

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

Security training group EC-Council's website defaced

February 28, 2014 | By Paul Mah

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

As reported by Ars Technica the hacker also passed 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 security attacks. There was no mention access, though it was done using a DNS

For more - check out this

Related Articles

- How a founder of Snowden bested Kaspersky: Anti-

Sign up for our

DNS attack writer a victim of his own creation

By Robert McMillan, EO Above Service
July 28, 2008 02:00:00 EDT

NEWS | Blogs | Newsletters | Videos | Events | Resources | MISRE | More | 81 | Facebook | Twitter | LinkedIn | RSS | Print | Email

Security | LANs & WAN | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center | SMB | Careers | Gearhead | Tech Deb

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

Latest News

- Is SDN your next security ni
- Brocade's fabric strategy as
- IBM workforce cuts raise que

ish looks like the winner of plans are unclear

new more Latest News

Widespread Hijacking of Search Traffic in the United States

AUGUST 4, 2011 | BY PETER ECKERSLEY

HOME ABOUT OUR WORK DEEPLINKS BLOG PRESS ROOM TAKE ACTION SHOP

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

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/7zi>

EFF membership packs include cam stickers to

Securelist

Internet threat level: 1

Watch us on YouTube

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

Blog

- DNSSec day in Colombia
- Google.ro and other RO domains victims of a possible DNS poisoning attack
- The sale of one thousand and one DSL routers
- Is it the end of the DNSChanger Trojan?
- The end of DNS-Changer

Massive DNS poisoning attacks in Brazil

Foto: Assolati
Fazcazery Lab Expert
Posted November 07, 11:39 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 included 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 5 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 several, as well as local market leaders including Lixi, 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 malware displaying this warning when opening Google:

Install Google Defence Para user a novo Google.com

The Washington Post

Security Fix

Brian Krebs on Computer Security

When Monetizing ISP Traffic Goes Horribly Wrong

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

NetworkWorld

Security | LANs & WAN | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center | SMB | Careers | Gearhead | Tech Deb | Communities

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

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

Martirosyan: Hacker attacks may continue for several days

NEWSLINE

- 11:02 a.m. - Georgian president calls his friend's family in Edinburgh
- 11:01 a.m. - S. Oshanian discusses losses of NATO new programs in Brussels
- 10:48 a.m. - Report: UK agency spied on chats
- 10:48 a.m. - G. Sahakian: Opposition does not need commission on March 1 events
- 10:43 a.m. - Ukraine parliament is illegitimate - Yanukovich
- 10:42 a.m. - Armenian police chief receives COCOTC's forensic office head
- 10:41 a.m. - Armenia men's soccer Sinterpool Airport in China
- 10:40 a.m. - Ukraine asks Russia to extradite Yanukovich
- 10:39 a.m. - Albanian migrants storm into Spanish borders of Serbia
- 10:38 a.m. - Presidents of Armenia and Georgia summarize results of talks
- 10:34 a.m. - Peace talks still an option, Syrian opposition says
- 10:33 a.m. - Tessa Proghranan: It's no need to dream of Maidan in Armenia
- 10:32 a.m. - Ireland: Ukraine today is divided into believe, not two
- 10:31 a.m. - Poland: There cannot be a military position in Karabakh conflict

27.02.2014, 19:27
Ajgor am

3/11/2014

PAM 2014

2

DNS Recording Injection

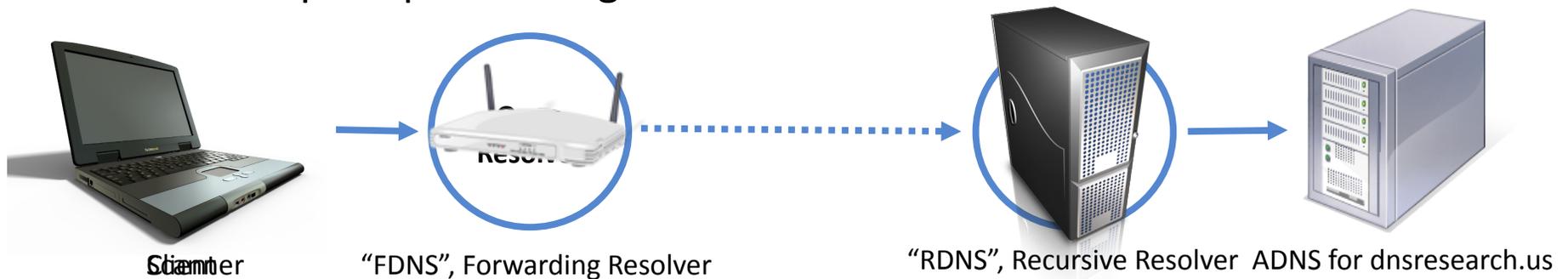
- Subverting the DNS name to address bindings
- Redirection to a malicious webserver
- Privacy issues
- Denial of service
- Phishing attacks
- Malware installation

