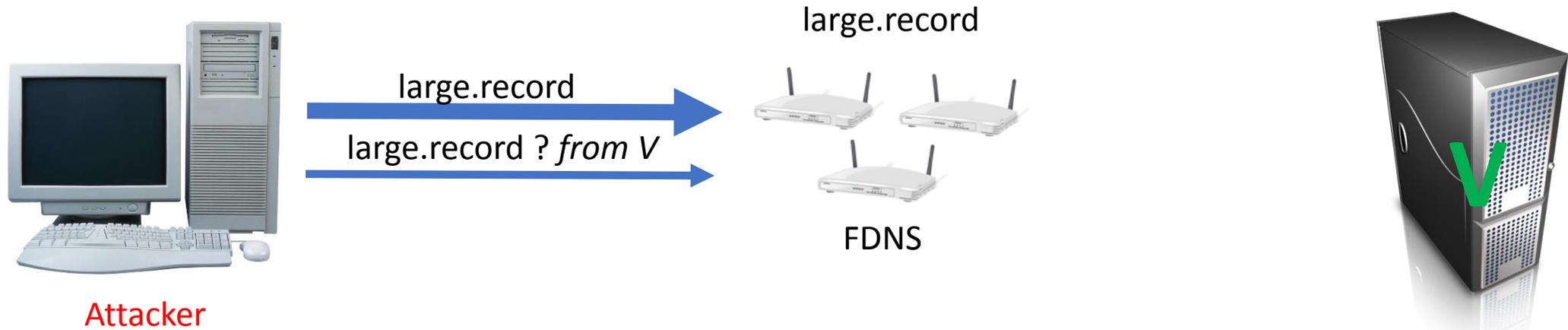
FDNS



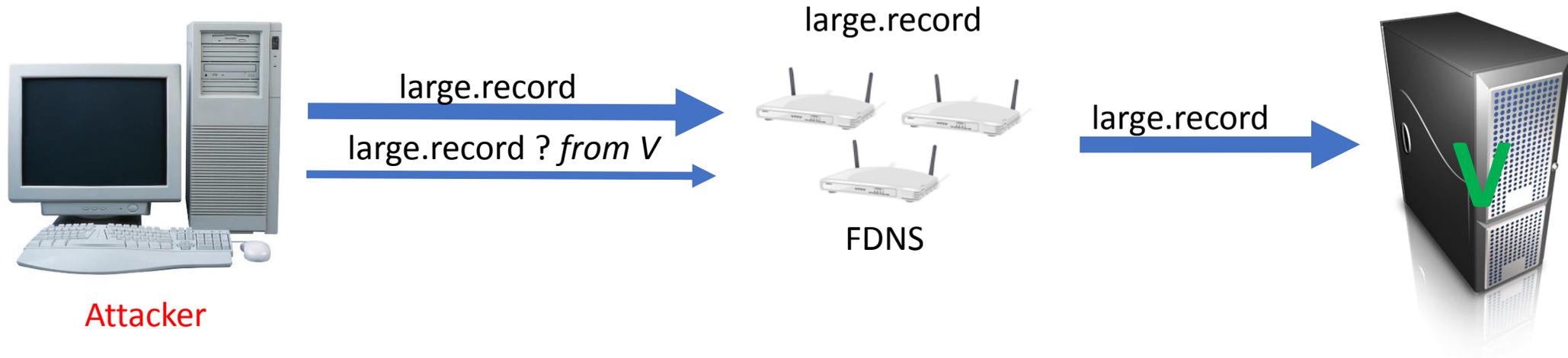
# Implication: Phantom DDoS Attacks



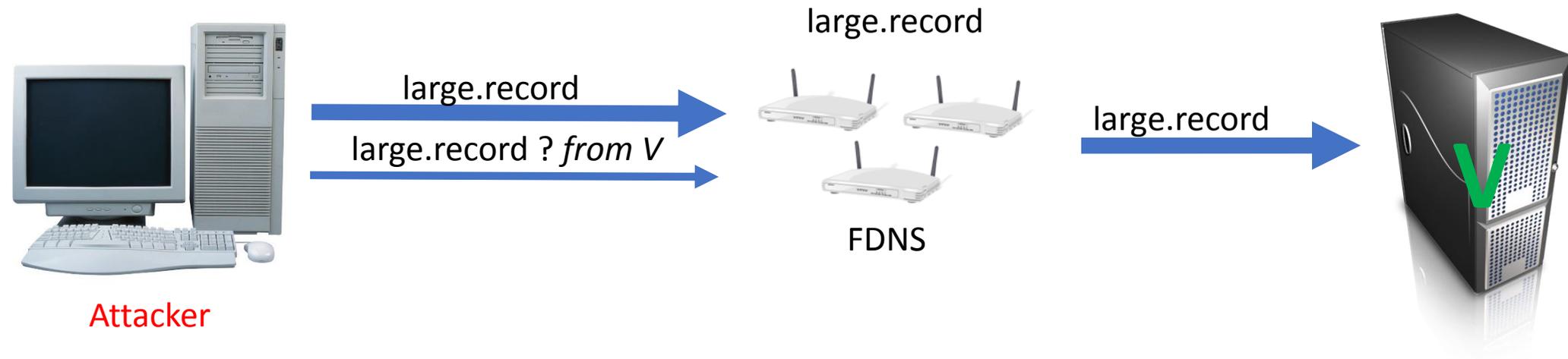
# Implication: Phantom DDoS Attacks



# Implication: Phantom DDoS Attacks



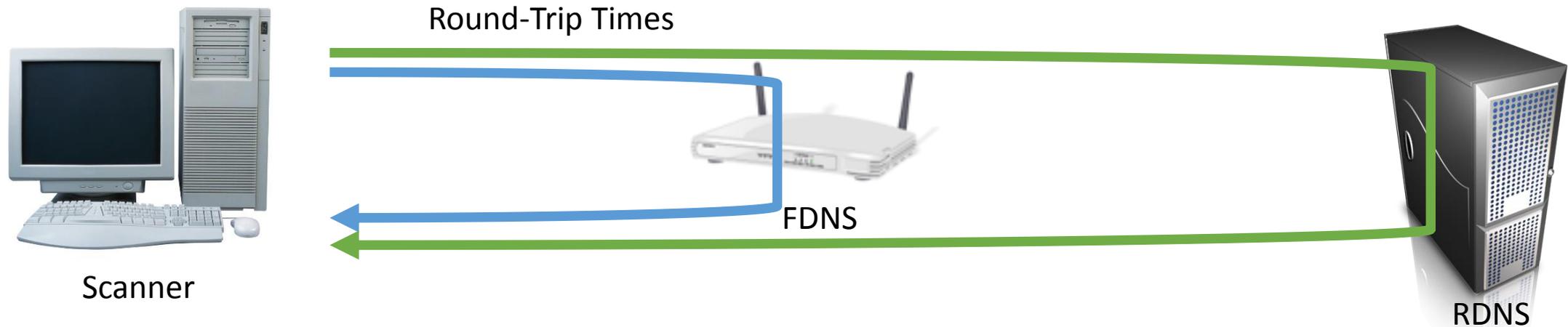
# Implication: Phantom DDoS Attacks



- Advantages for an attacker:
