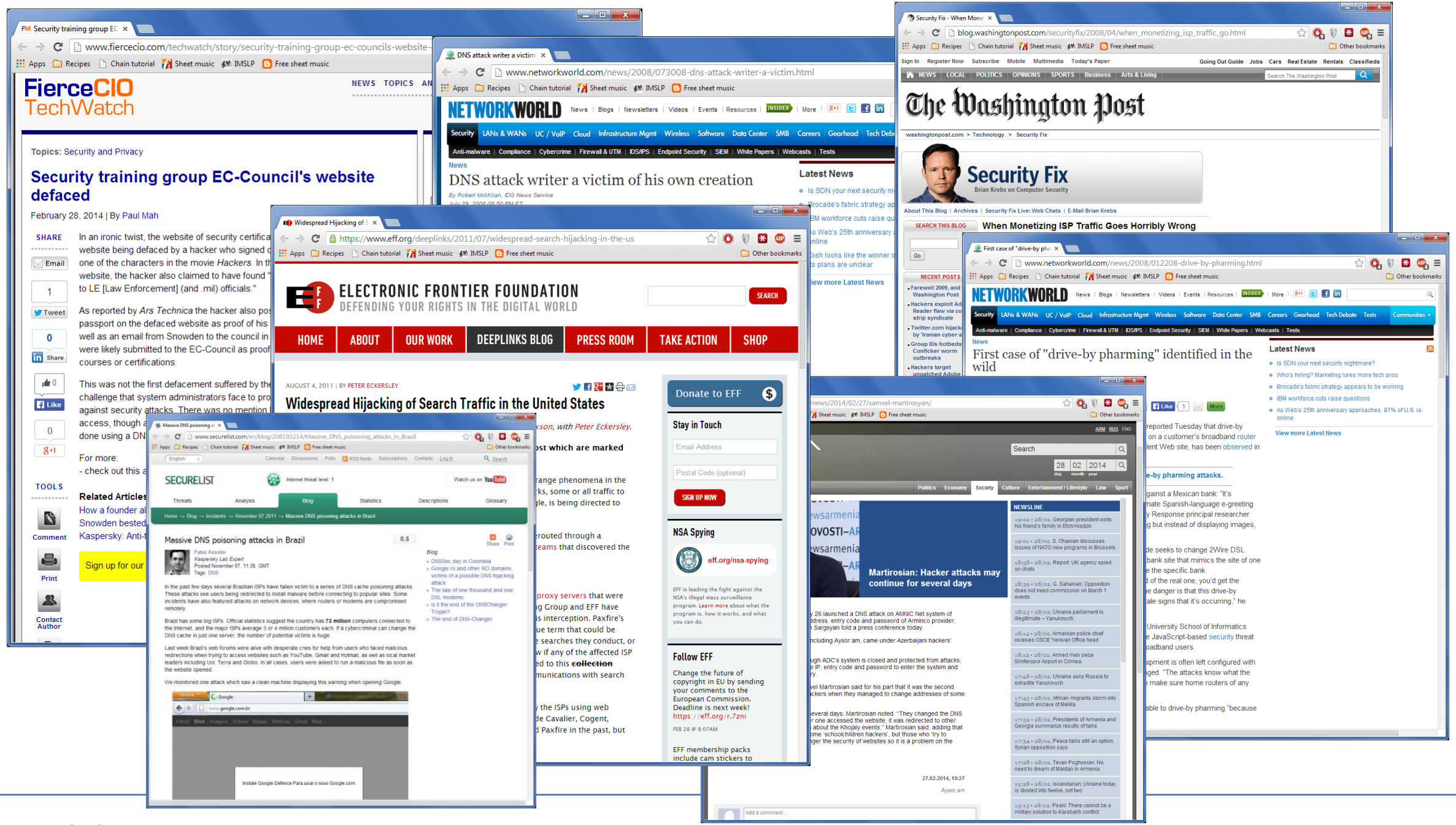
Assessing DNS Vulnerability to Record Injection

Kyle Schomp†, Tom Callahan†, Michael Rabinovich†, Mark Allman†‡

†Case Western Reserve University

‡International Computer Science Institute

Passive and Active Measurement Conference 2014


FierceCIO TechWatch
Topics: Security and Privacy
Security training group EC-Council's website defaced
February 28, 2014 | By Paul Mah
NETWORKWORLD
DNS attack writer a victim of his own creation
The Washington Post
Security Fix
Brian Krebs on Computer Security
When Monetizing ISP Traffic Goes Horribly Wrong
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
Widespread Hijacking of Search Traffic in the United States
First case of "drive-by pharming" identified in the wild
Massive DNS poisoning attacks in Brazil
SECURELIST
Martirosian: Hacker attacks may continue for several days

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)

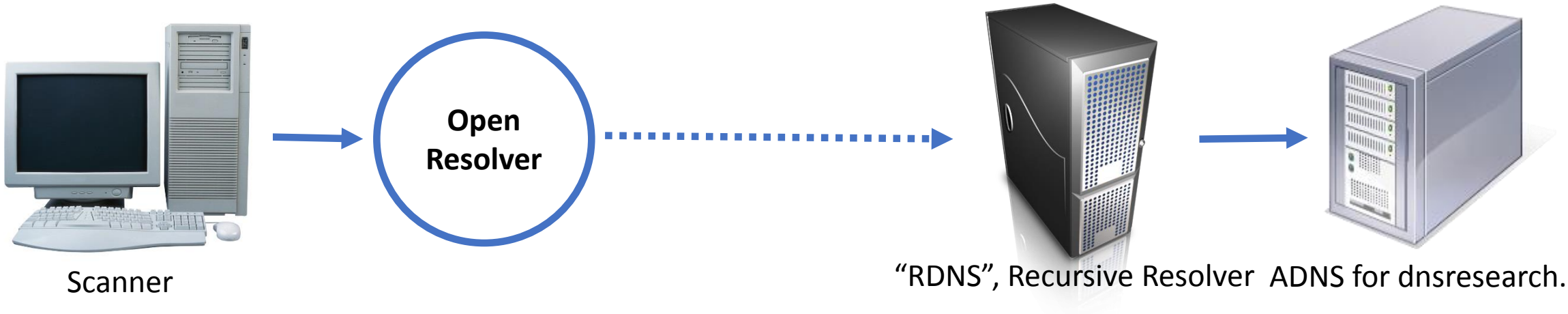
Dataset Collection Methodology

- 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

Scanner "FDNS", Forwarding Resolver "RDNS", Recursive Resolver ADNS for dnsresearch.us

- Test open and egress resolvers for vulnerability to record injection

Dataset Collection Methodology

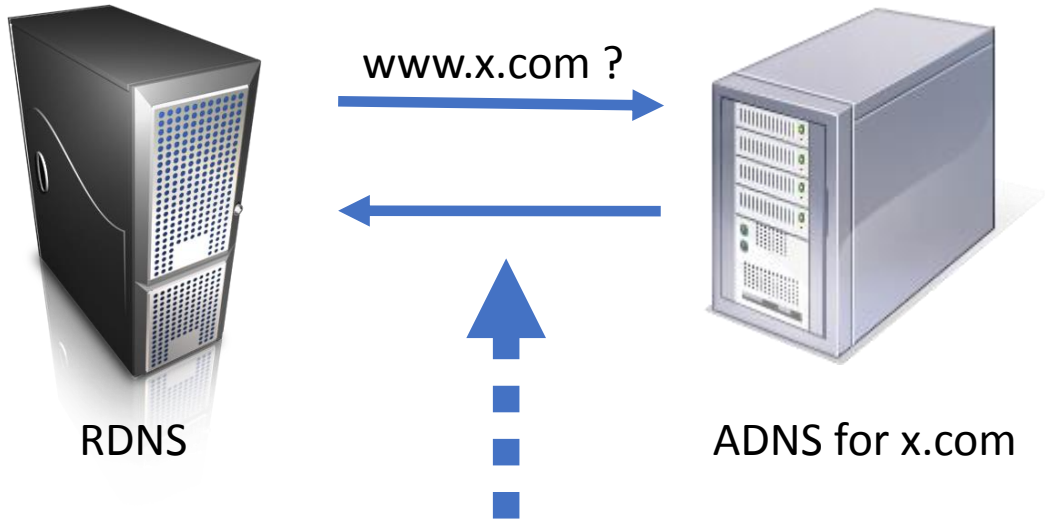
- Discover open resolvers by sampling randomly from the Internet
- Deploy our own authoritative DNS server (*ADNS*)
- DNS request probes target our own domain

Client "FDNS", Forwarding Resolver "RDNS", Recursive Resolver ADNS for dnsresearch.us

- Test open and egress resolvers for vulnerability to record injection

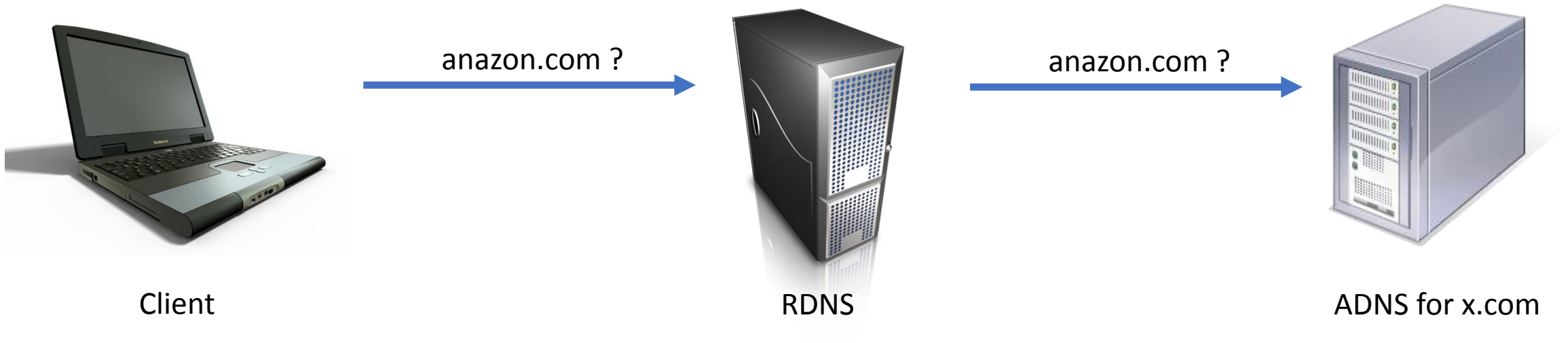
Bailiwick Violations

- 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!

