Unresolved Issues

Prevalence, Persistence, and Perils of Lame Delegations

Gautam Akiwate

IMC 2020

Mattijs Jonker, Raffaele Sommese, Geoffrey Voelker, Stefan Savage, and KC Claffy

UC San Diego

UNIVERSITY OF TWENTE.

What are Lame Delegations?

A lame delegation is when a nameserver delegated authority over a domain is unable to provide authoritative answers for that domain.

Motivation

Motivation

- Lame delegated domains take longer to resolve

Motivation

- Lame delegated domains take longer to resolve
- Increased load at nameservers
    - Lame delegated domains result in queries to nameservers that are not authoritative

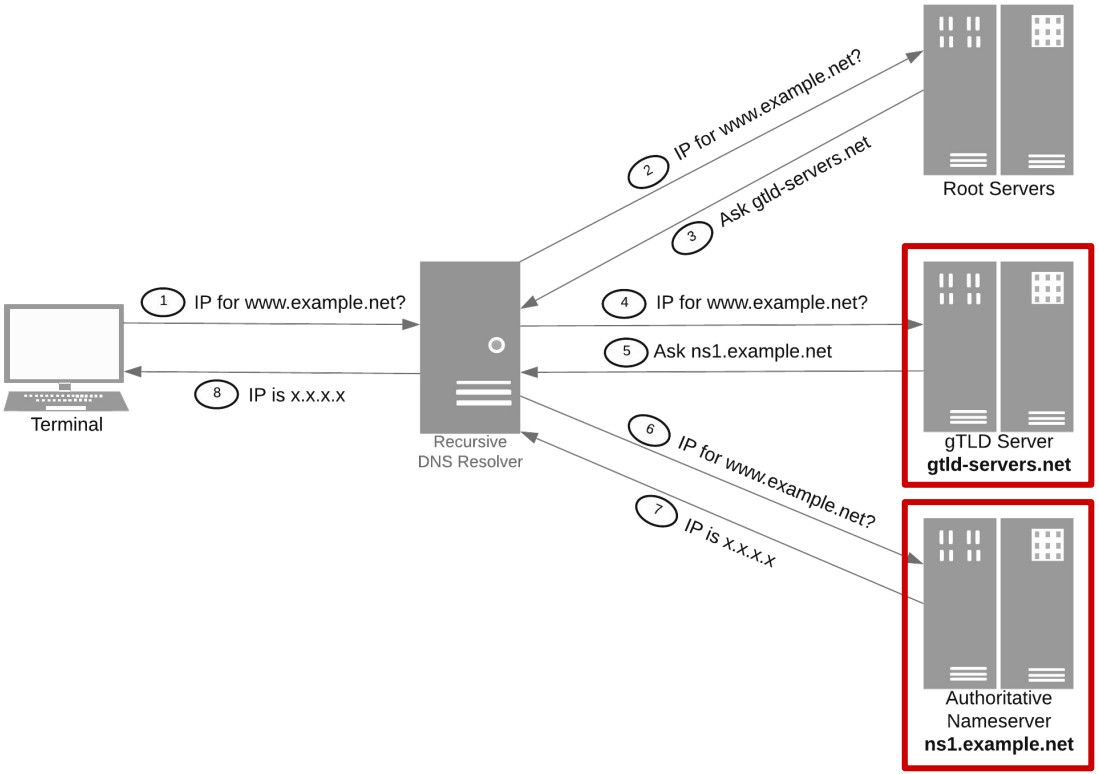
Motivation

- Lame delegated domains take longer to resolve
- Increased load at nameservers
  - Lame delegated domains result in queries to nameservers that are not authoritative
  - 12% of traffic to GoDaddy servers are for domains for which they are not authoritative