  - Achieve maximum amplification
  - Do not need ADNS
  - Or even a registered DNS record

# Context: Are Preplay Vulnerable FDNS Used?

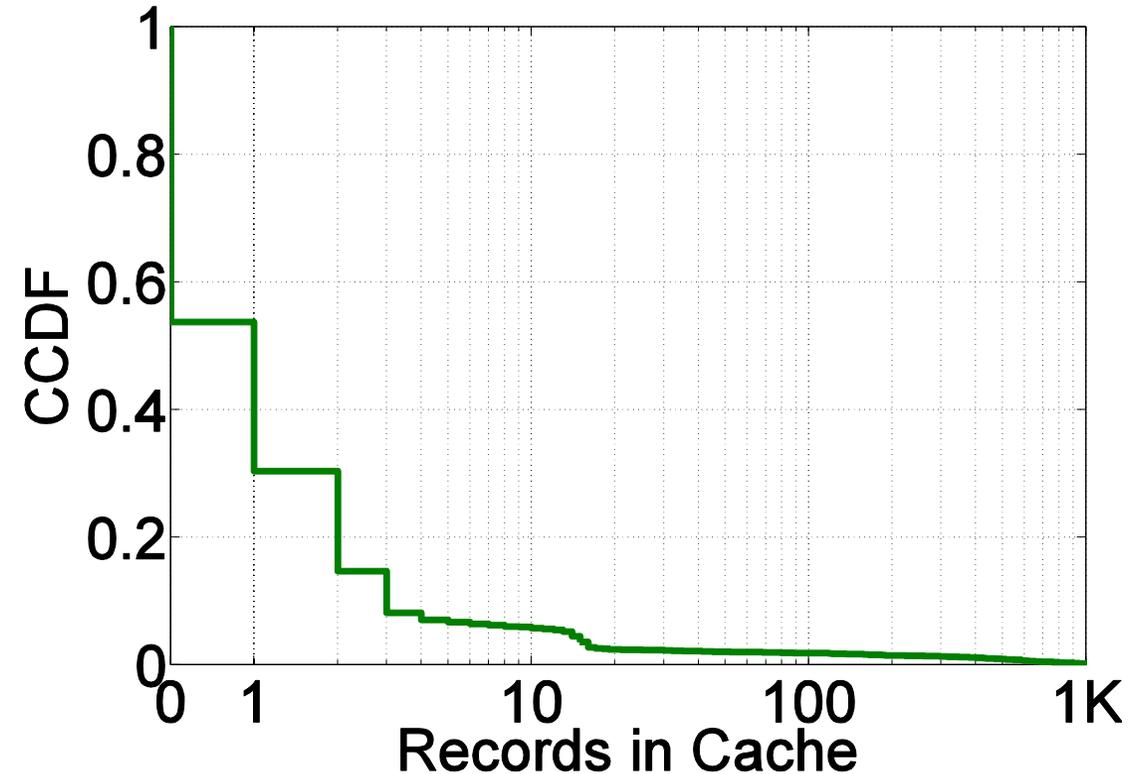
- Attack only effective if there are users behind the FDNS
- We test FDNS for use by looking for popular records in the FDNS's cache