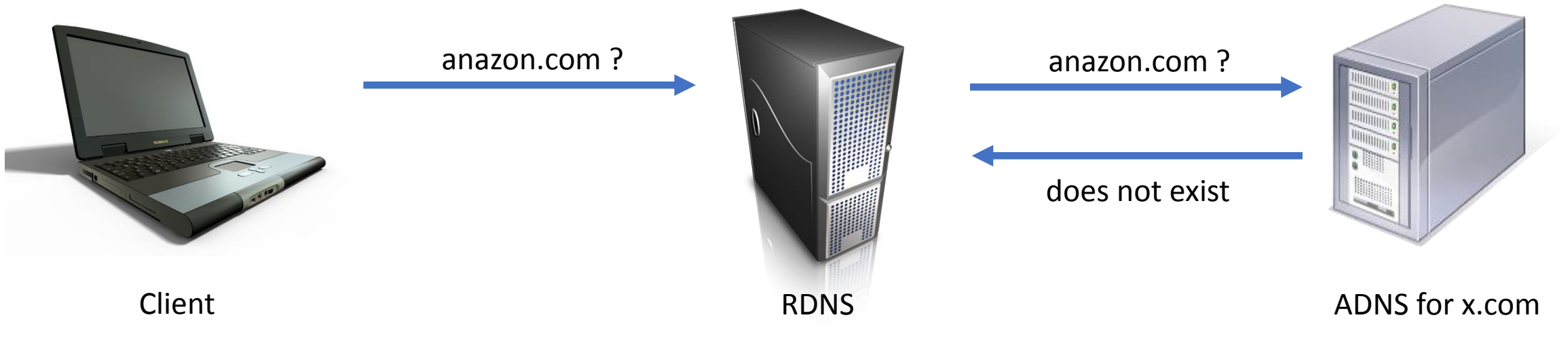


Query	www.x.com ?
Answer	1.2.3.4
Additional	www.hsbc.com A 2.3.4.5

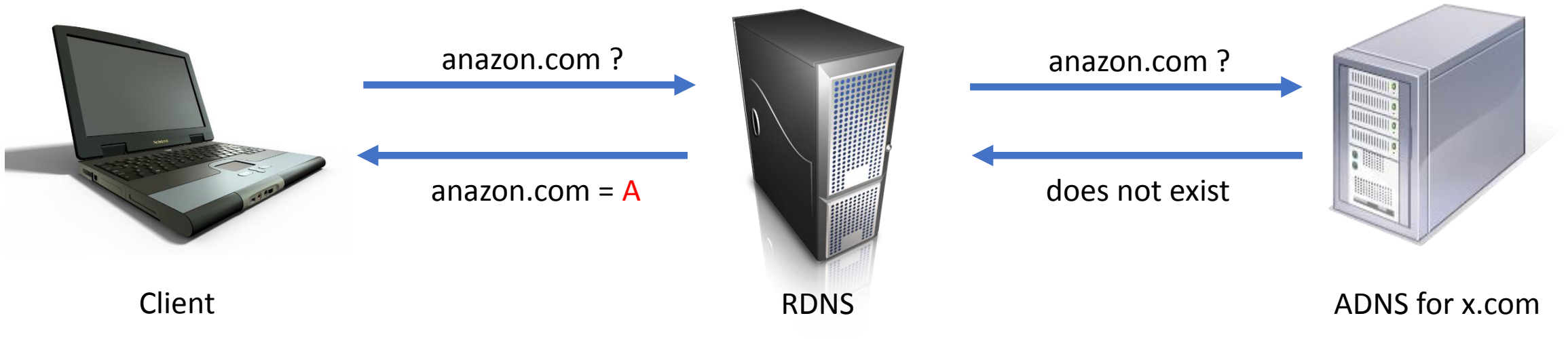
Negative Response Rewriting



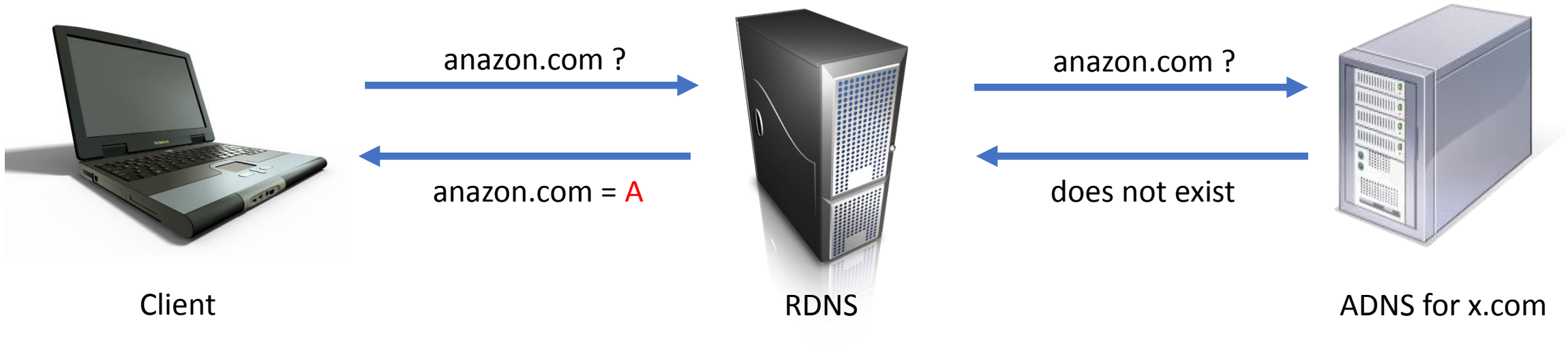
Negative Response Rewriting



Negative Response Rewriting

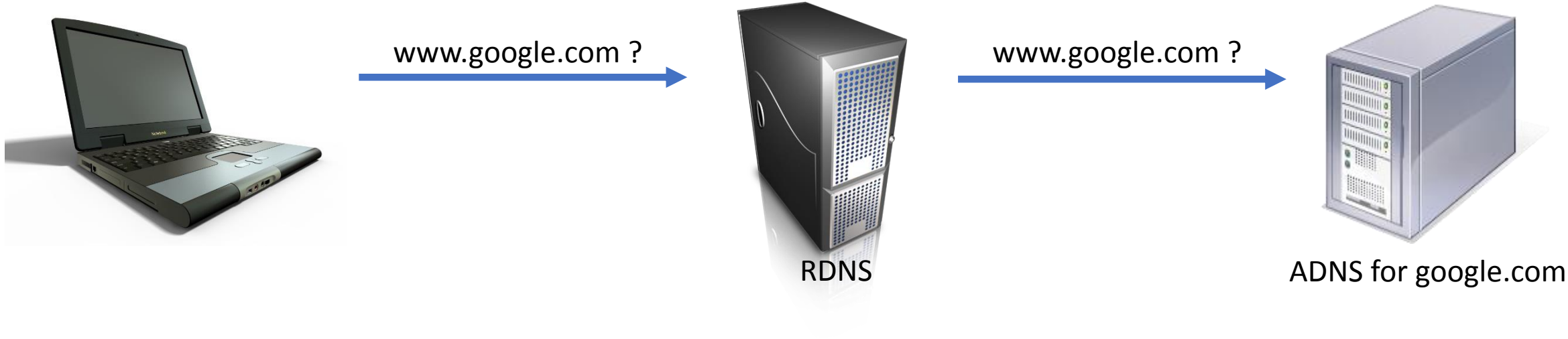


Negative Response Rewriting

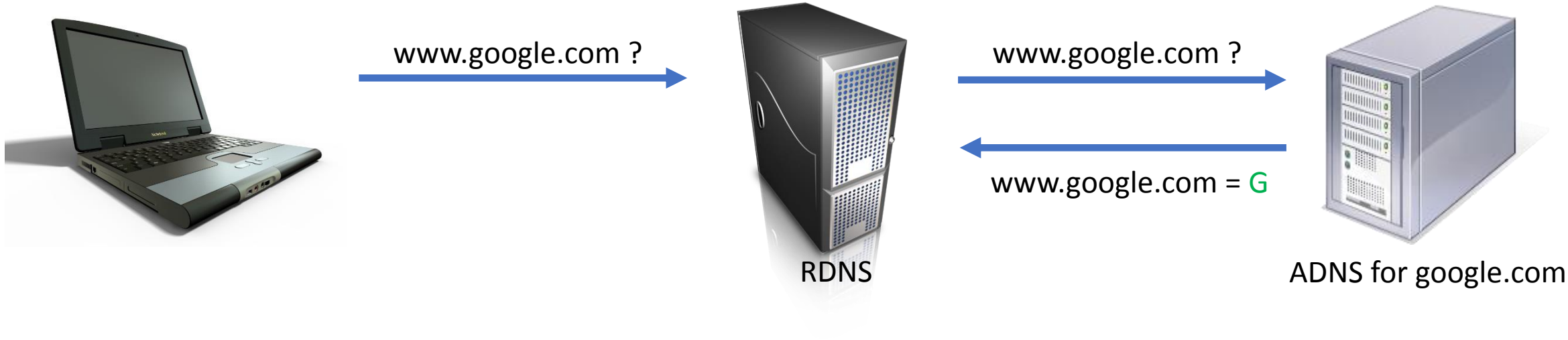


- Why? DNS provider profits from advertising at A
- Happens to 24% of open resolvers

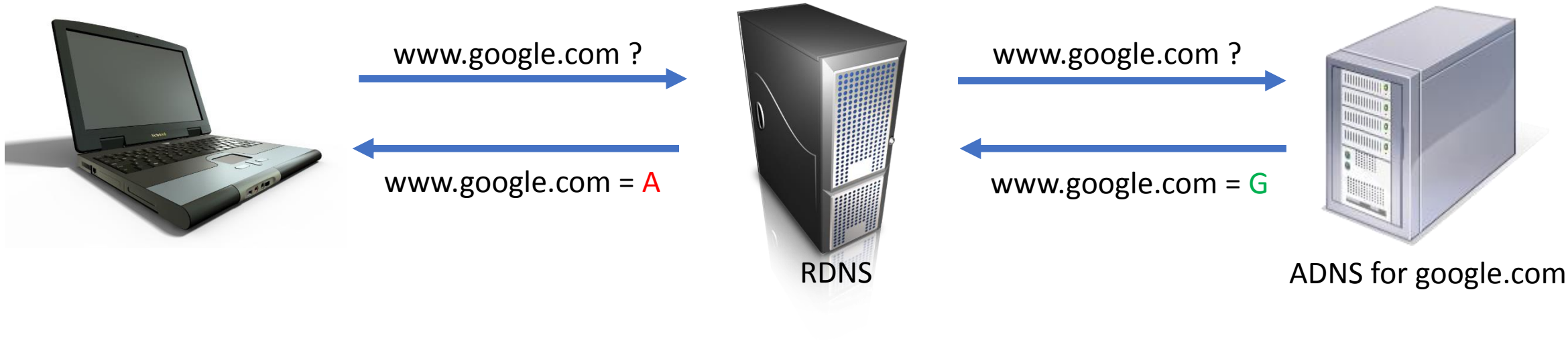
Search Engine Hijacking (Paxfire)



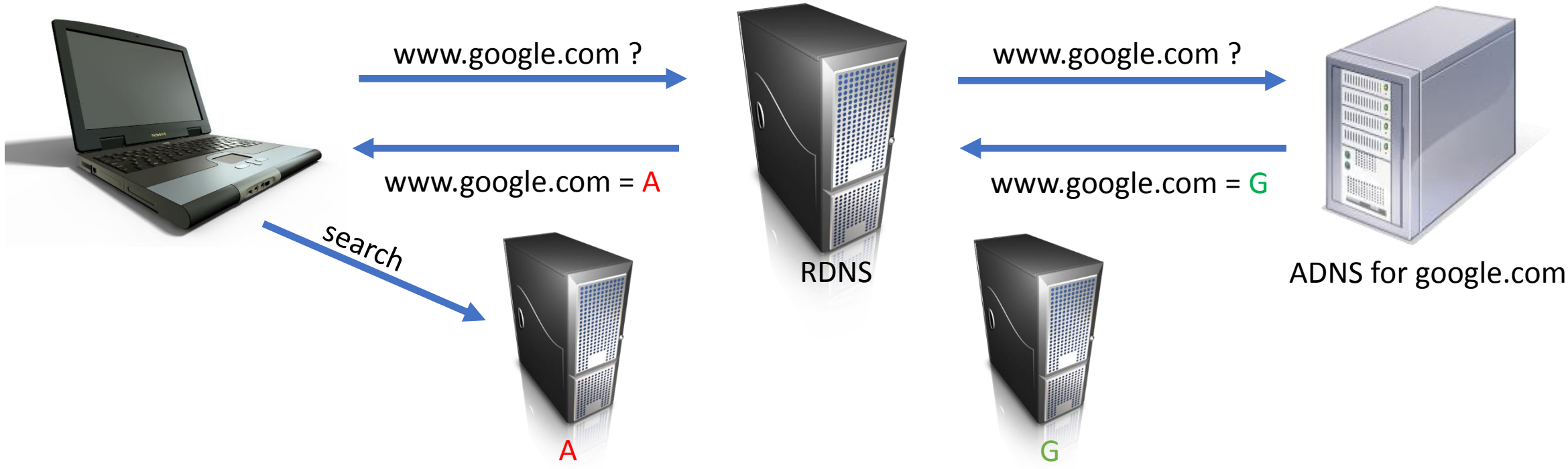
Search Engine Hijacking (Paxfire)



