OARC 36
29-30 November 2021

A Measurement-based Investigation of DNS Hijacking

Shuai Hao
Old Dominion University
Norfolk, Virginia, USA

Based on the Study

Rebekah Houser, Shuai Hao, Zhou Li, Daiping Liu, Chase Cotton, and Haining Wang.
A Comprehensive Measurement-based Investigation of DNS Hijacking,
International Symposium on Reliable Distributed System (***SRDS***), Sep. 2021.

paloalto NETWORKS
OLD DOMINION UNIVERSITY
UCI Samueli School of Engineering
University of California, Irvine
UNIVERSITY OF DELAWARE
VIRGINIA TECH

/ Shuai Hao

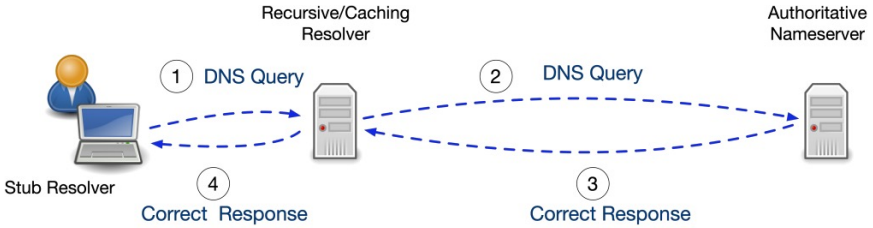
- **Assistant Professor,** 2019 – present,
  Department of Computer Science, ***Old Dominion University***, Norfolk, Virginia, USA
  - **Postdoc Researcher,** 2018 – 2019
    *Center for Applied Internet Data Analysis (**CAIDA**), UC San Diego,* La Jolla, California, USA
  - **Ph.D.,** 2017, Computer Science,
    College of William & Mary, Williamsburg, Virginia, USA

- **Research Overview**
  - Applying measurement, empirical, and data-driven approach to understand Internet Infrastructure and its security phenomena
    - Internet-Wide Vulnerability and Security
    - Internet Infrastructure and Measurement
    - Data-Driven Security Analytics
    - Cybercrime and Web security

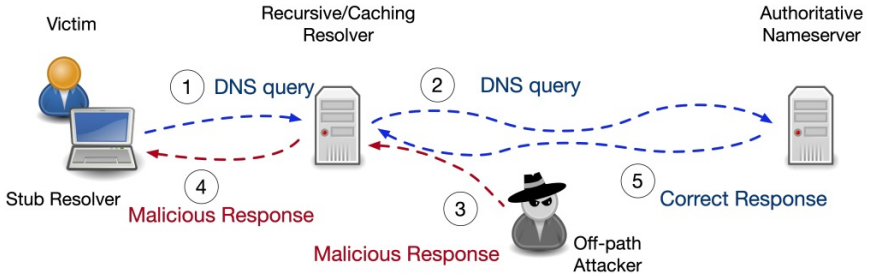
Outline

- Background and Motivation
- Measurements
- Detection
- Discussion

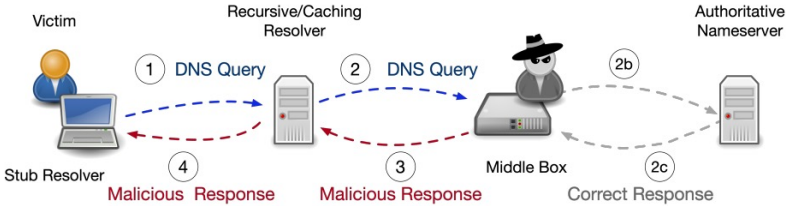
Background and Motivation



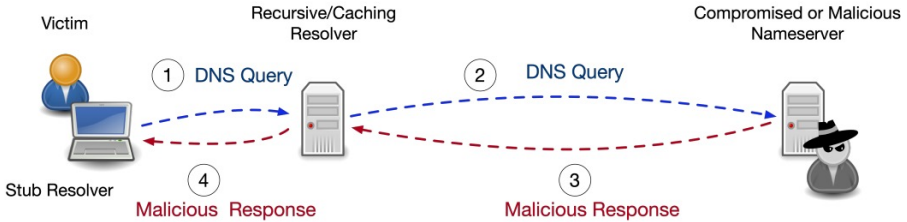
(a) The basic flow of a typical DNS resolution