- If a popular record returned in  $\ll$  RDNS RTT and  $\approx$  FDNS RTT, then FDNS is used

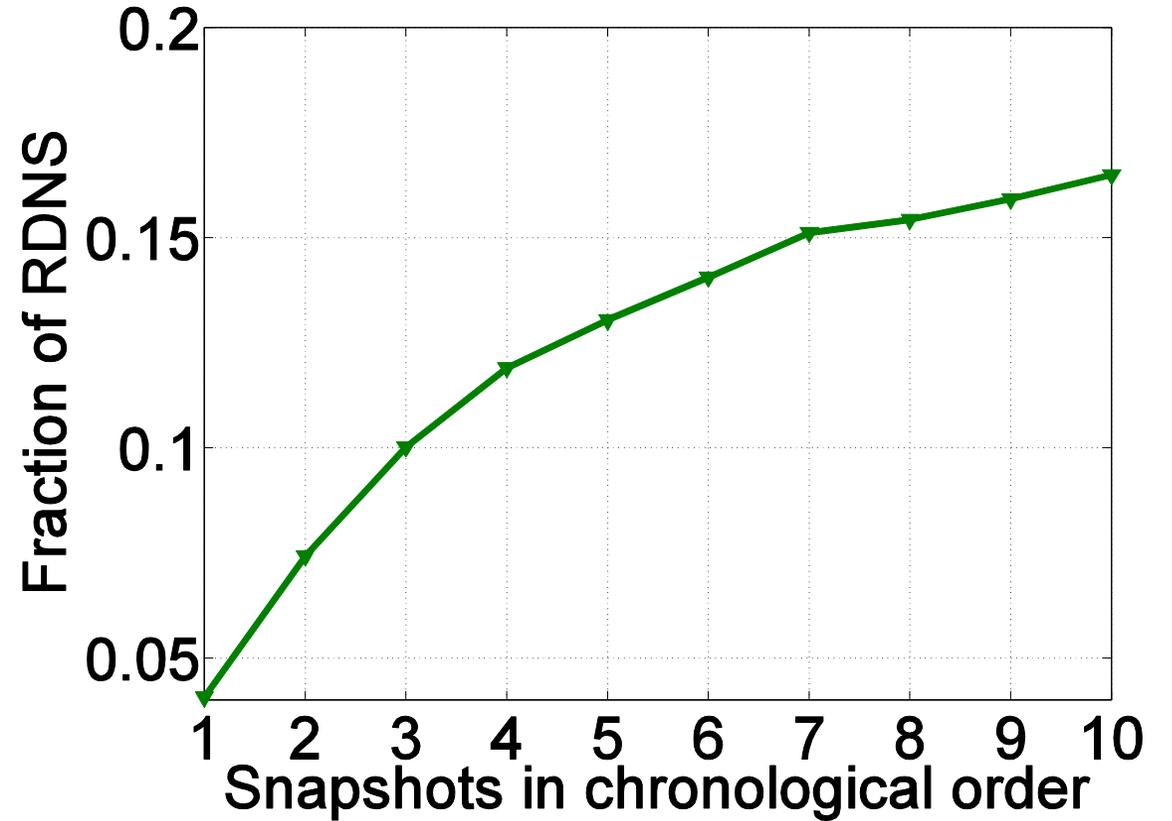
# Context: Preplay Vulnerable FDNS Are Used!