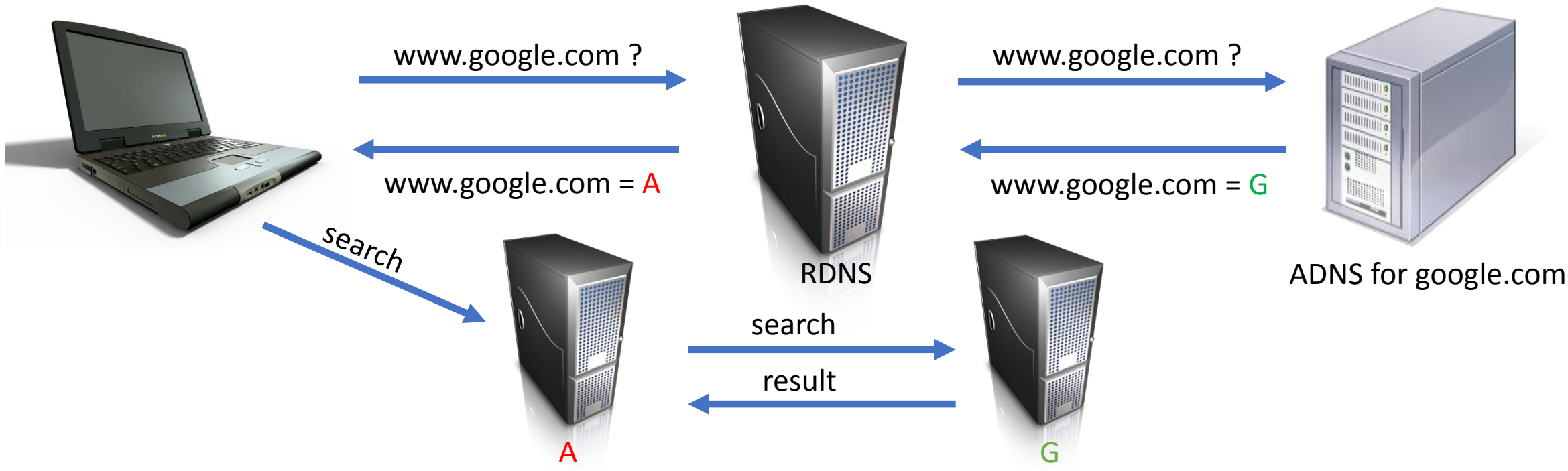
Search Engine Hijacking (Paxfire)



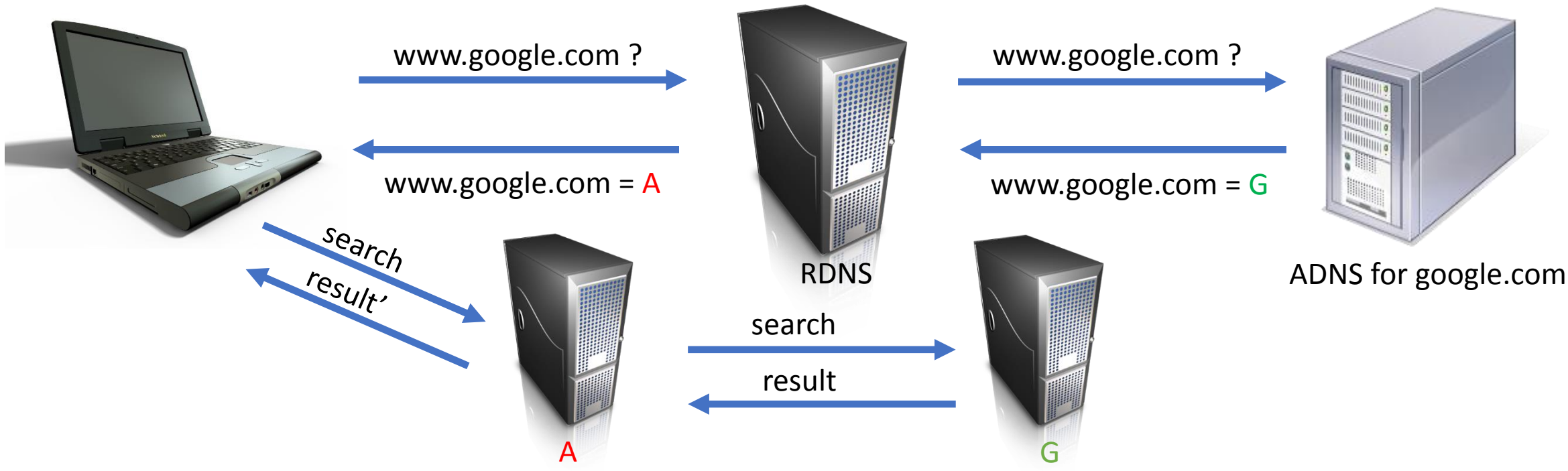
Search Engine Hijacking (Paxfire)



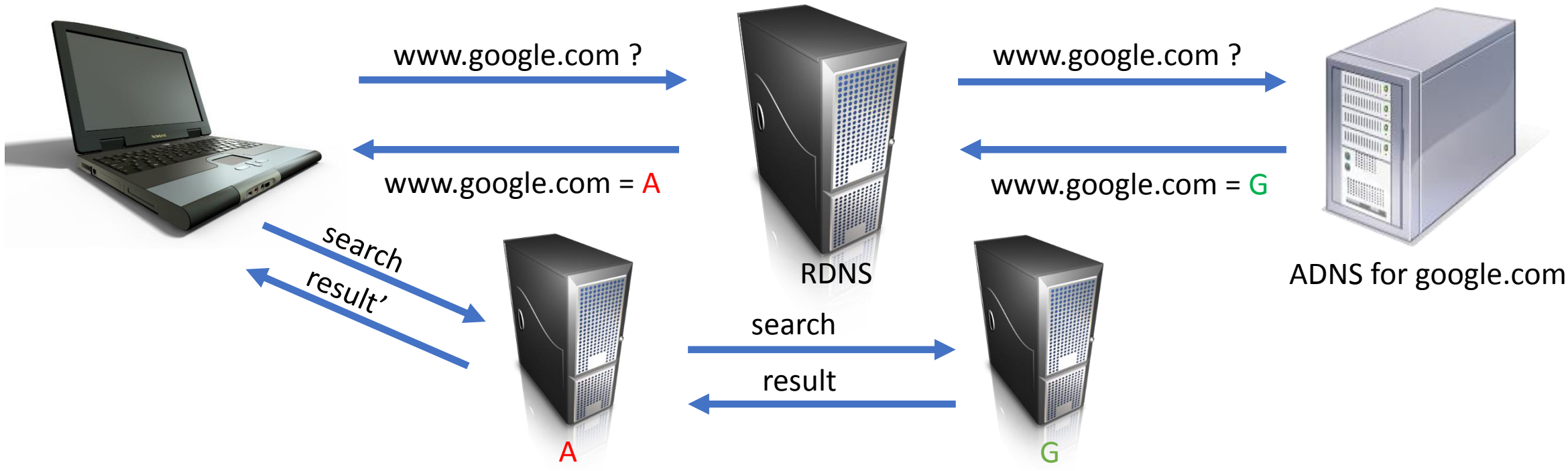
Search Engine Hijacking (Paxfire)



Search Engine Hijacking (Paxfire)



Search Engine Hijacking (Paxfire)



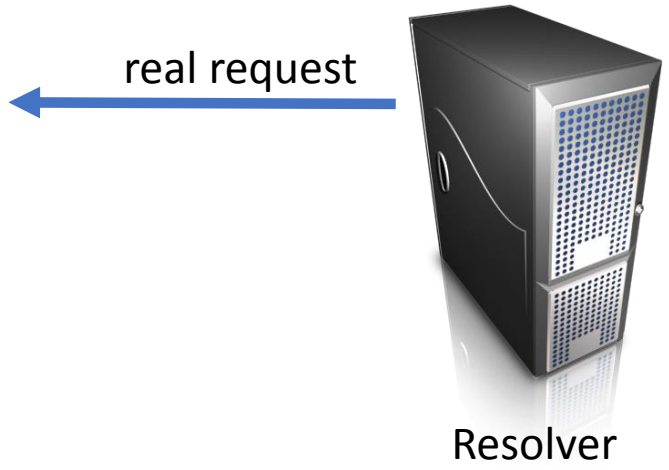
- Again, the primary reason is to monetize user's search traffic
- While once common, this is no longer a widespread practice

Off-path Attacks

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

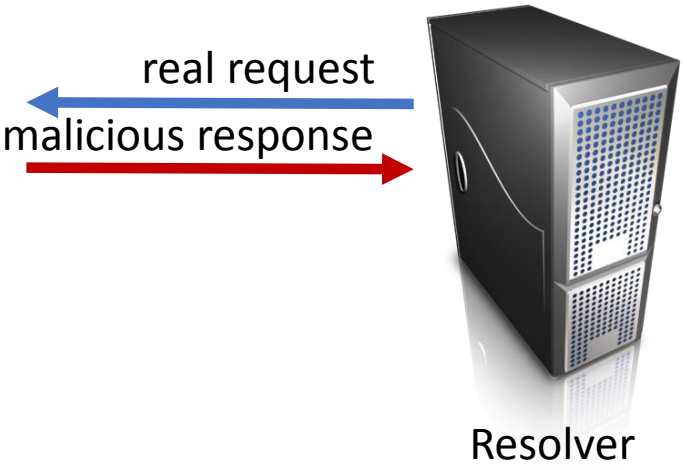
Off-path Attacks

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



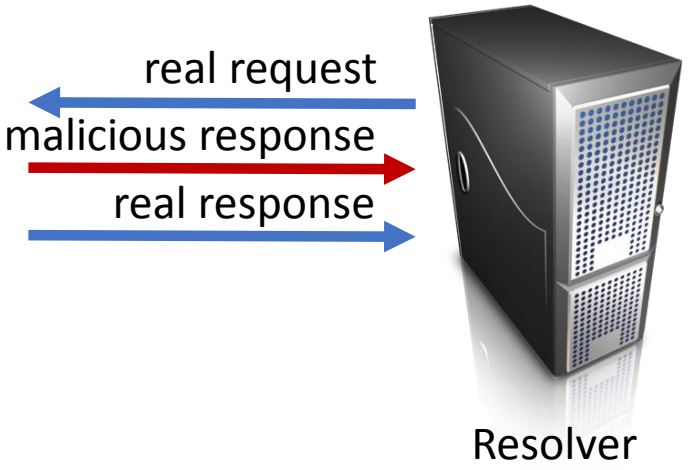
Off-path Attacks

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



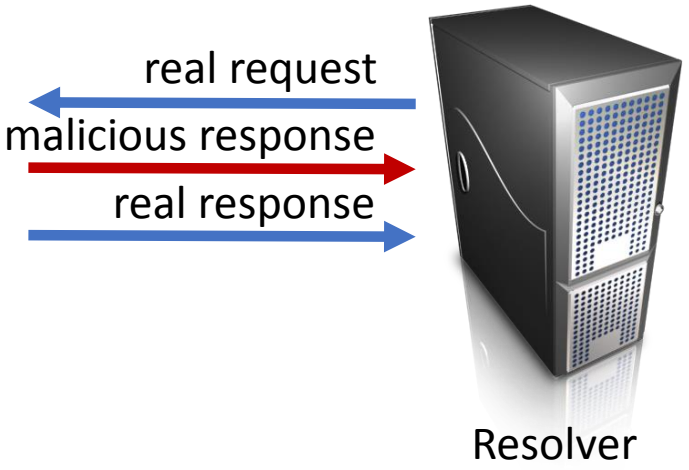
Off-path Attacks

- 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!