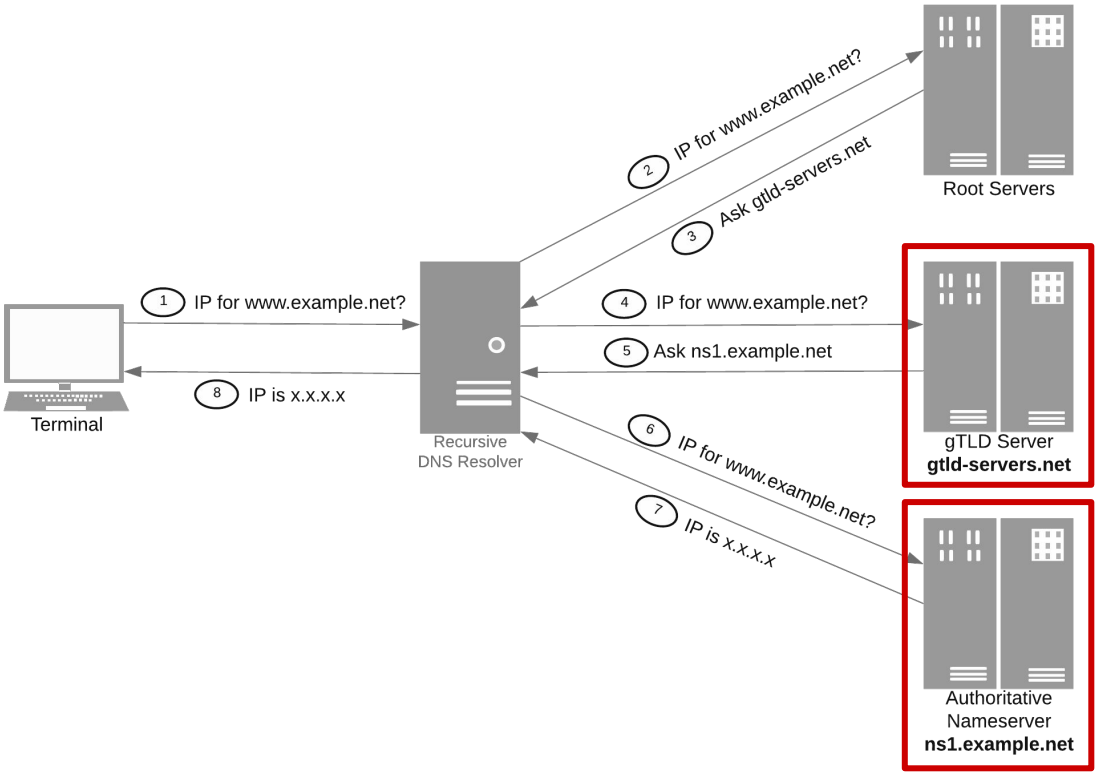
Motivation

- Lame delegated domains take longer to resolve
- Increased load at nameservers
  - Lame delegated domains result in queries to nameservers that are not authoritative
  - 12% of traffic to GoDaddy servers are for domains for which they are not authoritative
- Potential for security risks.
  - Potential for hijacking