- 53% of FDNS have 1 or more popular records in cache
  - (lower bound)
- So, many Preplay vulnerable FDNS are used



# Context: Effects of Sampling on RDNS

- RDNS discovery dependent upon FDNS that share the RDNS
- Fraction of RDNS vulnerable to Kaminsky continues to grow
- Frequently shared RDNS *less vulnerable* to Kaminsky
  - 3% of FDNS in front of Kaminsky vulnerable RDNS



# Summary

- Bailiwick violations are rare
- Negative response rewriting occurs in 24% of FDNS
- Search engine hijacking no longer prevalent
- 16% of RDNS still have the Kaminsky vulnerability
  - But these are the less frequently used RDNS
- 7-9% of FDNS (2-3M) can be trivially poisoned due to the Preplay vulnerability

# Thank you! Questions?

Kyle Schomp – [kgs7@case.edu](mailto:kgs7@case.edu)

For access to our datasets: <http://dns-scans.eecs.cwru.edu/>

# Additional Slides

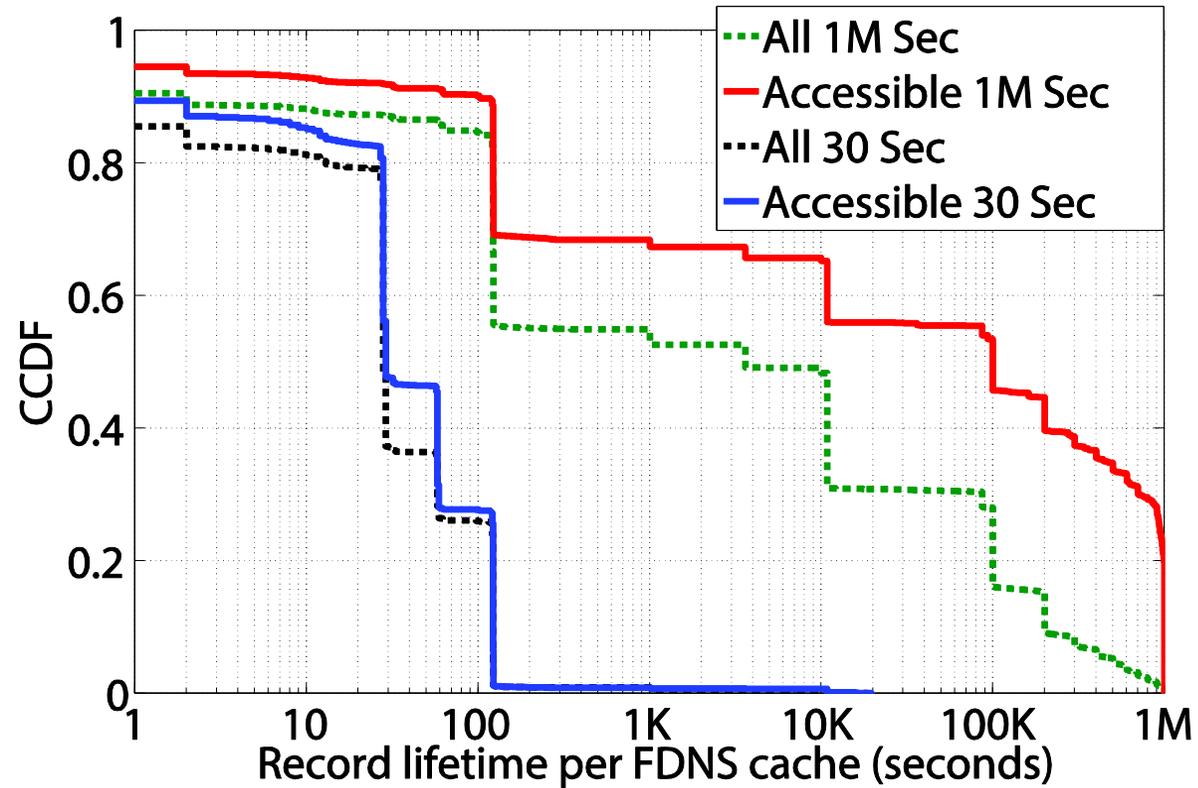
# Datasets

Scan	Start	Dur. (days)	ODNS	RDNS
$S_1$	2/29/12	17	1.09M	69.5K
$S_2$	3/1/13	11	40.5K	5.3K
$S_3$	7/9/13	12	2.31M	86.1K