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

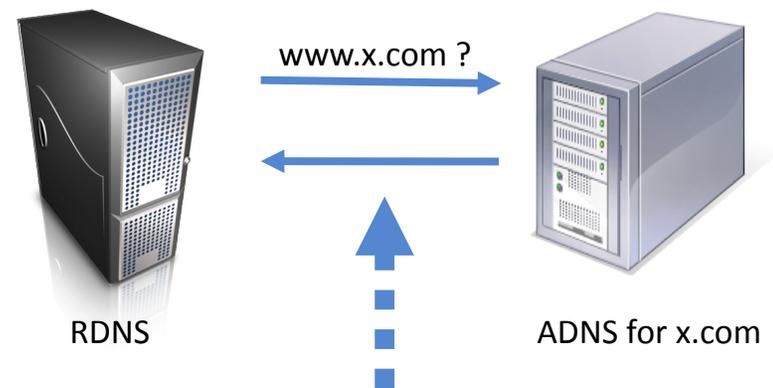
- Discover open resolvers by sampling randomly from the Internet
- Deploy our own authoritative DNS server (*ADNS*)
- DNS request probes target our own domain



- Test open and egress resolvers for vulnerability to record injection

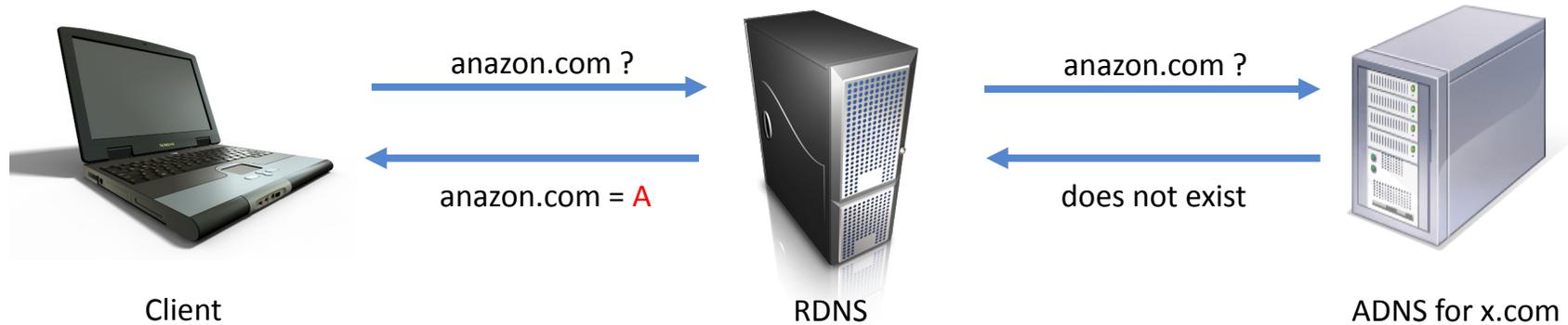
Bailiwick Violations

- 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!