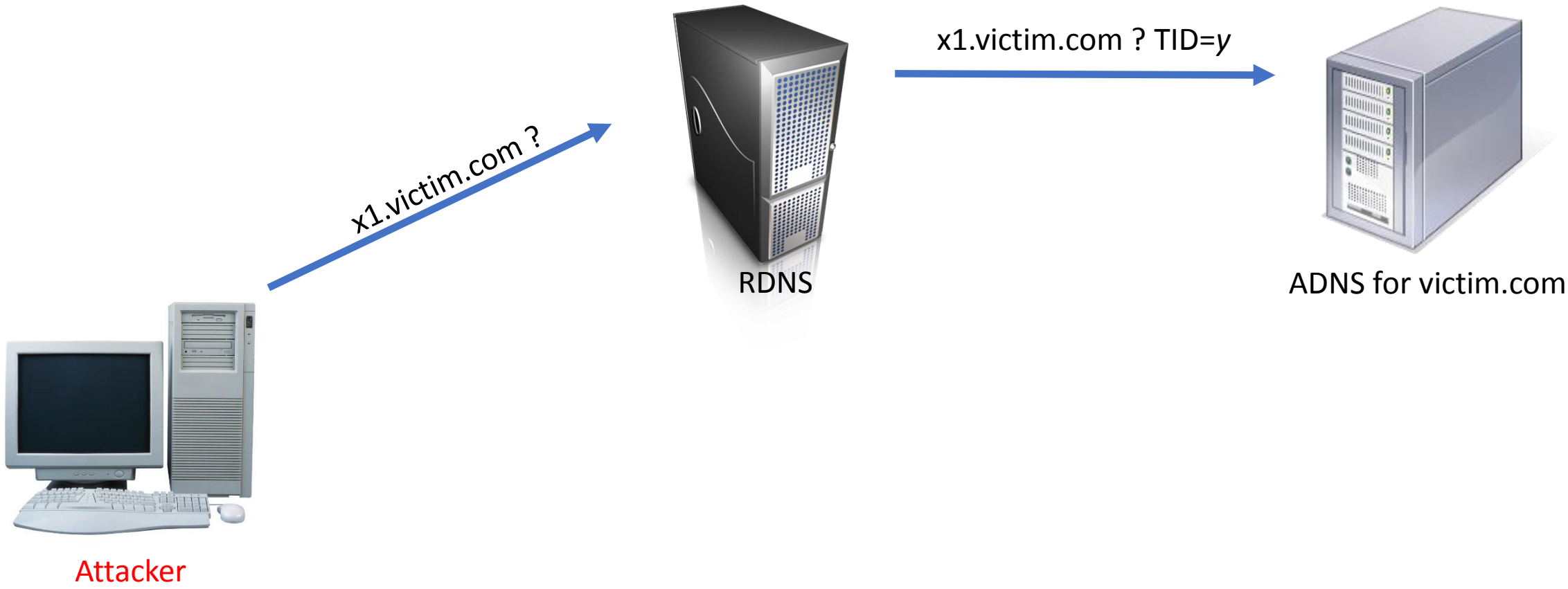
Kaminsky Vulnerability (cont.)

RDNS

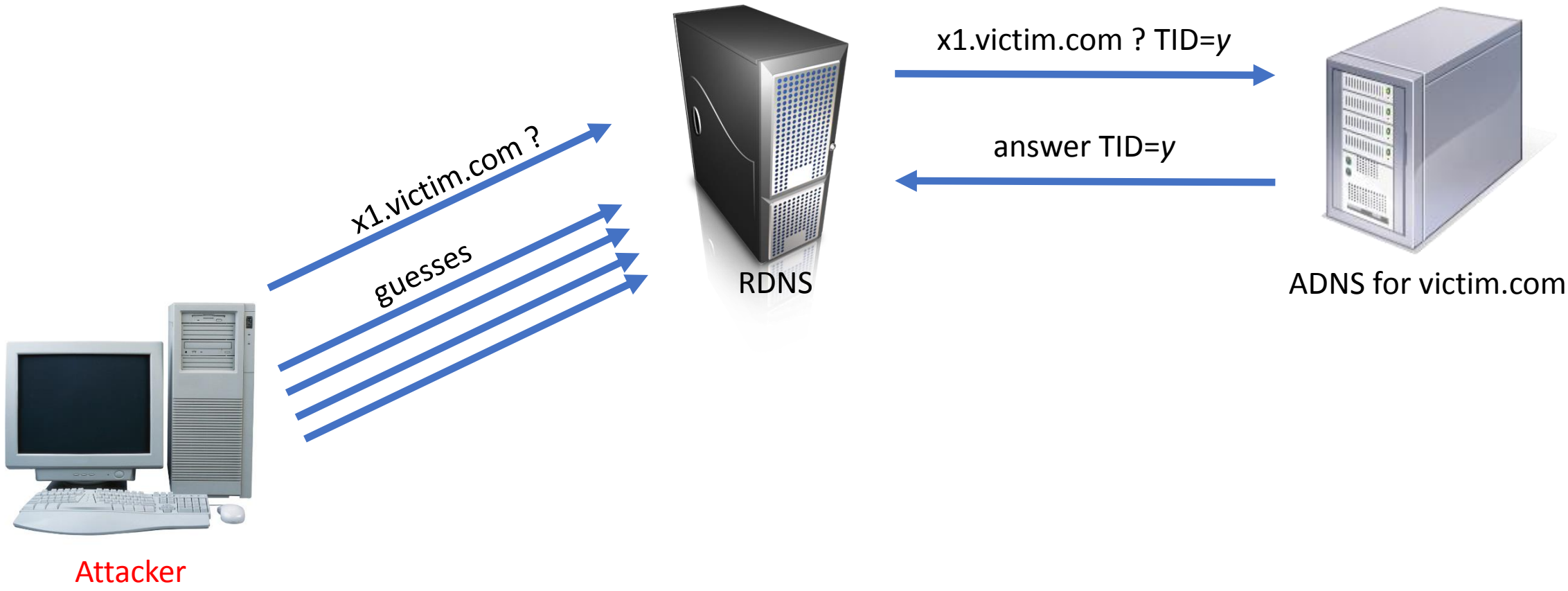
ADNS for victim.com

Attacker

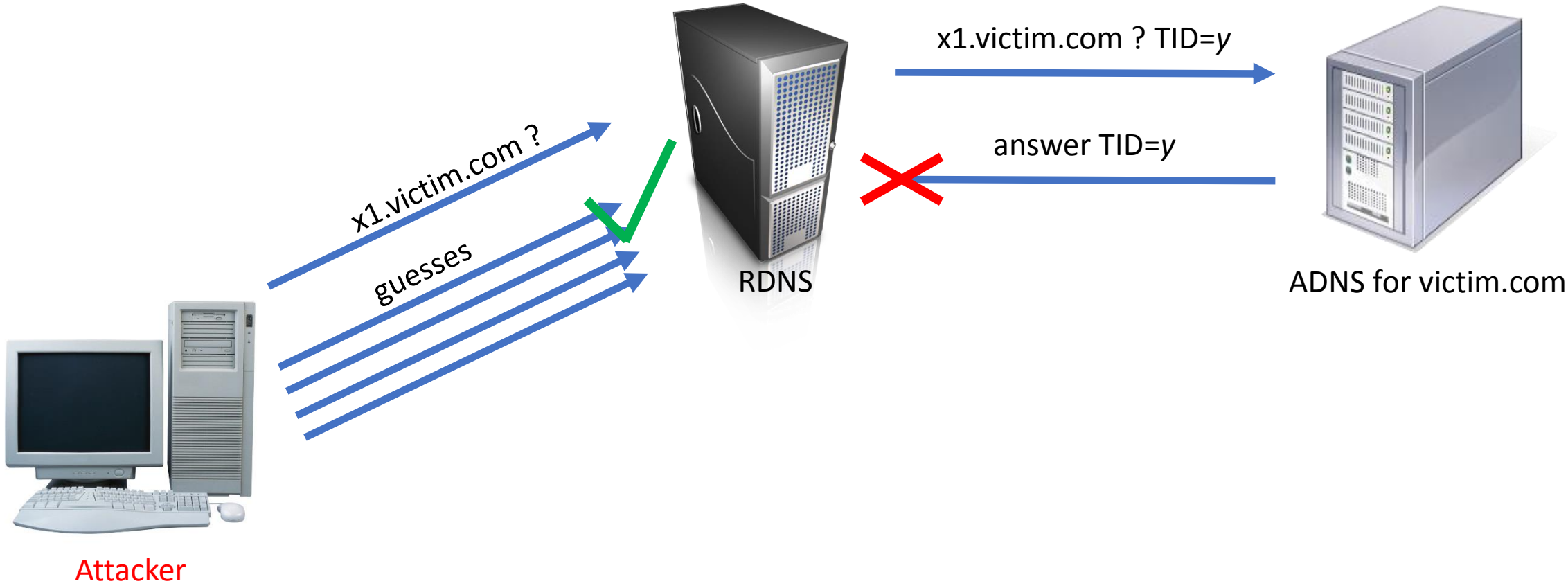
Kaminsky Vulnerability (cont.)



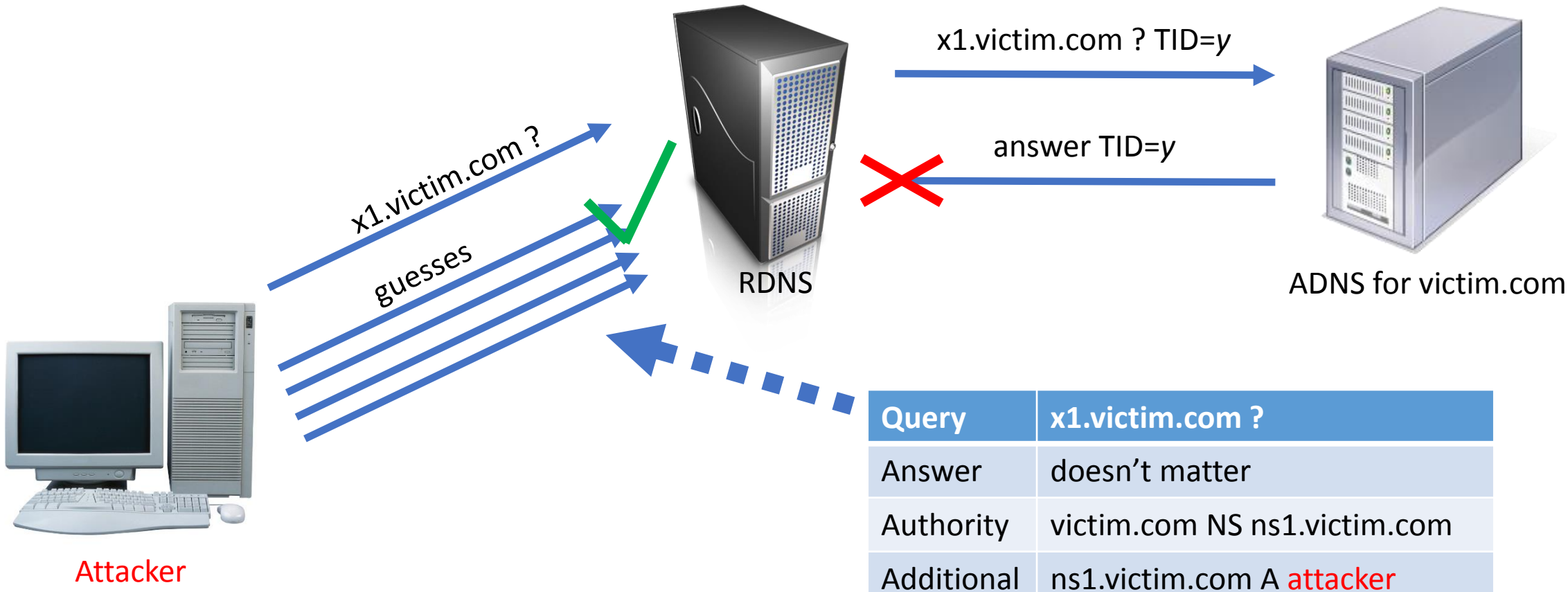
Kaminsky Vulnerability (cont.)



Kaminsky Vulnerability (cont.)



Kaminsky Vulnerability (cont.)



Query	x1.victim.com ?
Answer	doesn't matter
Authority	victim.com NS ns1.victim.com
Additional	ns1.victim.com A attacker

Kaminsky Vulnerability (cont.)

www.victim.com ?

RDNS

ADNS for victim.com

Attacker

Kaminsky Vulnerability (cont.)

www.victim.com ?

RDNS

ADNS for victim.com

www.victim.com ?