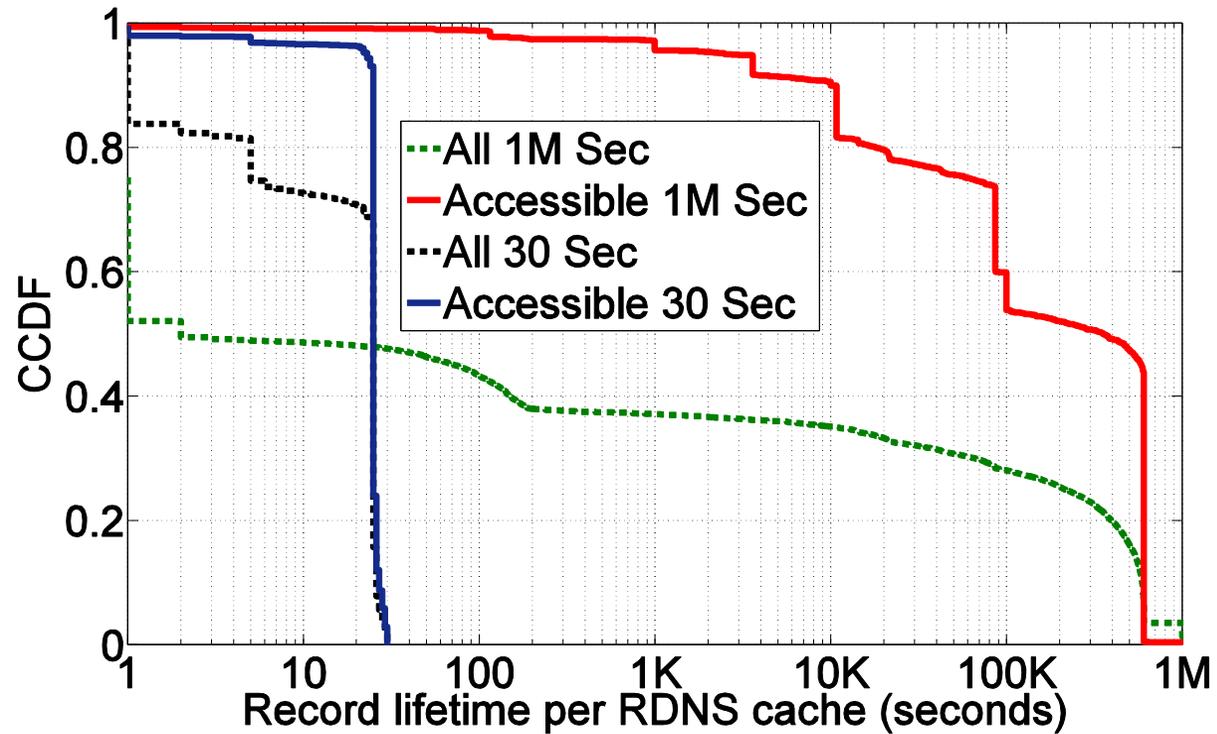
# Residential Network Device Criteria

Criterion	No. ODNSES	% ODNSES
RomPager	258K	24%
Basic auth realm	265K	24%
PBL Listed by SpamHaus	566K	51%
PBL Listed by ISP	180K	17%
Wrong port	529K	48%
<b>Total</b>	<b>849K</b>	<b>78%</b>