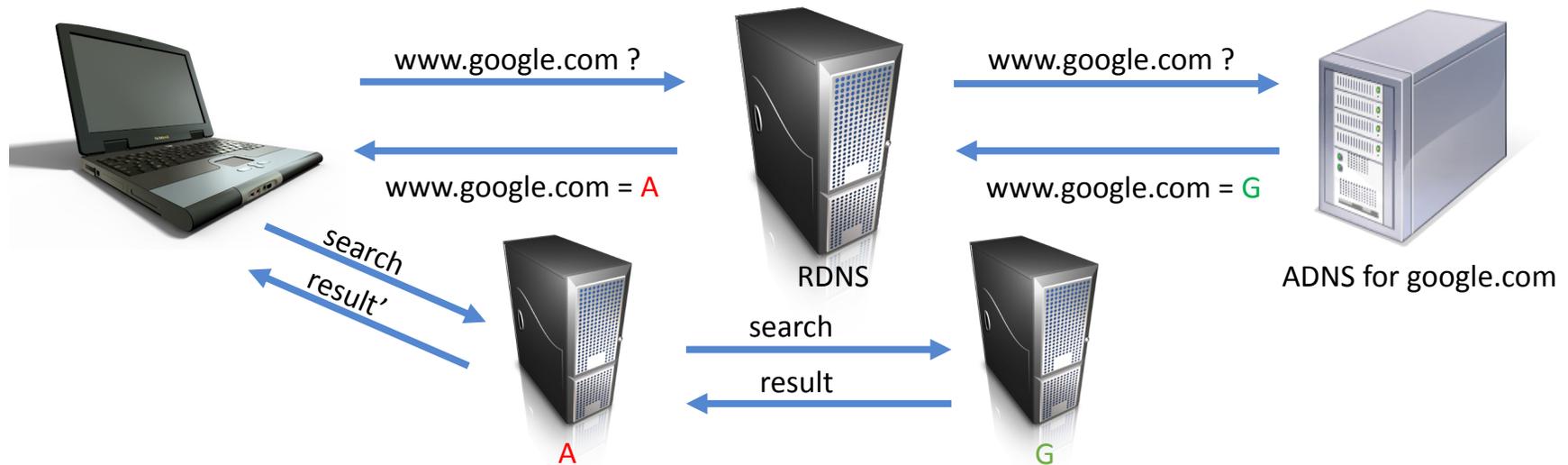
Query	www.x.com ?
Answer	1.2.3.4
Additional	www.hsbc.com A 2.3.4.5

Negative Response Rewriting



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

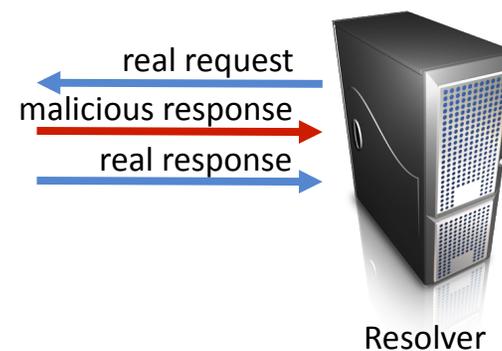
Search Engine Hijacking (Paxfire)



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

Off-path Attacks

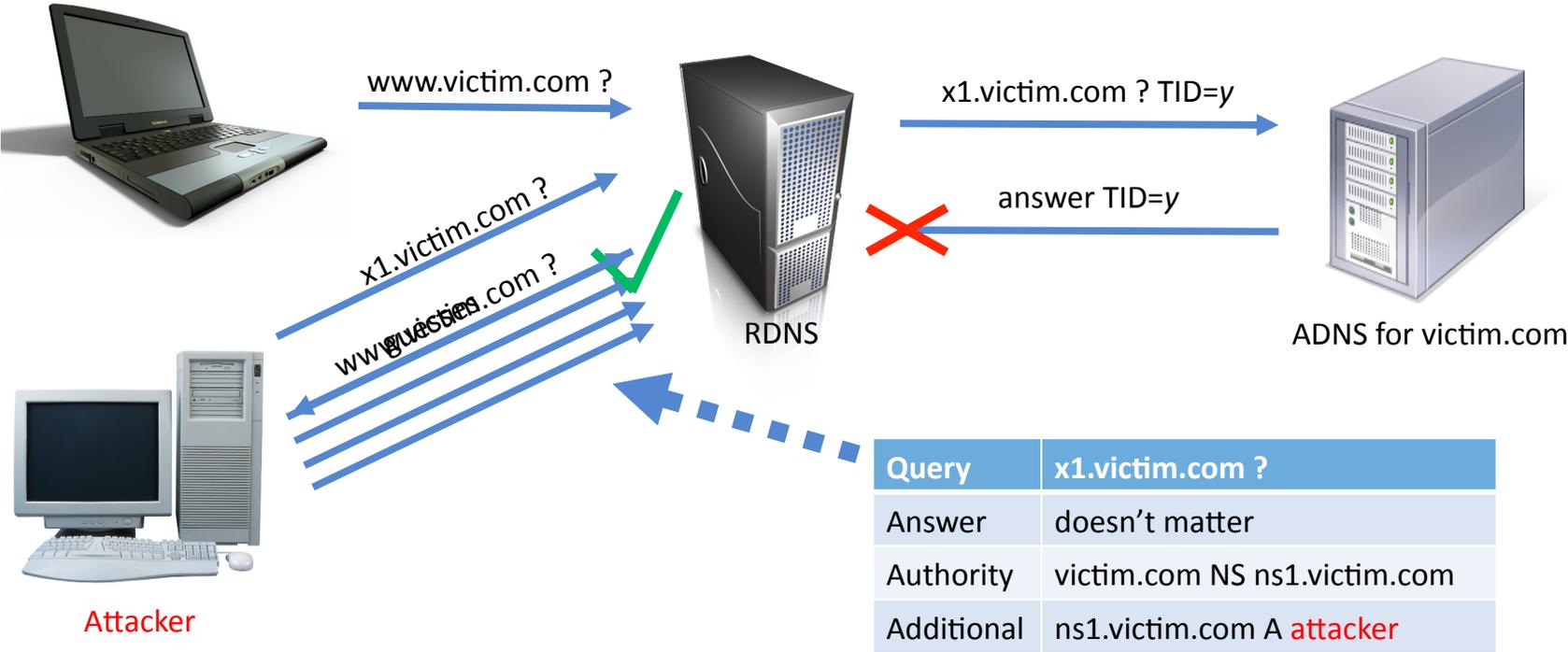
- Craft an acceptable DNS response to squeeze between the real DNS request and response
- Fields to match:
 - IP addresses: source and destination
 - Port numbers: source and destination
 - Query string and transaction ID