Attacker

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

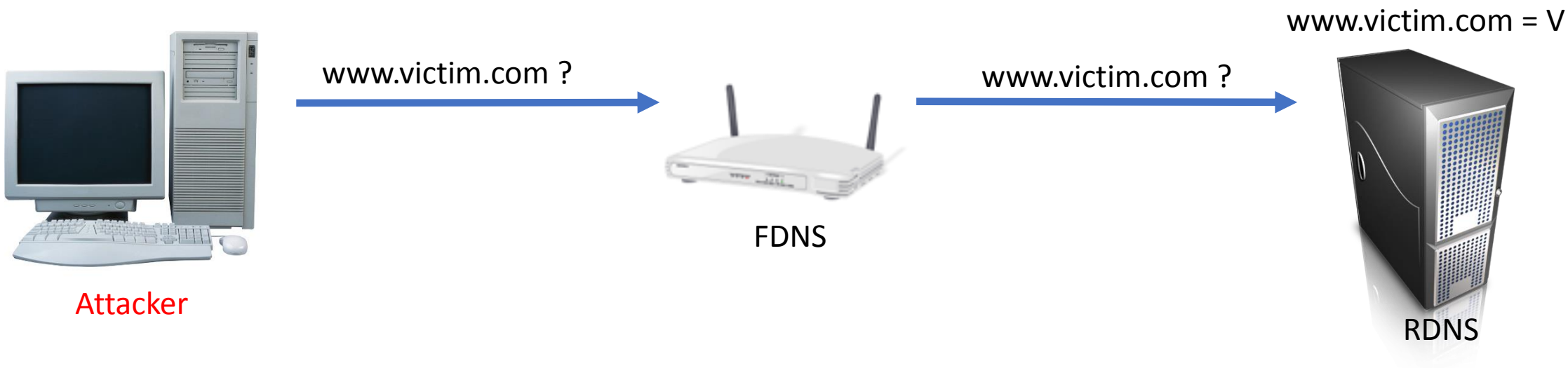
- Send multiple DNS requests through each RDNS
  - Classify RDNS where 10 or more DNS requests arrive at our ADNS
- Nearly all classified resolvers appear to use random transaction IDs
- 16% of classified resolvers use *static* ephemeral ports!
- 0x20 encoding rare
  - (lower bound)

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

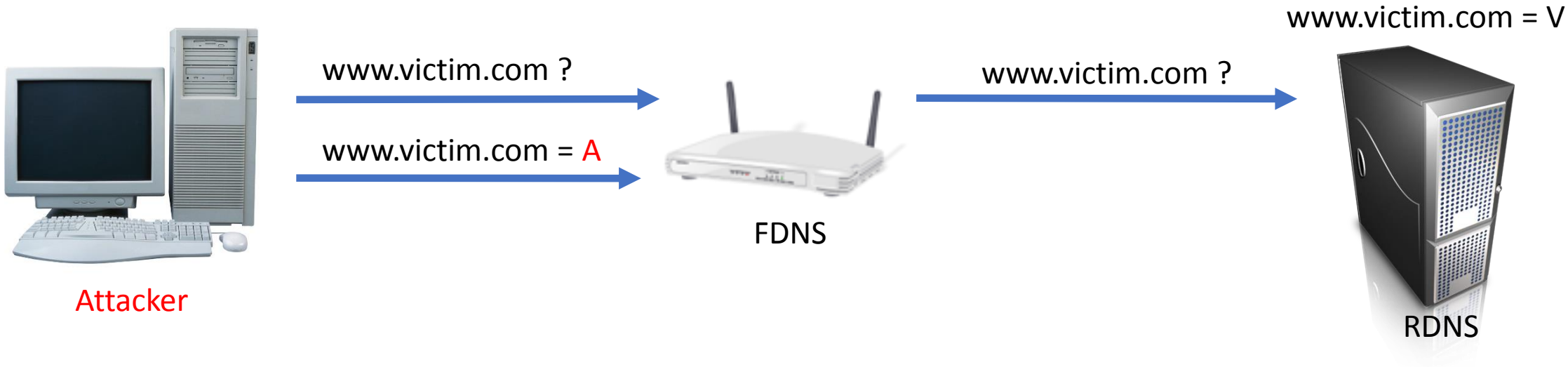
Preplay Vulnerability

- 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 vulnerablility that is much easier to exploit than the Kaminsky vulnerability

Preplay Vulnerability (cont.)

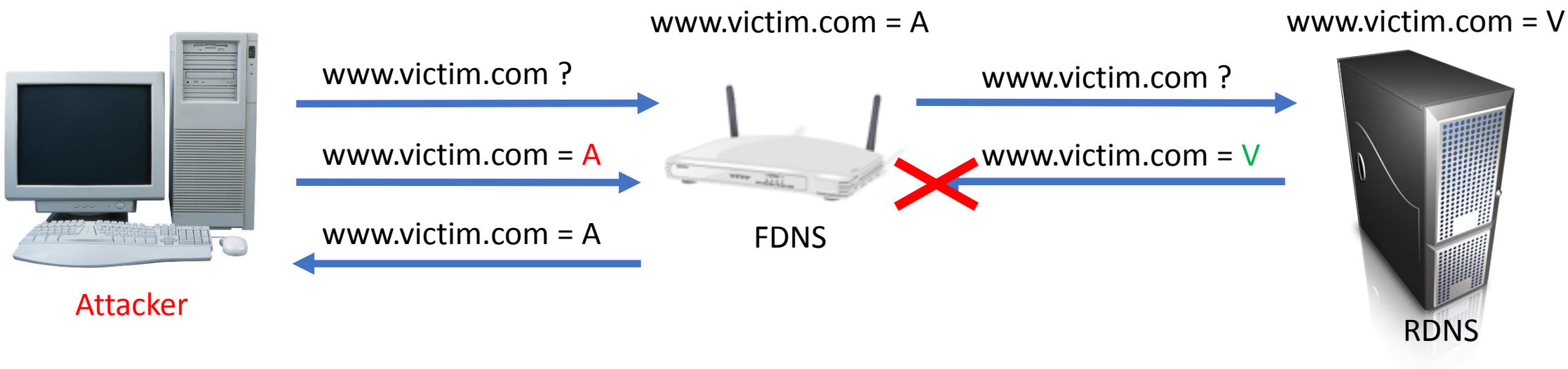


Preplay Vulnerability (cont.)

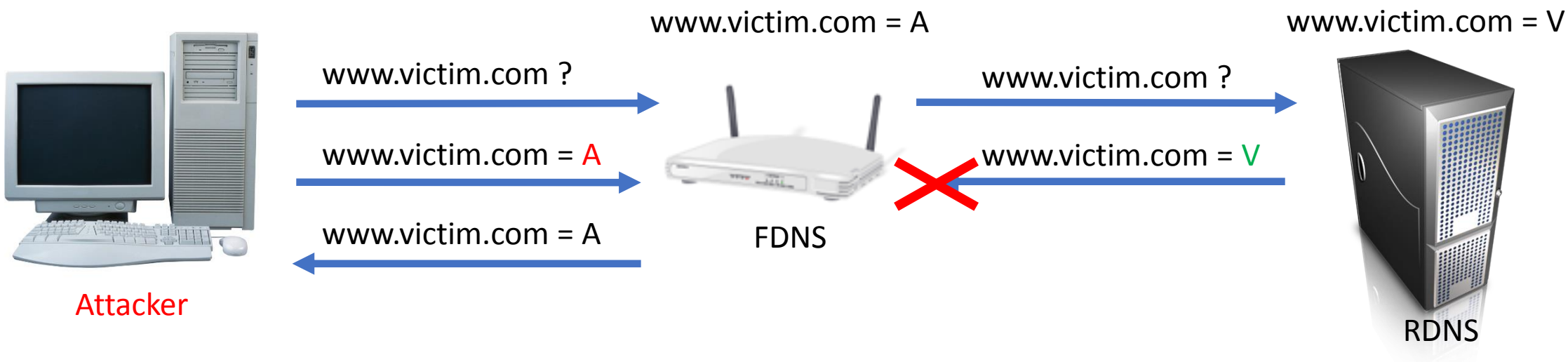


Preplay Vulnerability (cont.)

Preplay Vulnerability (cont.)



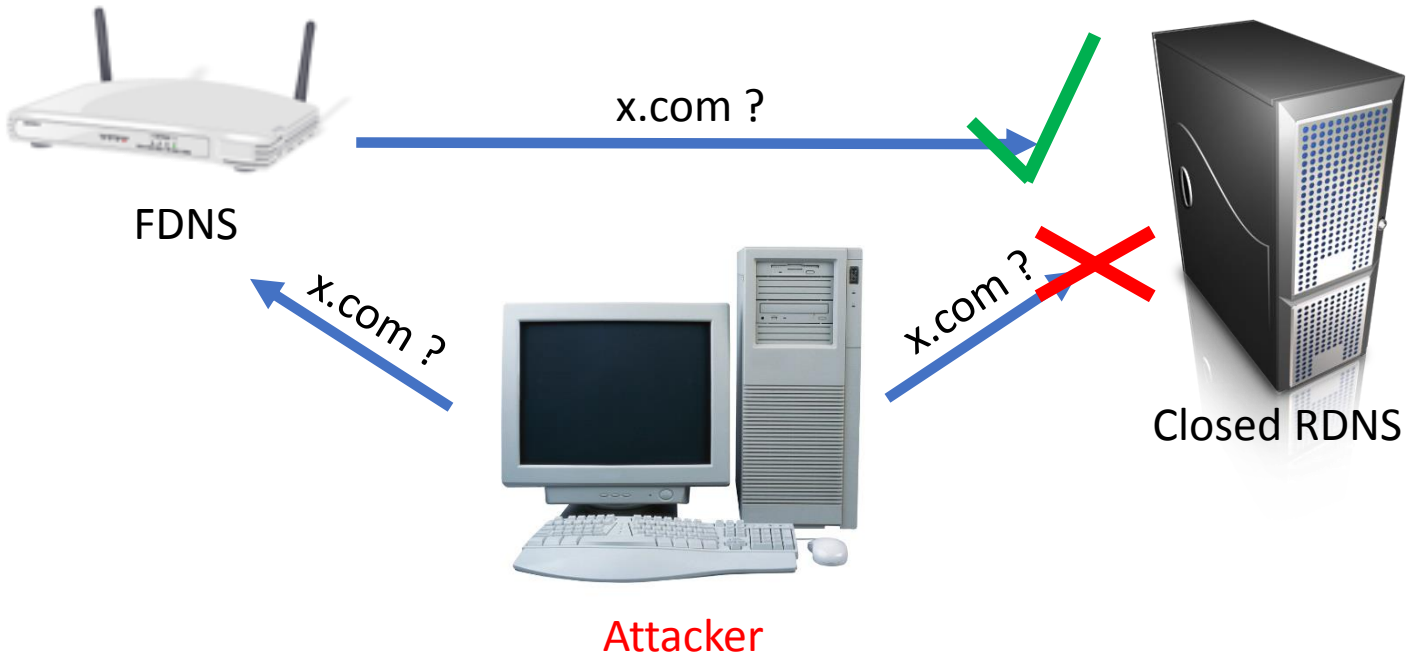
Preplay Vulnerability (cont.)