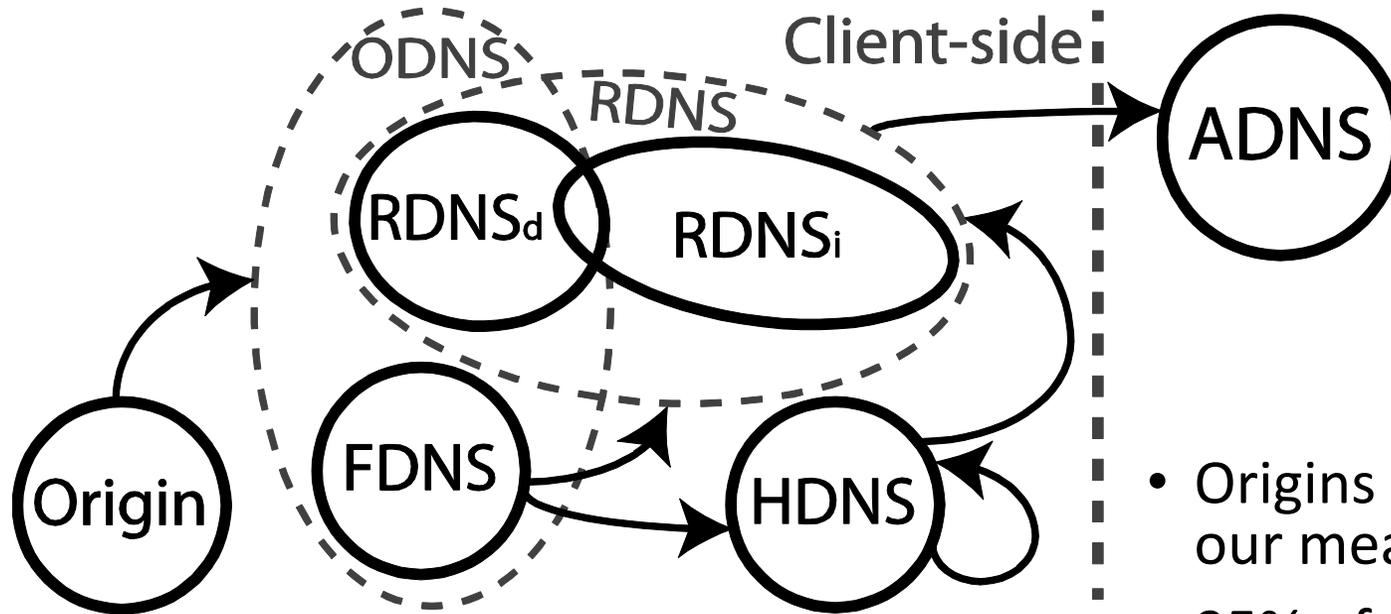
# FDNS Cache Behavior



# RDNS Cache Behavior



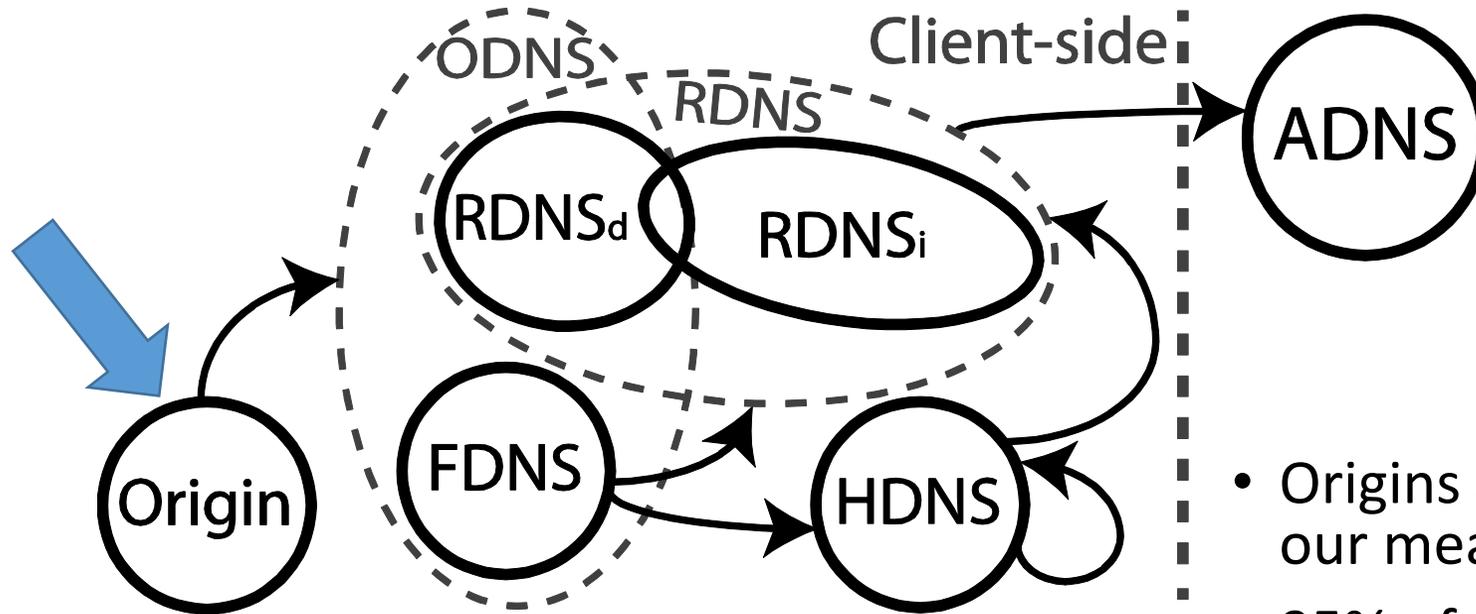
# The Client-Side DNS Infrastructure



Structure of the client-side DNS infrastructure observed in our datasets.

- Origins are either end user devices or our measurement points
- 95% of ODNS are FDNS
- 78% of ODNS are likely residential network devices