(b) Off-path spoofing attack



(c) MITM attack



(d) Domain hijacking

Background and Motivation

KrebsonSecurity
In-depth security news and investigation

Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com

2011-2016

2018-2019

2017-2019

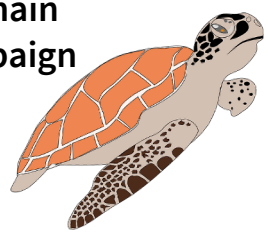
Naked Security

Angler exploit kit rings in 2016 with CryptoWall ransomware

Whatever happened on New Year's Eve, however, wasn't the end of Angler, because it was soon back to its 2015 infection levels. EXPLOIT KITS ...

Jan 21, 2016

Sea Turtle domain hijacking campaign



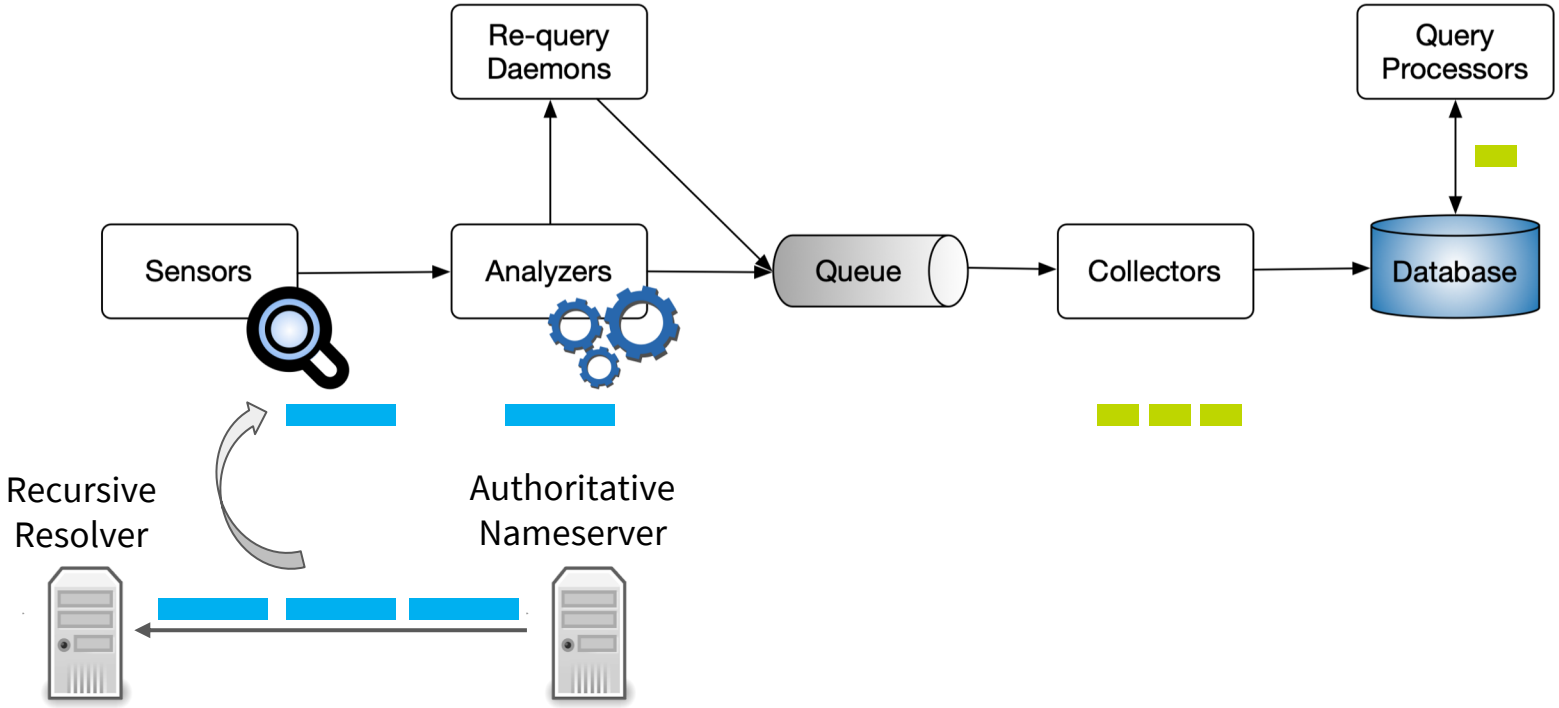
Background and Motivation

- **Goal of our Study**
  - Conduct an analysis based on confirmed DNS hijacking attacks to characterize known hijacking attack
  - Identify features for potential defense or monitoring mechanism

Outline

- Background and Motivation
- Measurements
- Detection
- Discussion

Measurements – Passive DNS Replication



Measurements – Dataset

```