- 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

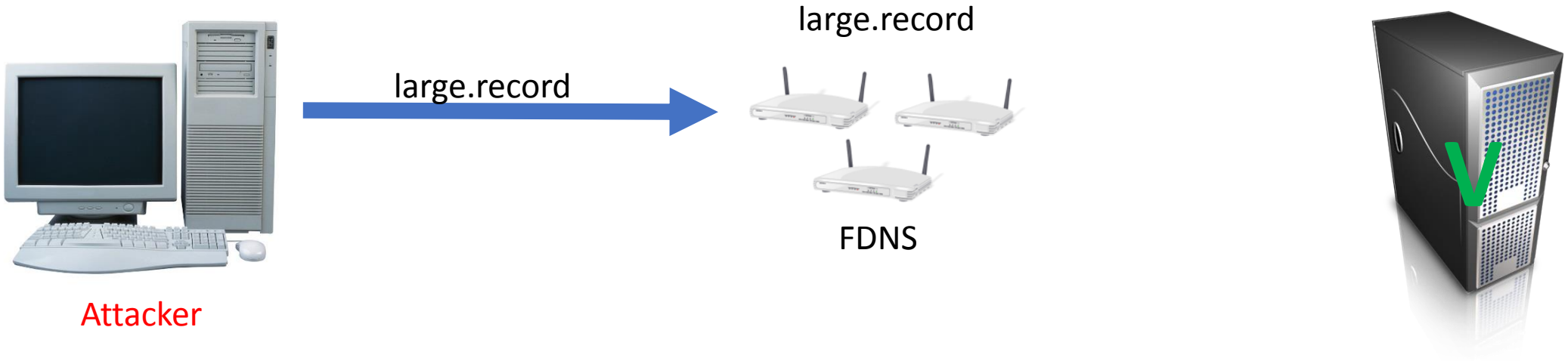


Implication: Phantom DDoS Attacks

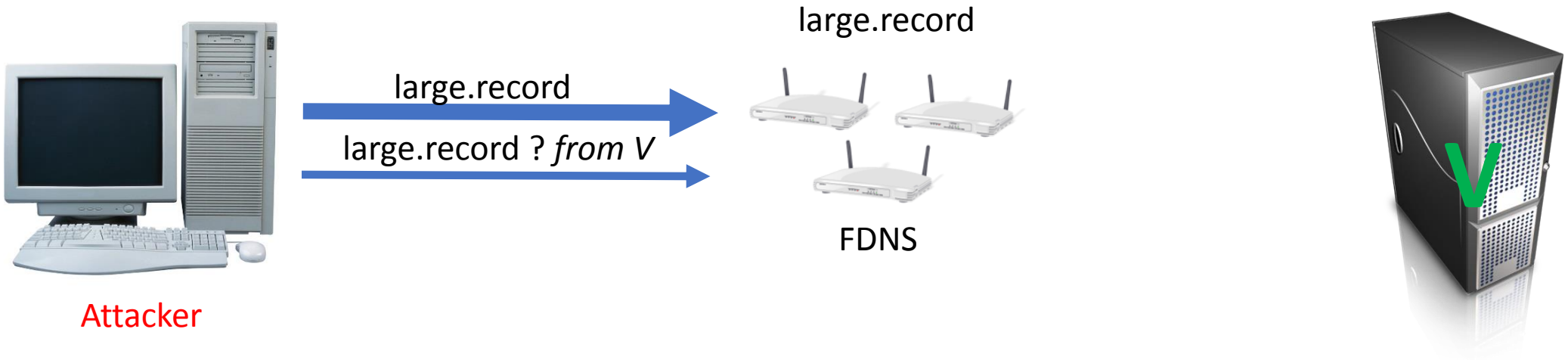
Attacker

FDNS

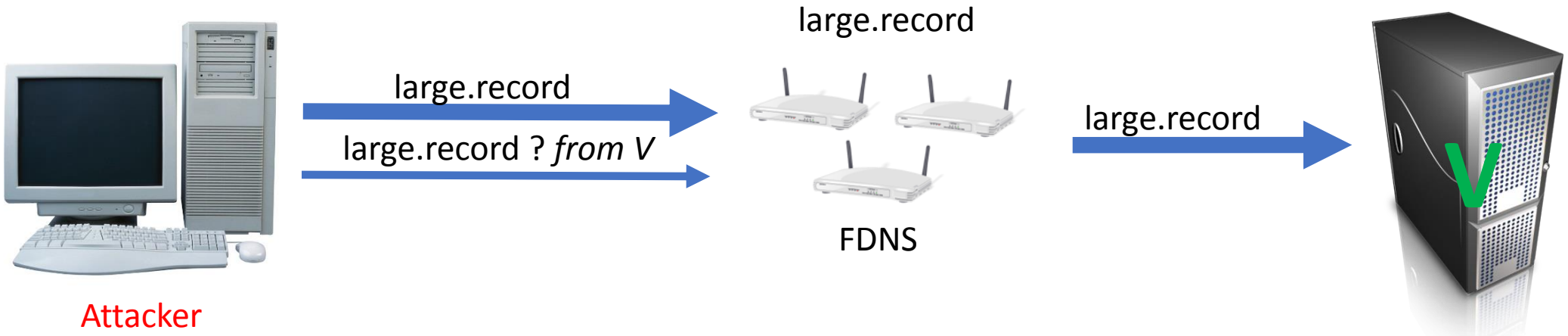
Implication: Phantom DDoS Attacks



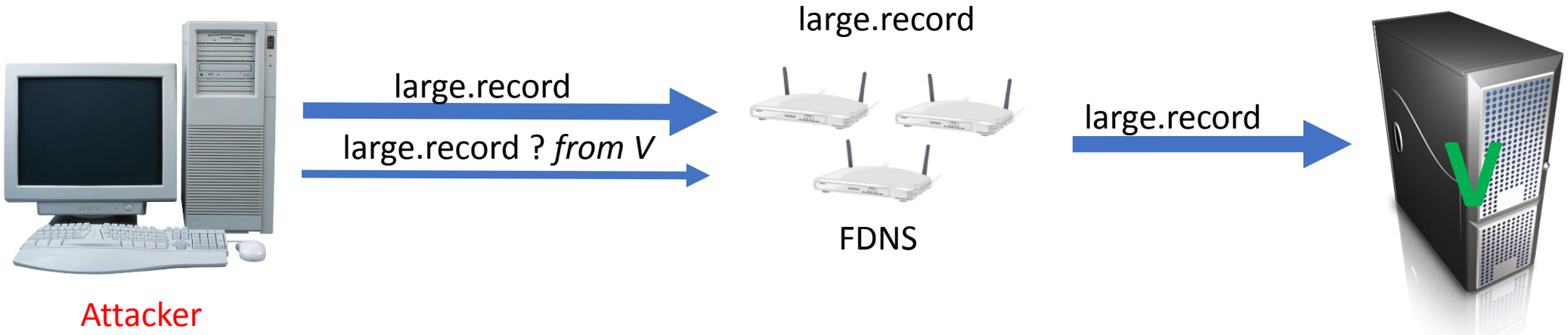
Implication: Phantom DDoS Attacks



Implication: Phantom DDoS Attacks



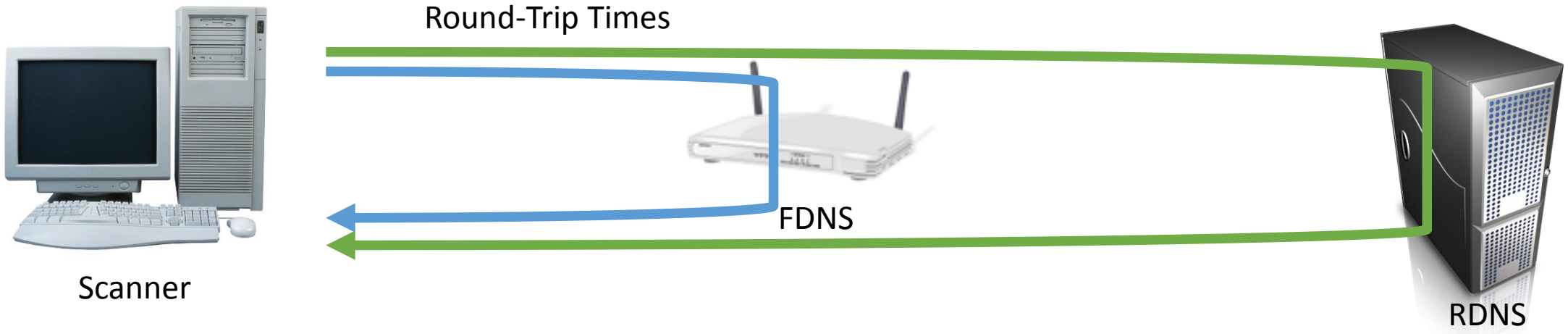
Implication: Phantom DDoS Attacks



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

Context: Are Preplay Vulnerable FDNS Used?

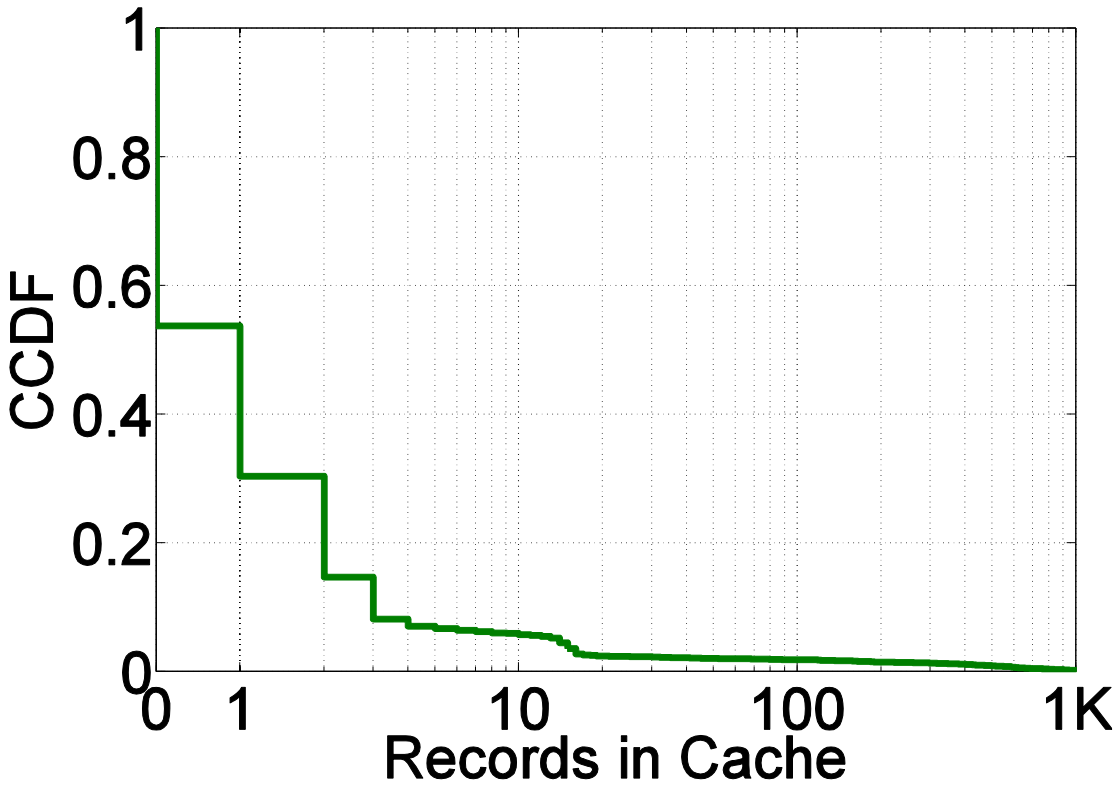
- Attack only effective if there are users behind the FDNS
- We test FDNS for use by looking for popular records in the FDNS's cache