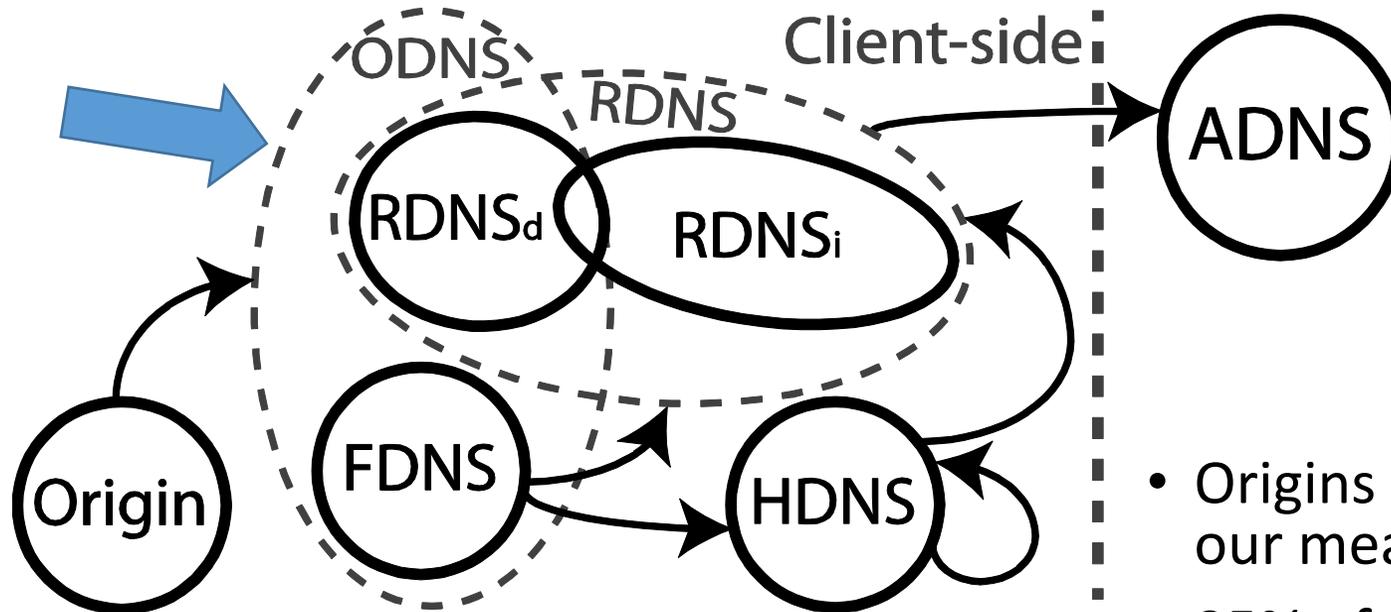
# The Client-Side DNS Infrastructure



Structure of the client-side DNS infrastructure observed in our datasets.

- Origins are either end user devices or our measurement points
- 95% of ODNS are FDNS
- 78% of ODNS are likely residential network devices