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.)



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

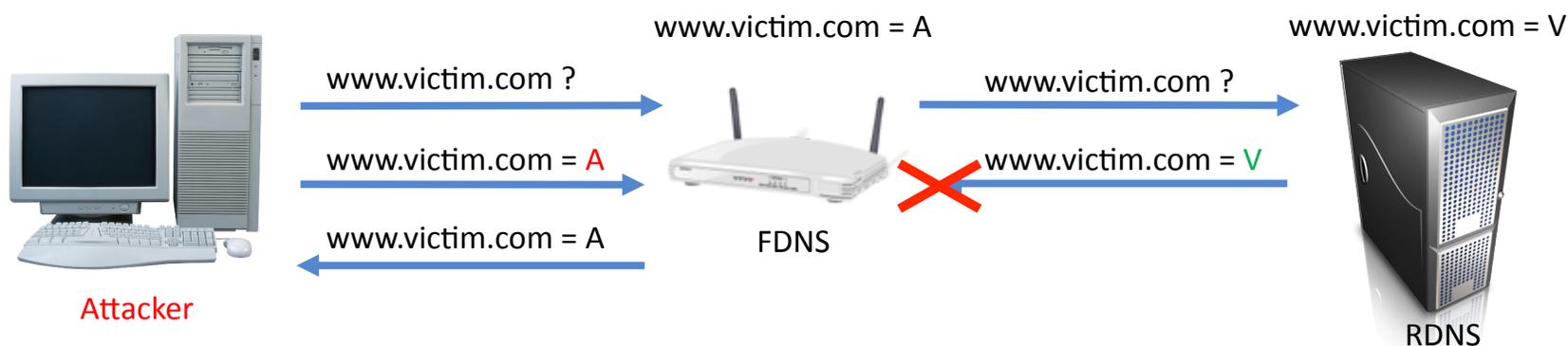
- Send multiple DNS requests through each RDNS
 - Classify RDNS where 10 or more DNS requests arrive at our ADNS
- Nearly all classified resolvers appear to use random transaction IDs
- 16% of classified resolvers use *static* ephemeral ports!
- 0x20 encoding rare
 - (lower bound)