Lame Delegations in Practice

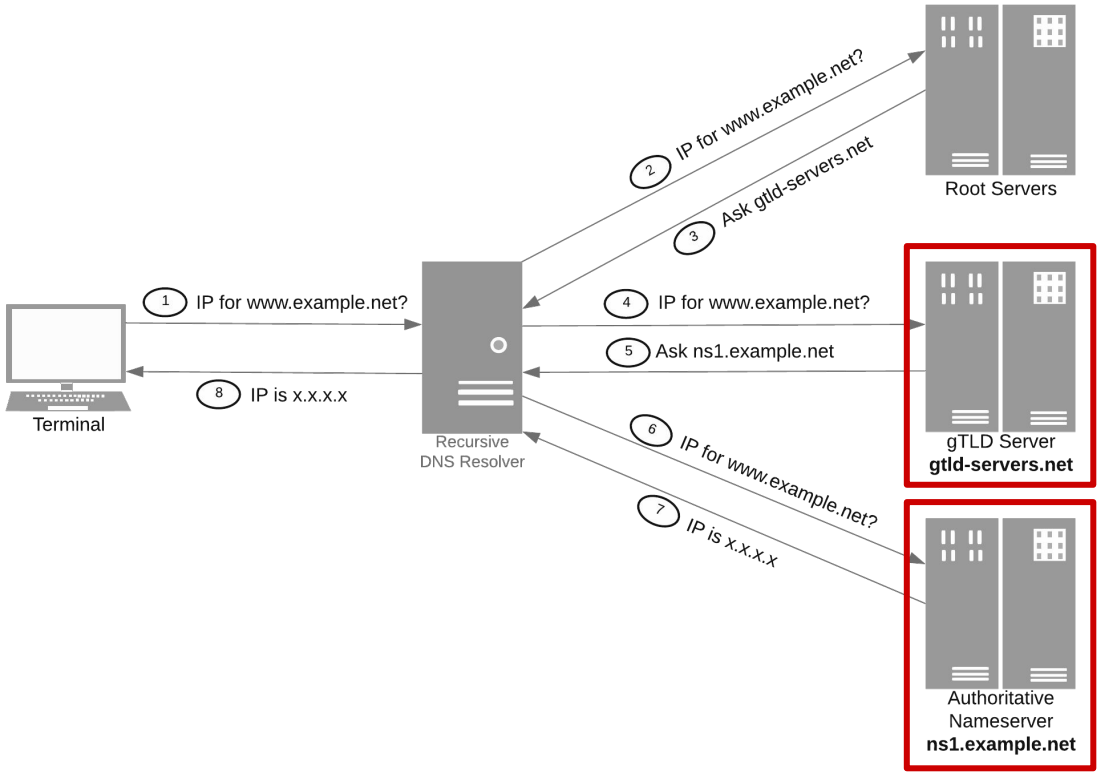


Lame Delegations in Practice



Incorrect NS listed

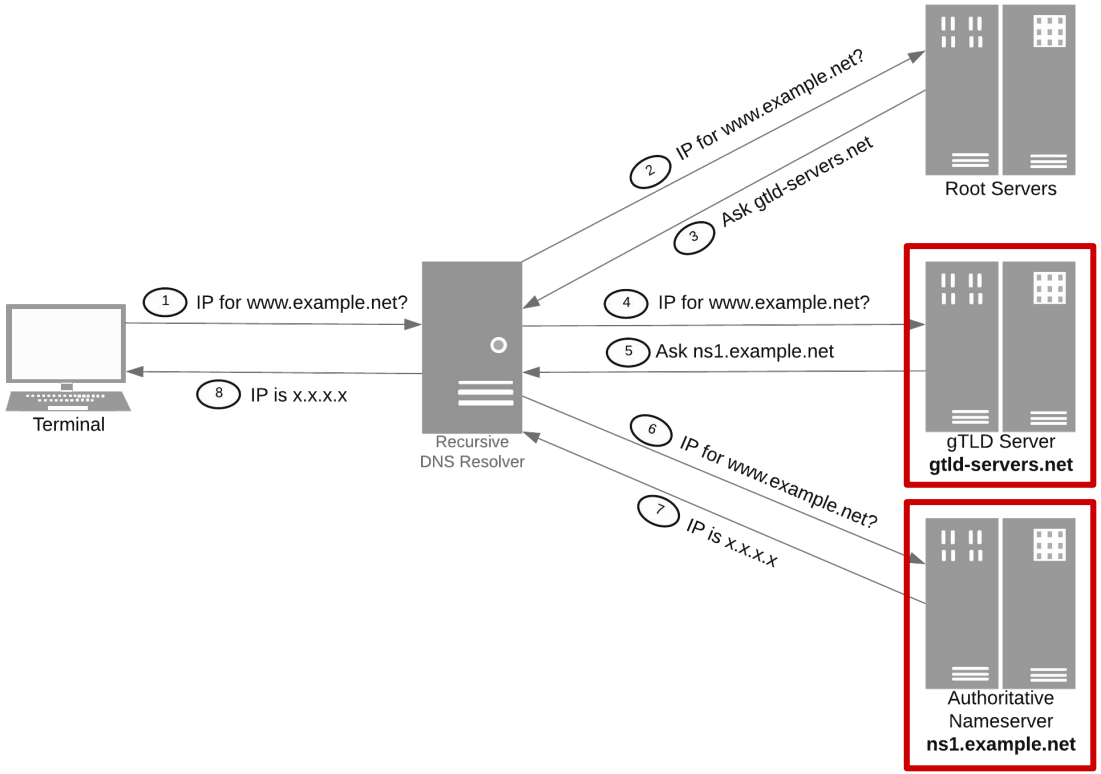
Lame Delegations in Practice



Incorrect NS listed

Misconfigured NS
Unreachable/Unavailable

Lame Delegations in Practice



Passive Analysis

Incorrect NS listed

Active Measurement

Misconfigured NS
Unreachable/Unavailable

Lame Delegations: Passive Analysis

Lame Delegations: Passive Analysis

- Longitudinal analysis using nine years of TLD zone files

Data Set: Eight Years of TLD Zone Files

DNS Coffee --- https://dns.coffee

- Daily snapshot of TLD zone files over **9 years**
- As of October 2020, collects and analyzes ~1250 TLDs
- Includes legacy gTLDs, new gTLDs, and three ccTLDs