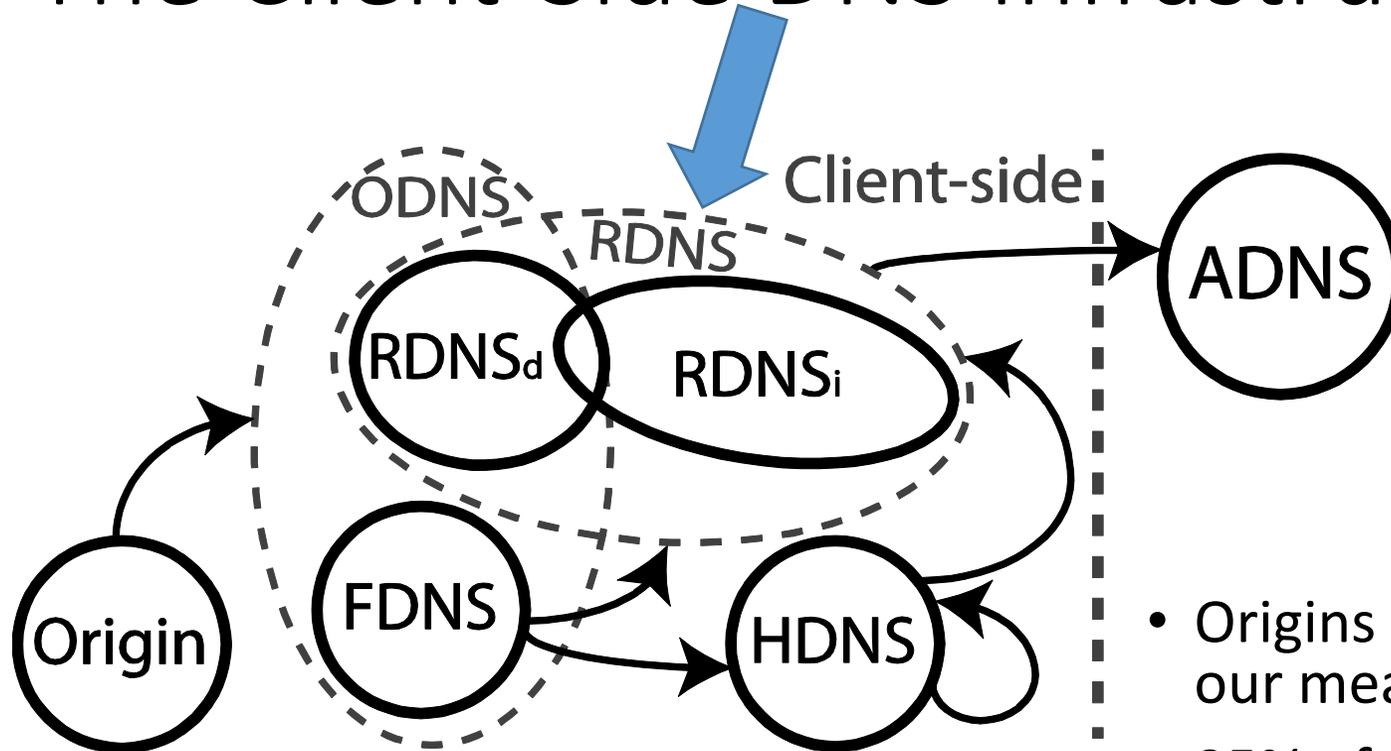
# The Client-Side DNS Infrastructure



Structure of the client-side DNS infrastructure observed in our datasets.

- Origins are either end user devices or our measurement points
- 95% of ODNS are FDNS
- 78% of ODNS are likely residential network devices

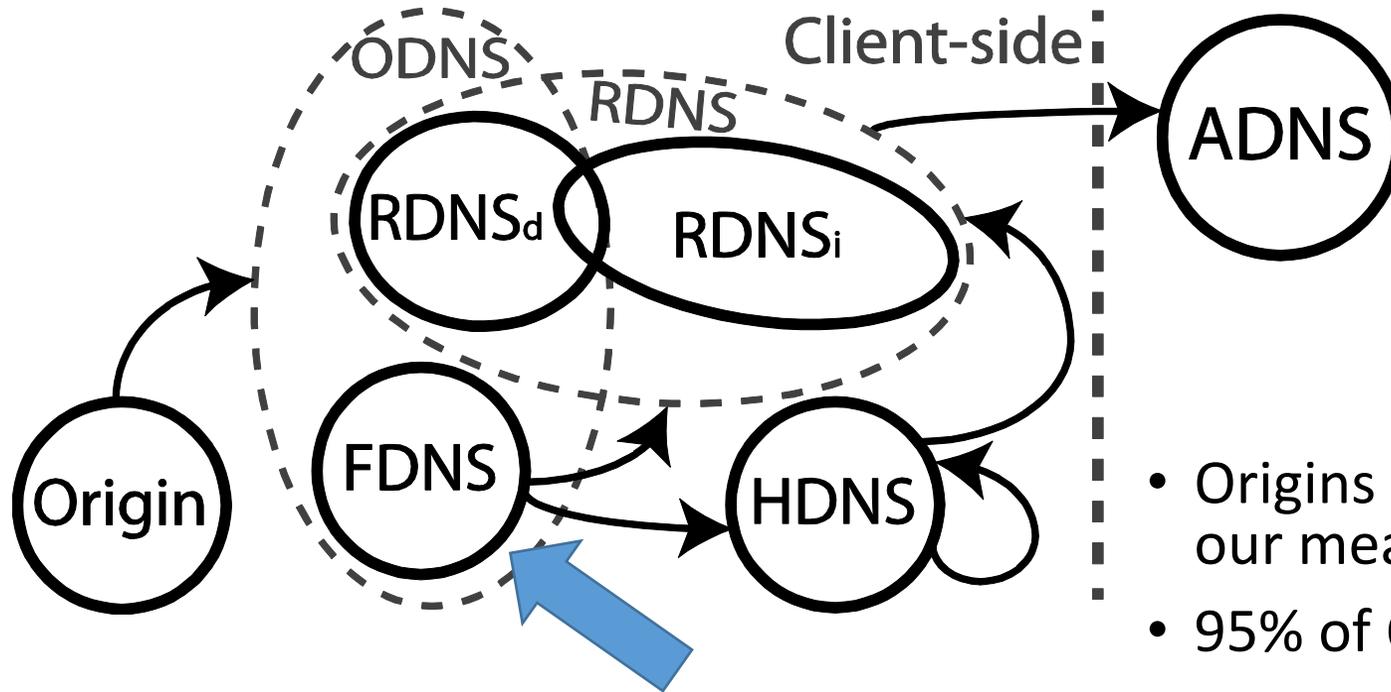
# The Client-Side DNS Infrastructure



Structure of the client-side DNS infrastructure observed in our datasets.

- Origins are either end user devices or our measurement points
- 95% of ODNS are FDNS
- 78% of ODNS are likely residential network devices

# The Client-Side DNS Infrastructure



Structure of the client-side DNS infrastructure observed in our datasets.

- Origins are either end user devices or our measurement points
- 95% of ODNS are FDNS
- 78% of ODNS are likely residential network devices

# Presentation Organization

- The Attacks
- Implications of our findings
  - Indirect Attacks, Phantom Amplification Attacks
- Context for our findings
  - Are FDNS Used, Effects of Sampling
- Summary