"rrname": "www.ietf.org",
"rrtype": "A",
"rdata": "4.31.198.44",
```

Data derived directly from DNS responses

```
"time_first": 1384865833,
"time_last": 1389022219,
"count": 59
```

Metadata added by tools building PDNS database

Measurements – Dataset

- **Passive DNS Dataset**
  - Input from a *global network* of sensors and from zone files
  - Data collected for over *10 years*
  - Contains over *130 billion* sets of records with data

Measurements – Dataset

From news/stories/reports of DNS hijacking attacks or attack campaigns, we identified 34 such incidents that occurred over a period of 12 years (2008 to 2020)

We retrieved Indicators of Compromise (IOCs) for evidence of the attacks

	IP_A	NS_A	$FQDN_H$	$Apex_H$
Angler	454	0	22,571	5,249
Spammy Bear	1	0	4,007	4,007
Sea Turtle	33	5	30	21
Other	34	41	65	65

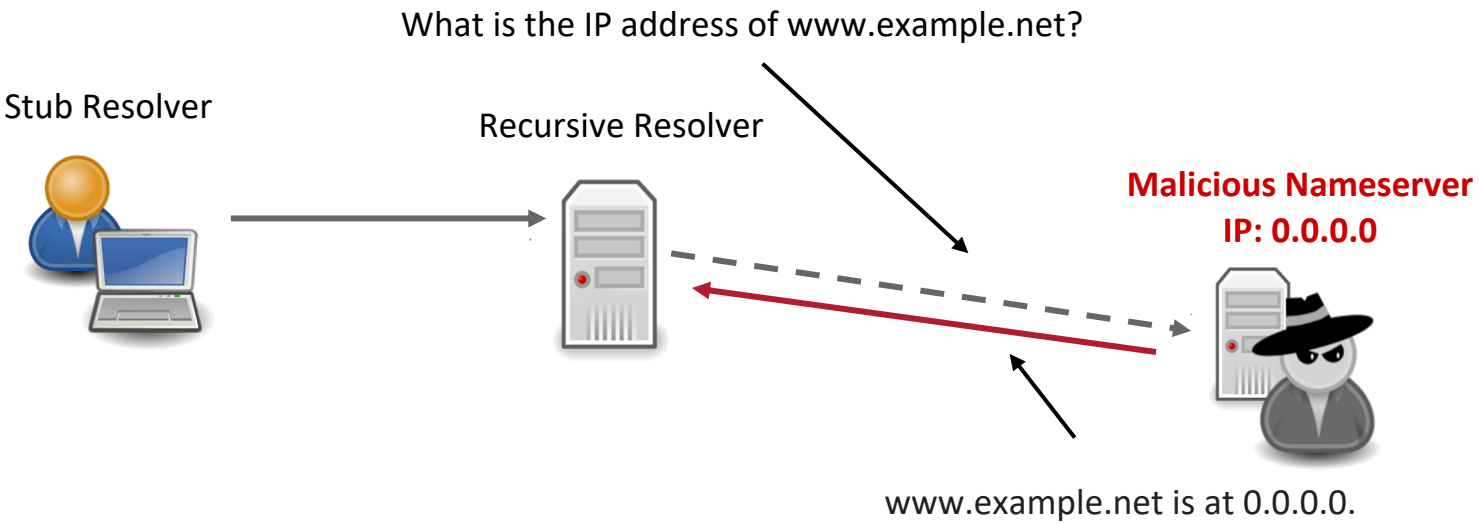
IP_A = Attacker IP addresses, NS_A = Attacker nameservers, $FQDN_H$ = Hijacked FQDNs, $Apex_H$ = Apex domain of hijacked FQDNs