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

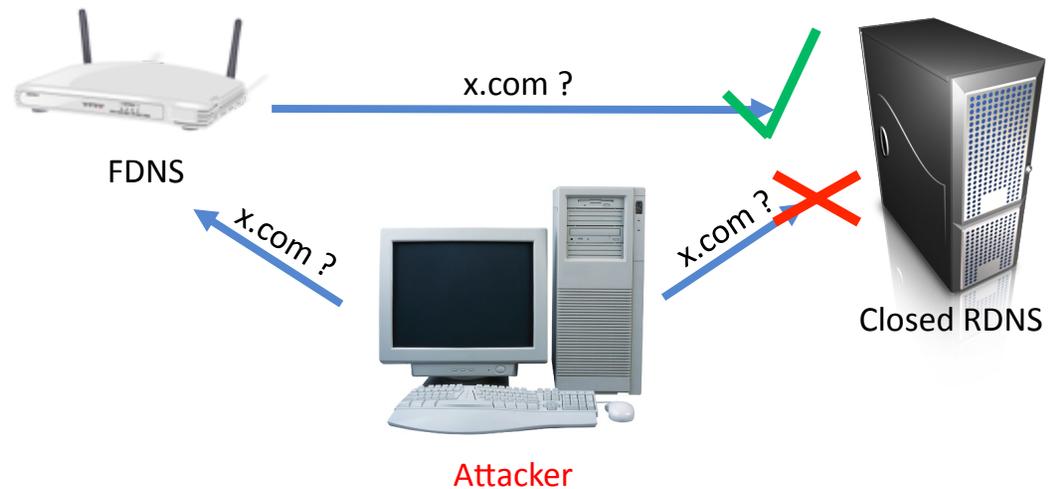
Preplay Vulnerability (cont.)



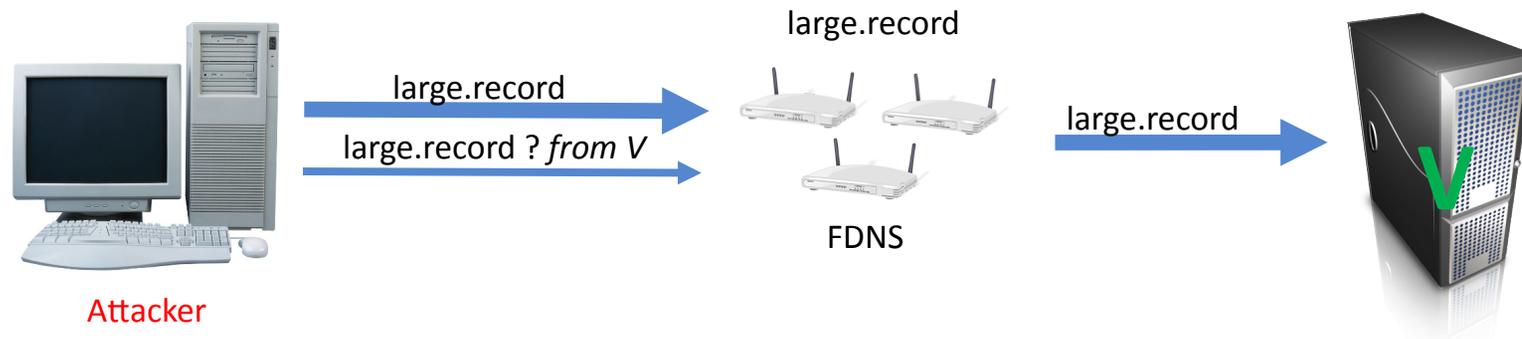
- RDNS IP address, transaction ID, and port numbers are not validated!
- 7-9% FDNS are vulnerable
- 2-3 million out of the ~32 million open resolvers on the Internet

Implication: Indirect Attacks

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



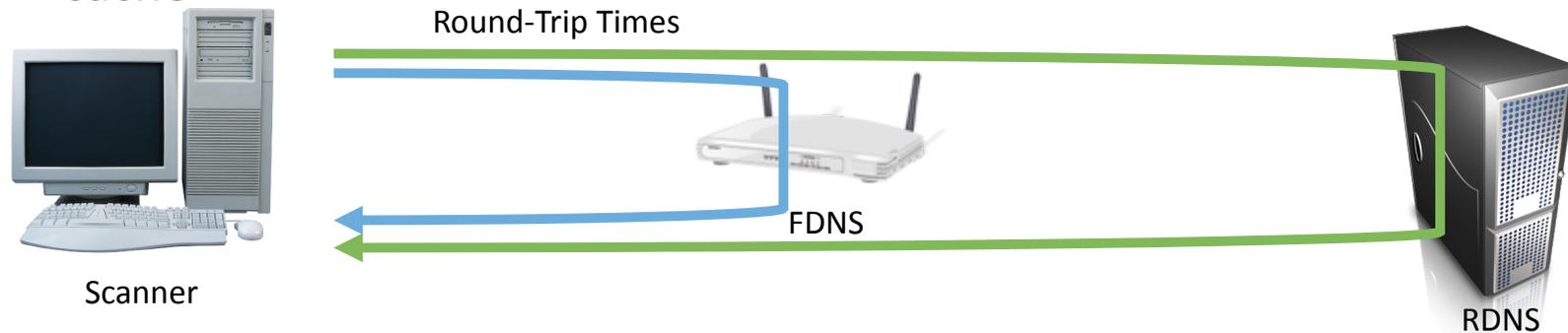
Implication: Phantom DDoS Attacks



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

Context: Are Preplay Vulnerable FDNS Used?