- If a popular record returned in ≪ RDNS RTT and ≈ FDNS RTT, then FDNS is used

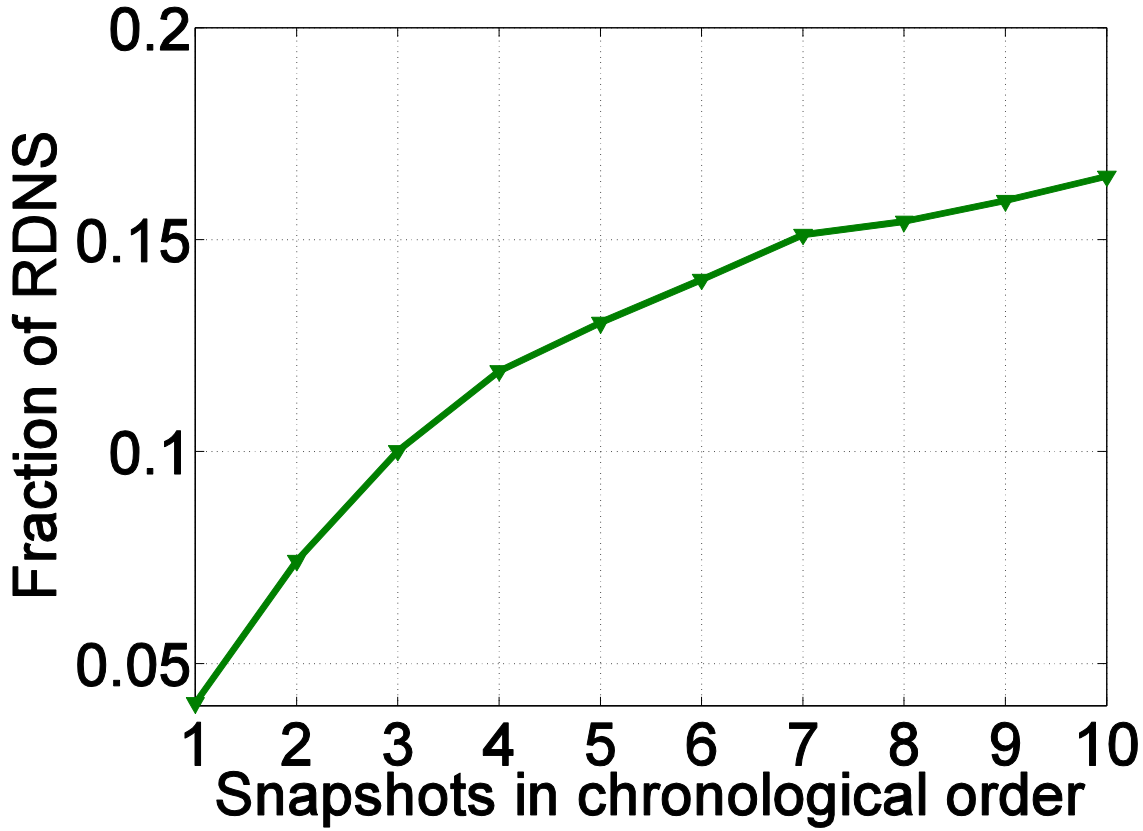
Context: Preplay Vulnerable FDNS Are Used!

- 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

CASE WESTERN RESERVE UNIVERSITY EST. 1826

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Thank you! Questions?