Measurements – Characterization

- Attacker infrastructure
- New `rrnames` in DNS records for hijacked domains
- Record Types Changed

Measurements – Infrastructure

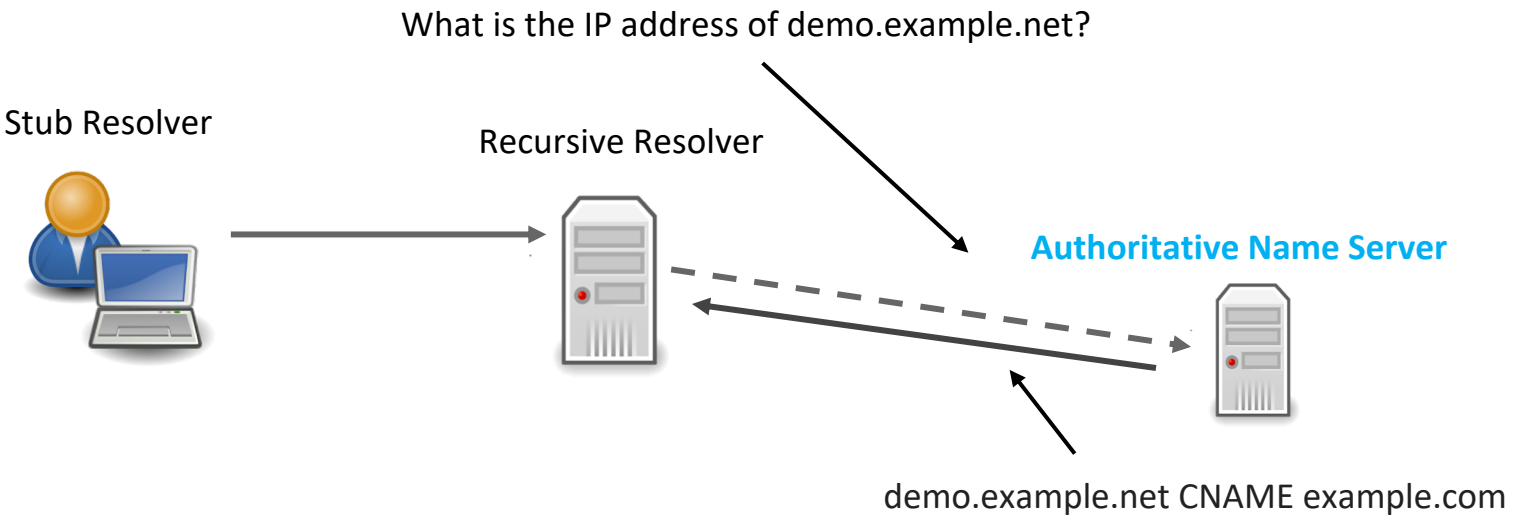
- Autonomous Systems
- Shared Hosting



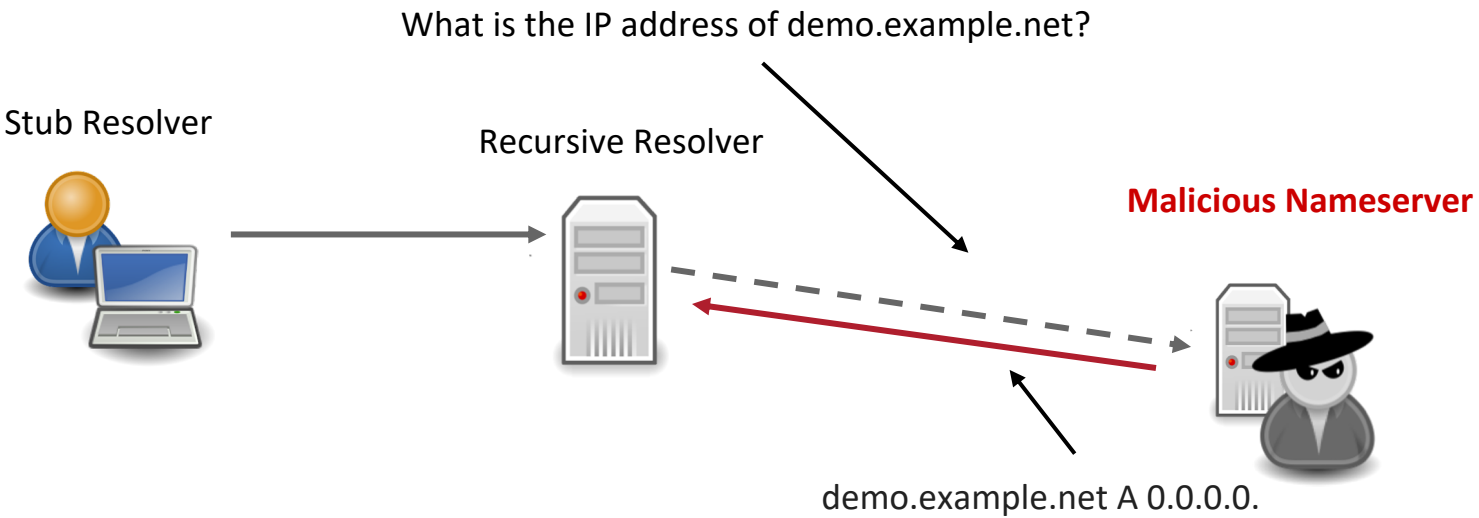
Measurements – Infrastructure

```
;; first seen: 2013-08-27 20:20:13 -0000
;;  last seen: 2013-08-28 03:18:15 -0000
nytimes.com. IN NS ns1.syrianelectronicarmy.com.
nytimes.com. IN NS ns2.syrianelectronicarmy.com.

;; first seen: 2013-08-27 20:20:13 -0000
;;  last seen: 2013-08-28 03:18:15 -0000
nytimes.com. IN A 141.105.64.37

;; first seen: 2013-06-17 08:01:54 -0000
;;  last seen: 2013-08-28 02:11:40 -0000
ns1.syrianelectronicarmy.com. IN A 141.105.64.37

;; first seen: 2013-06-17 08:01:54 -0000
;;  last seen: 2013-08-28 02:11:41 -0000
ns2.syrianelectronicarmy.com. IN A 141.105.64.37
```