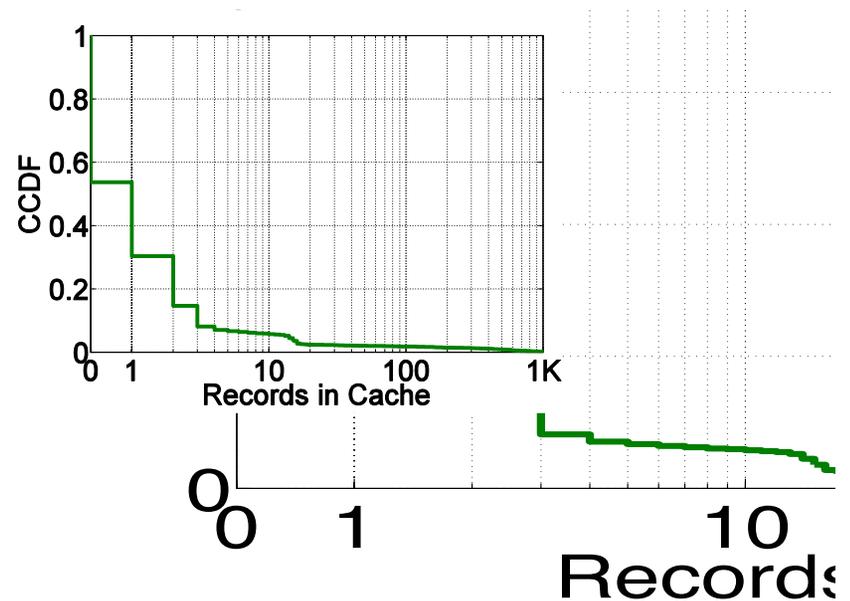
- Attack only effective if there are users behind the FDNS
- We test FDNS for use by looking for popular records in the FDNS's cache



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

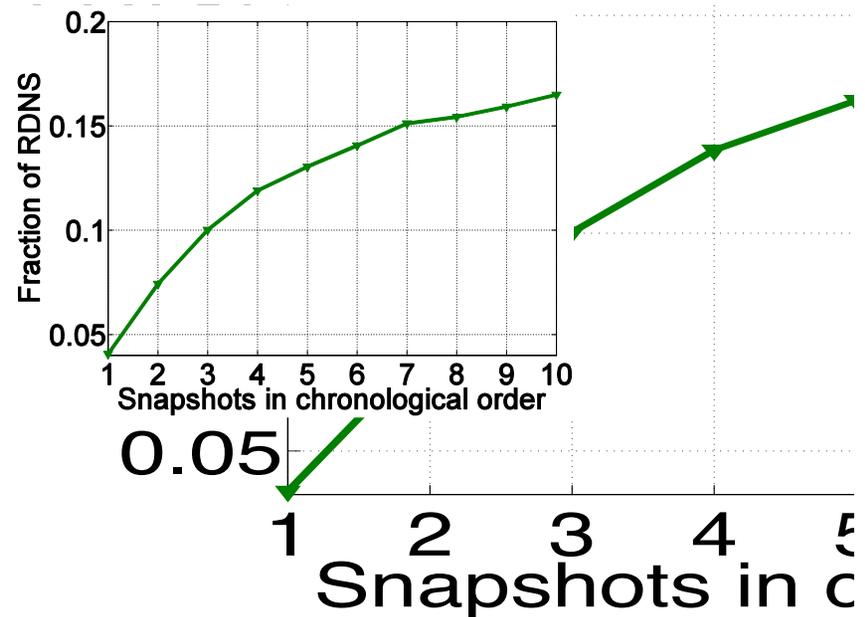
Context: Preplay Vulnerable FDNS Are Used!

- 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

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