Kyle Schomp – kgs7@case.edu

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

Additional Slides

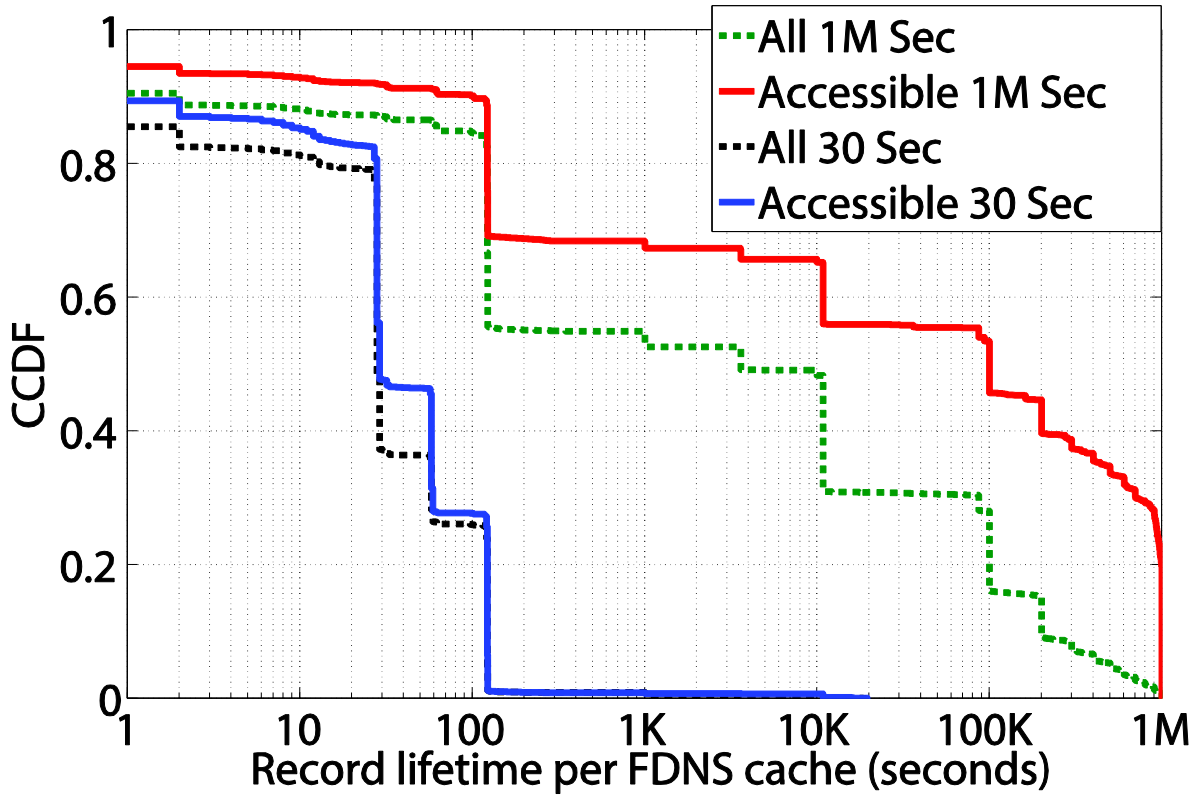
Datasets

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

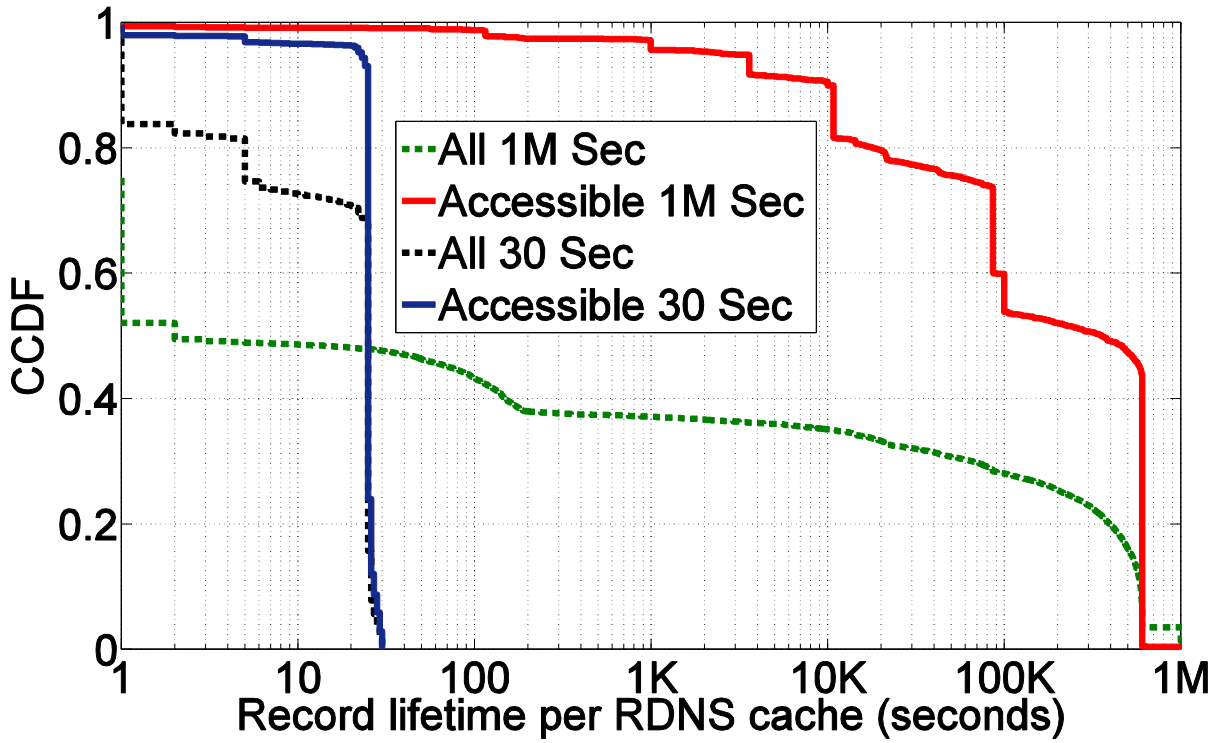
Residential Network Device Criteria

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%
Total	849K	78%

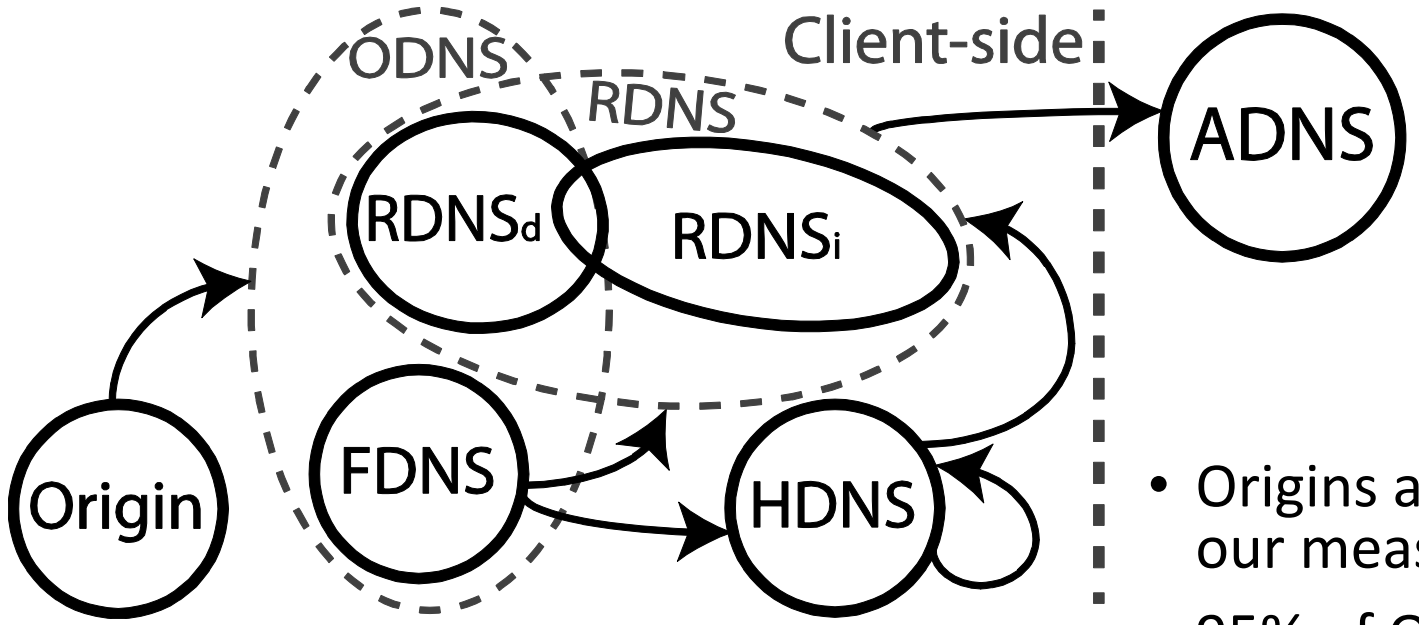
FDNS Cache Behavior



RDNS Cache Behavior



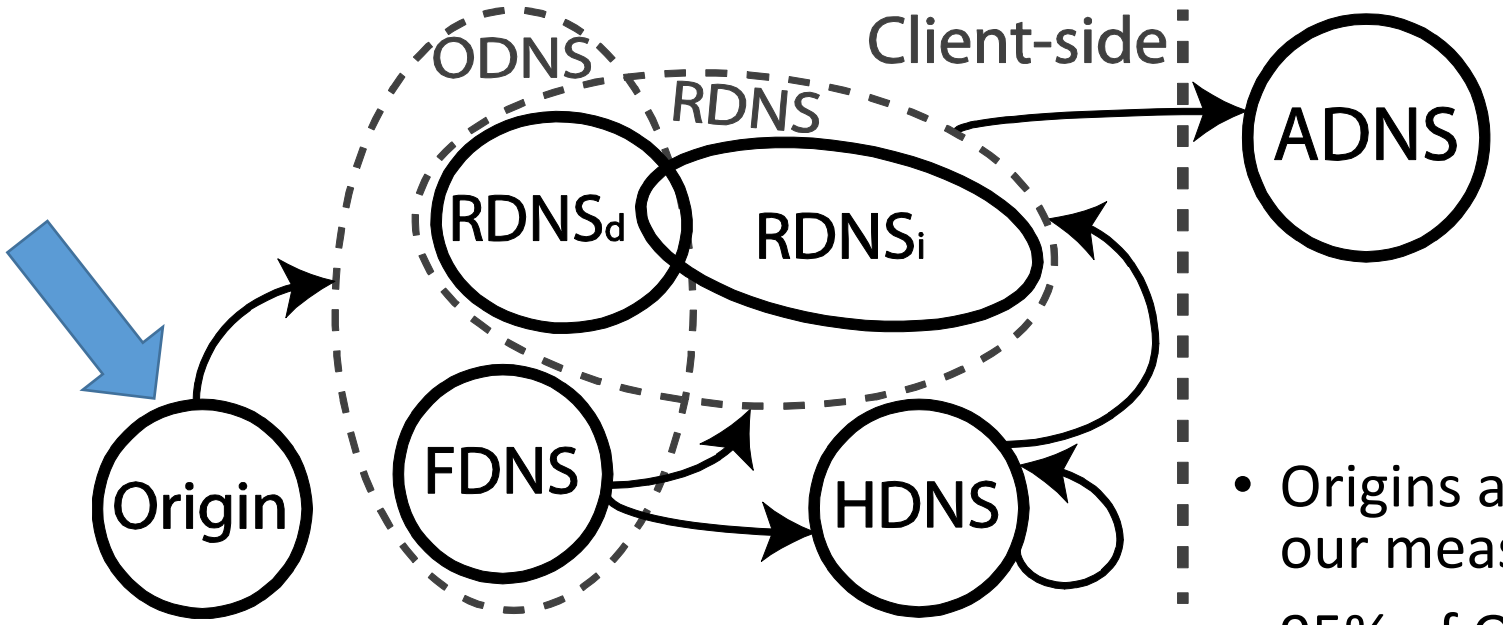
The Client-Side DNS Infrastructure



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

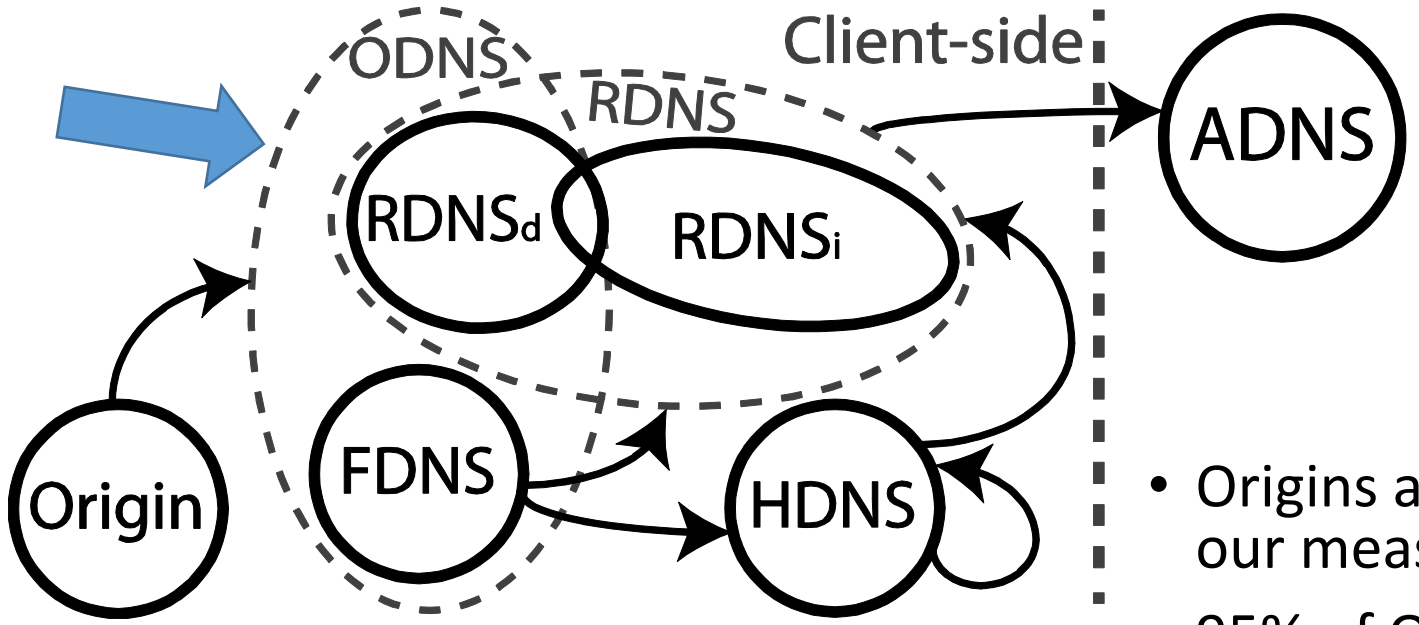
The Client-Side DNS Infrastructure



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

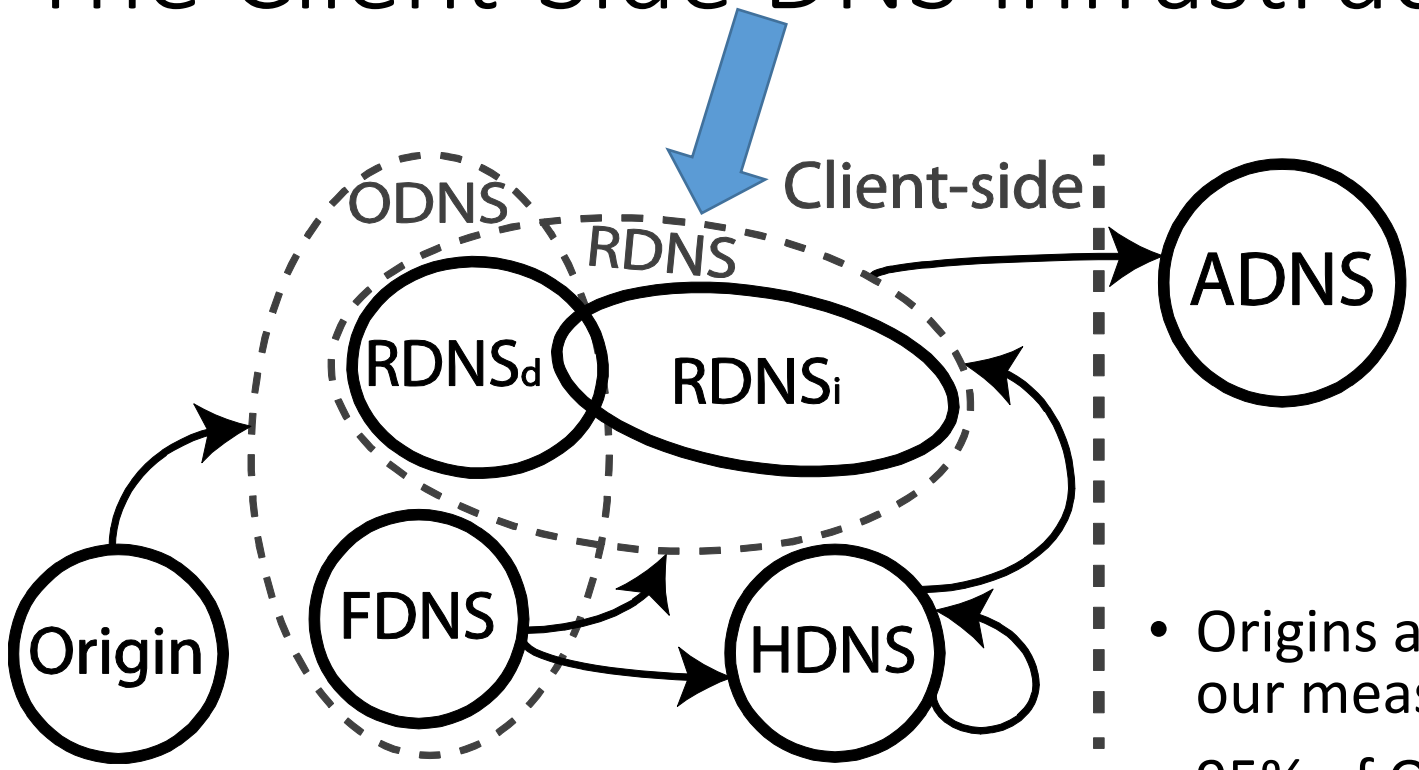
The Client-Side DNS Infrastructure



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

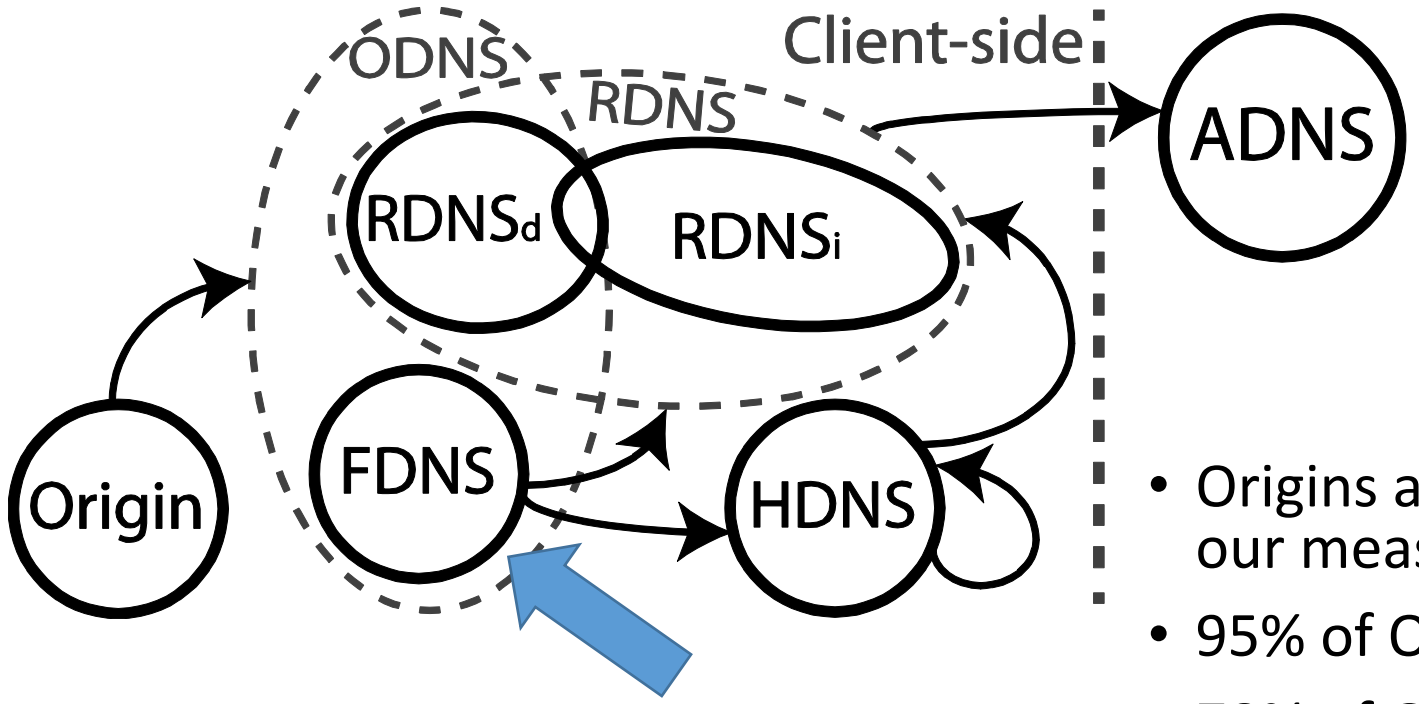
The Client-Side DNS Infrastructure



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