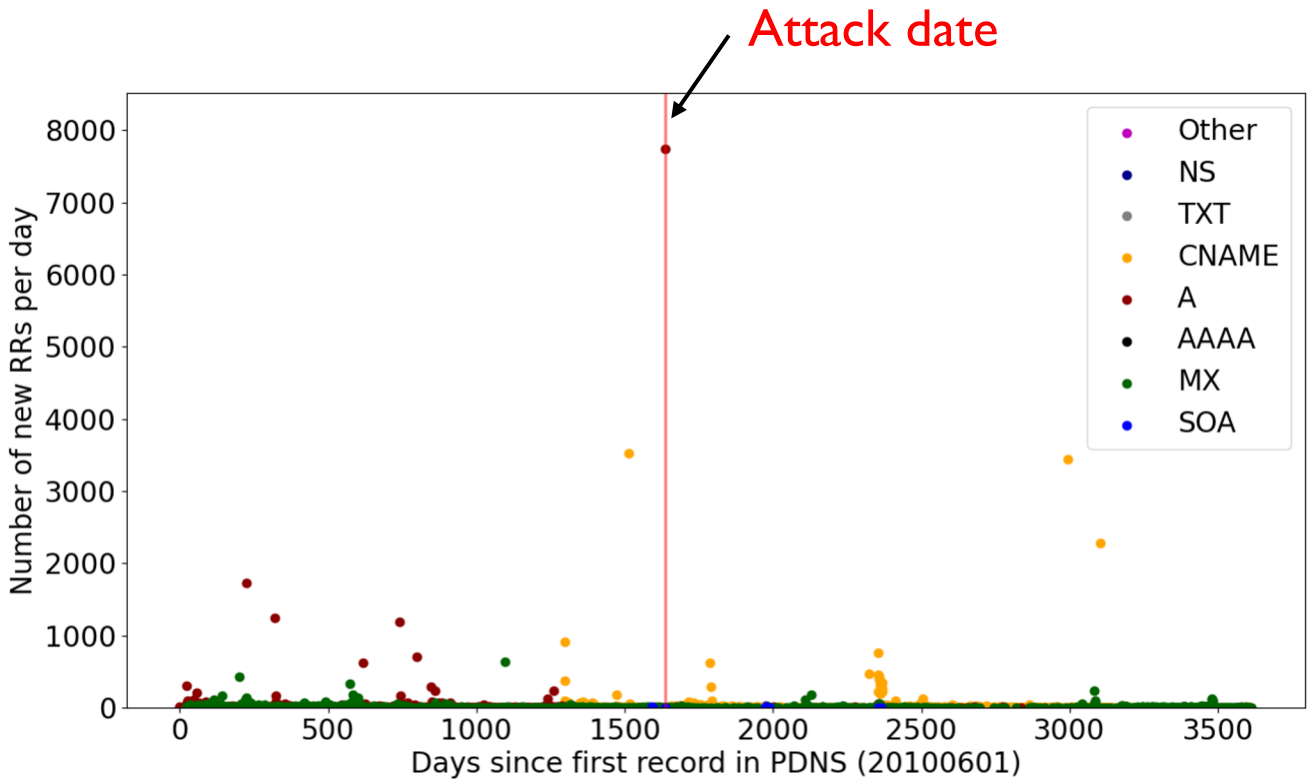
Measurements – New `rrnames`



Measurements – New `rrnames`



Measurements – New `rrnames`



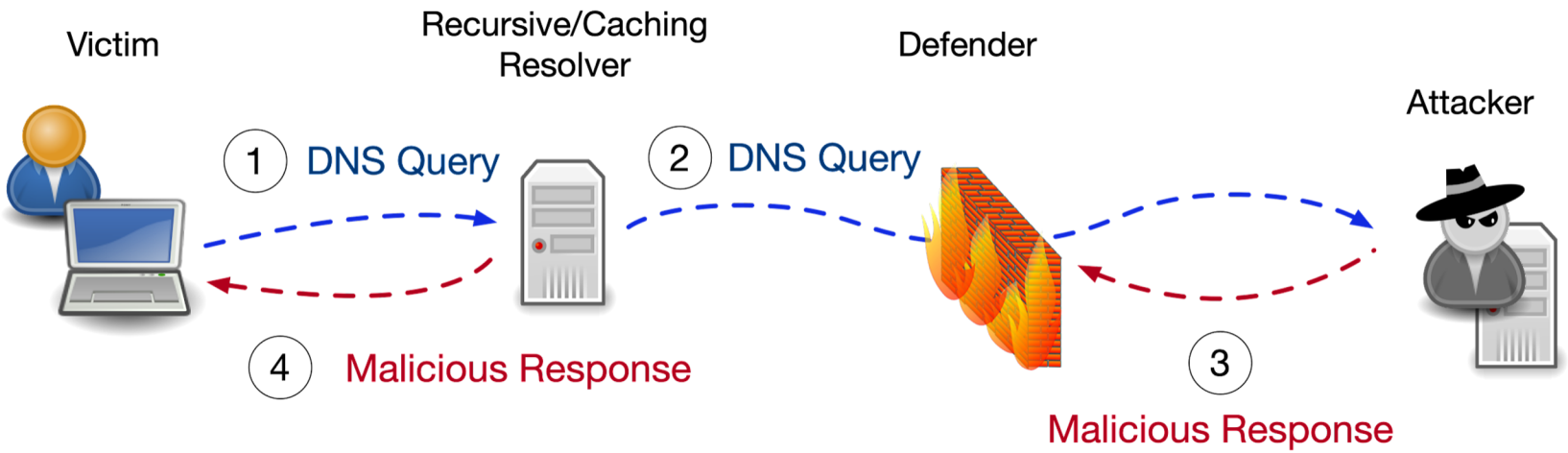
Measurements – Record Types Changed

RRTYPEs Changed	% Days	RRTYPEs Changed	% Days
A	29.63%	A	32.23%
NS A	20.99%	A AAAA	19.69%
NS CNAME A MX	11.11%	CNAME	14.93%
NS CNAME A	6.17%	AAAA	7.09%
NS A SOA	4.94%	A CNAME	6.01%
A AAAA	3.70%	MX	5.69%
NS	3.70%	A MX	1.88%
NS A AAAA SAO	3.70%	A AAAA CNAME	1.56%
NS A MX	2.47%	AAAA MX	1.52%
NS CNAME A AAAA SOA	2.47%	NS SOA A AAAA CNAME	0.82%
NS A MX SOA	2.47%	CNAME MX	0.81%
NS CNAME A AAAA MX SOA	2.47%	NS A CNAME	0.70%

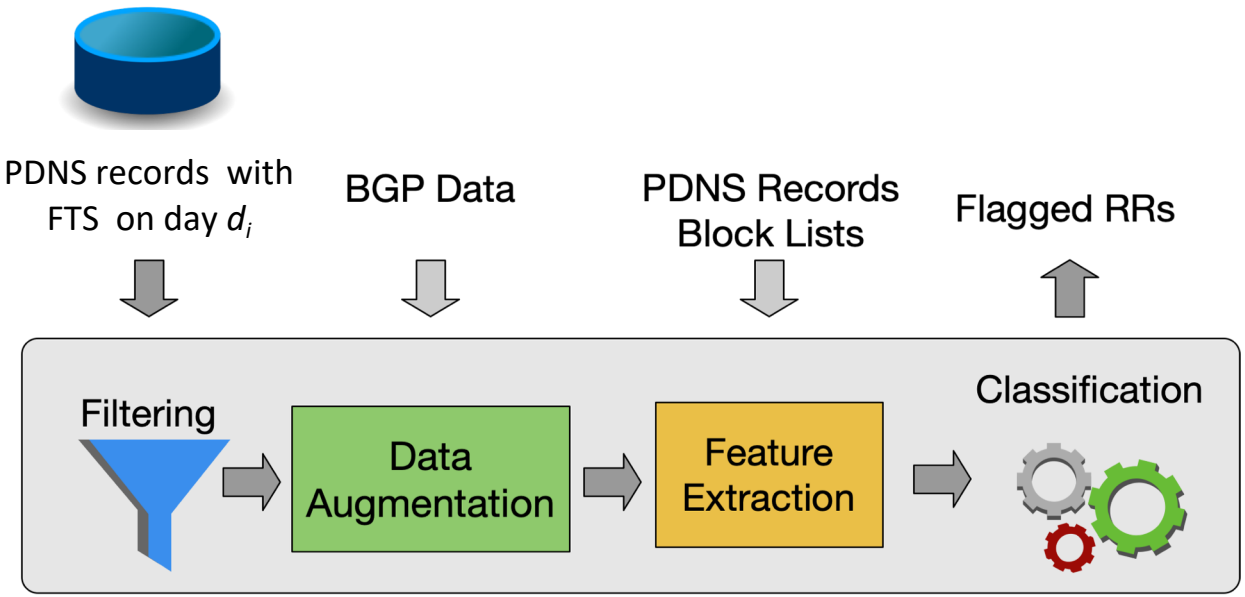
Outline

- Background and Motivation
- Measurements
- Detection
- Discussion

Detection – Threat Model



Detection – Experiment Design



Detection – Features

Feature Group	Description	Count
New A RR Features	Counts of new RRs, IPs, Countries, and Autonomous System Owners ASN blocklist information	5
New NS RR Features	Counts of new RRs, nameservers, and nameserver registered domains NS for registered domain or subdomain	5
New MX RR features	Counts of new RRs, mail servers, and mail server registered domains Preference information	4
Previously seen RRs	Number of A or NS records seen previously Number of Autonomous System owners in previously seen A records Number of nameserver registered domains in previously seen NS records	4
General Features	New RRs (other than A, NS, MX, or CNAME), new rrnames	2

Detection – Dataset

- **Dataset: PDNS records collected for hijacked domains and for domain similar to those commonly targeted in domain hijackings**
  - Alexa Top
  - Region-specific Alexa Popular
  - Alexa Business

Domain Group	Number of Domains	PDNS Records (million)
Hijacked Domains	86	13.6
Alexa Top	96	556.4
Region-specific Top	361	42.8
Alexa Business	359	44.3

Detection – Results

	Years in Dataset	Precision	Recall	FPR
Random Forest	2010-2013	0.85	0.73	0.02%
	2013-2016	0.85	0.65	0.02%
	2016-2020	0.8	0.57	0.04%
SVM	2010-2013	0.88	0.93	0.02%
	2013-2016	0.72	0.76	0.05%
	2016-2020	0.70	0.4	0.08%

Outline

- Background and Motivation
- Measurements
- Detection
- Discussion

Limitations and Future Direction

- Understanding the ability to detect attacks in real time would require testing in a live environment
  - Leveraging real DNS traces collected from security products deployed in global enterprise networks
- Attackers could evade the proposed approach by using DNS or hosting providers shared with their target

Summary and Conclusion

- A preliminary effort to investigating the characterization of domain hijacking and explore the potential detection/monitoring
- Domain hijacking attacks manifest themselves in various changes to hijacked domains' DNS records. These changes may be detected and leveraged to detect the attack.
- Changes to `NS` records are key indicator of domain hijacking attacks. Developing more sophisticated features related to these changes is a promising area of future research.

OARC 36
29-30 November 2021

Thank You!

A Measurement-based Investigation of DNS Hijacking

Shuai Hao, Old Dominion University
shao@odu.edu
https://shhaos.github.io

Based on the Study

Rebekah Houser, Shuai Hao, Zhou Li, Daiping Liu, Chase Cotton, and Haining Wang.
A Comprehensive Measurement-based Investigation of DNS Hijacking,
International Symposium on Reliable Distributed System (***SRDS***), Sep. 2021.

paloalto NETWORKS · OLD DOMINION UNIVERSITY · UCI Samueli School of Engineering, University of California, Irvine · University of Delaware · Virginia Tech