Domains	Nameservers (NS)	IPv4 (A)	IPv6 (AAAA)
499.3 M	19.9 M	5.1 M	91.9 k

Lame Delegations: Passive Analysis

- Longitudinal analysis using nine years of TLD zone files
- Use *“static resolution”* to determine if nameserver can be resolved.
- Conservative assumptions. Lower bound of lame delegations.

“Static Resolution” of Zone Files

NS and A Records from Zone Files  “Resolvable” Time Periods for Nameservers

“Static Resolution” of Zone Files

NS and A Records from Zone Files  “Resolvable” Time Periods for Nameservers

- Nameserver is “resolvable”
  - Glue record

“Static Resolution” of Zone Files

NS and A Records from Zone Files → “Resolvable” Time Periods for Nameservers

- Nameserver is “resolvable”
  - Glue record
  - Nameserver domain has a nameserver that is “resolvable”

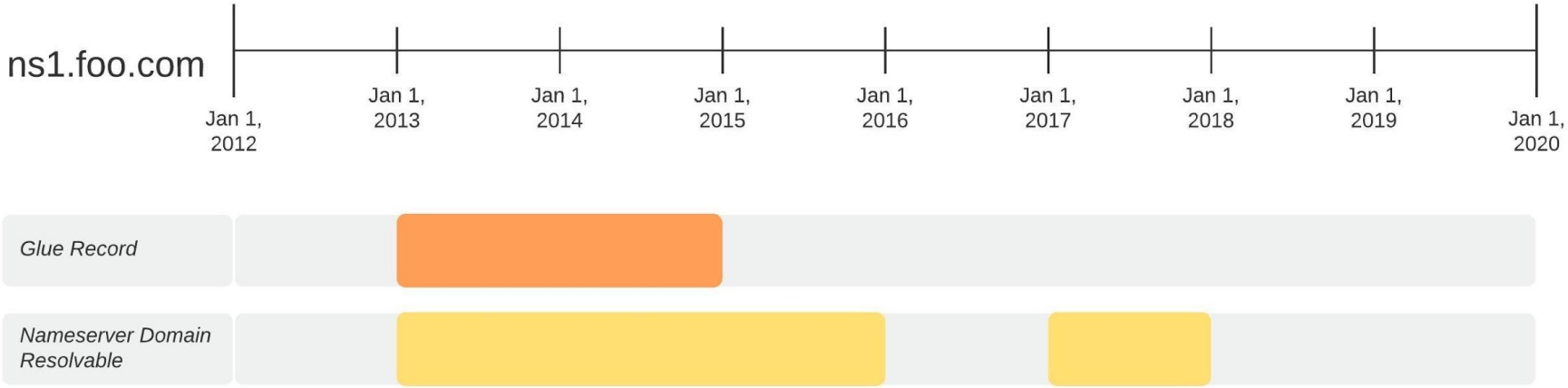
“Static Resolution” of Zone Files

NS and A Records from Zone Files → “Resolvable” Time Periods for Nameservers

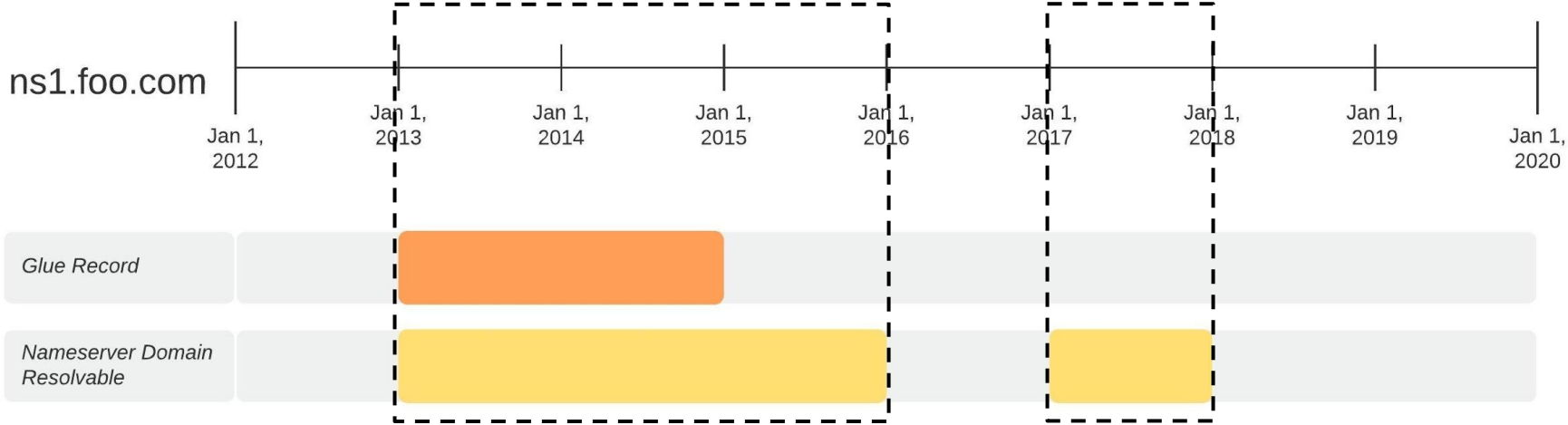
- Conservative Assumptions
  - Assume nameserver is “resolvable” when in doubt

- Nameserver is “resolvable”
  - Glue record
  - Nameserver domain has a nameserver that is “resolvable”

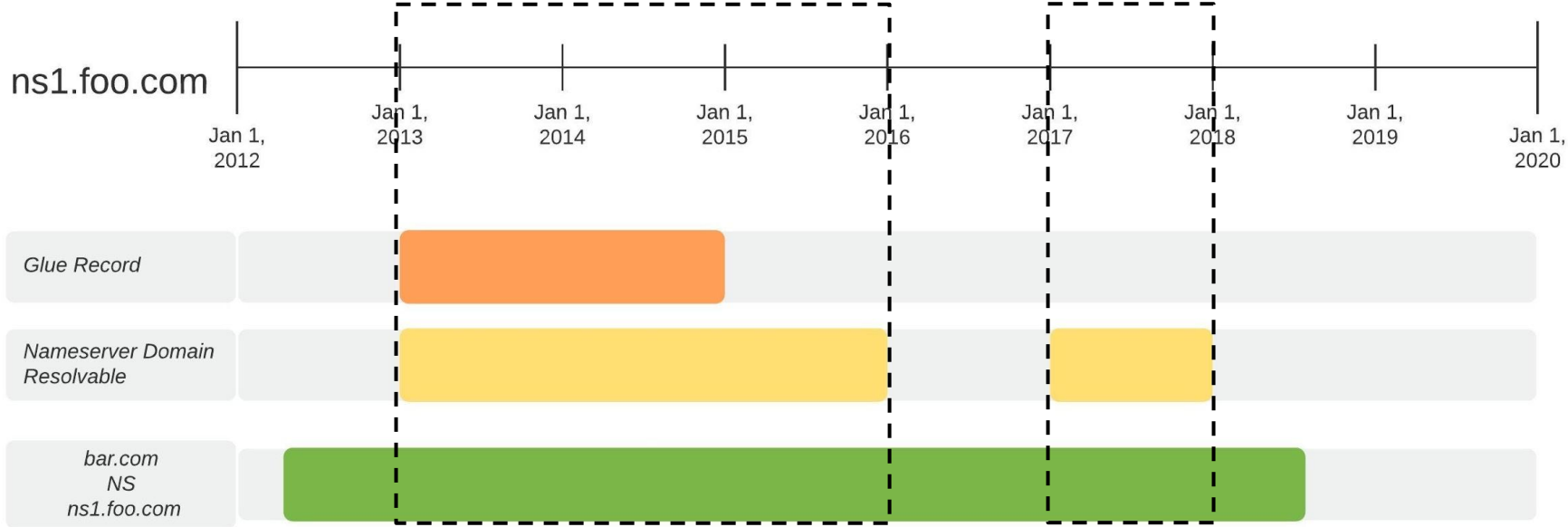
Nameserver Resolvable Time Periods



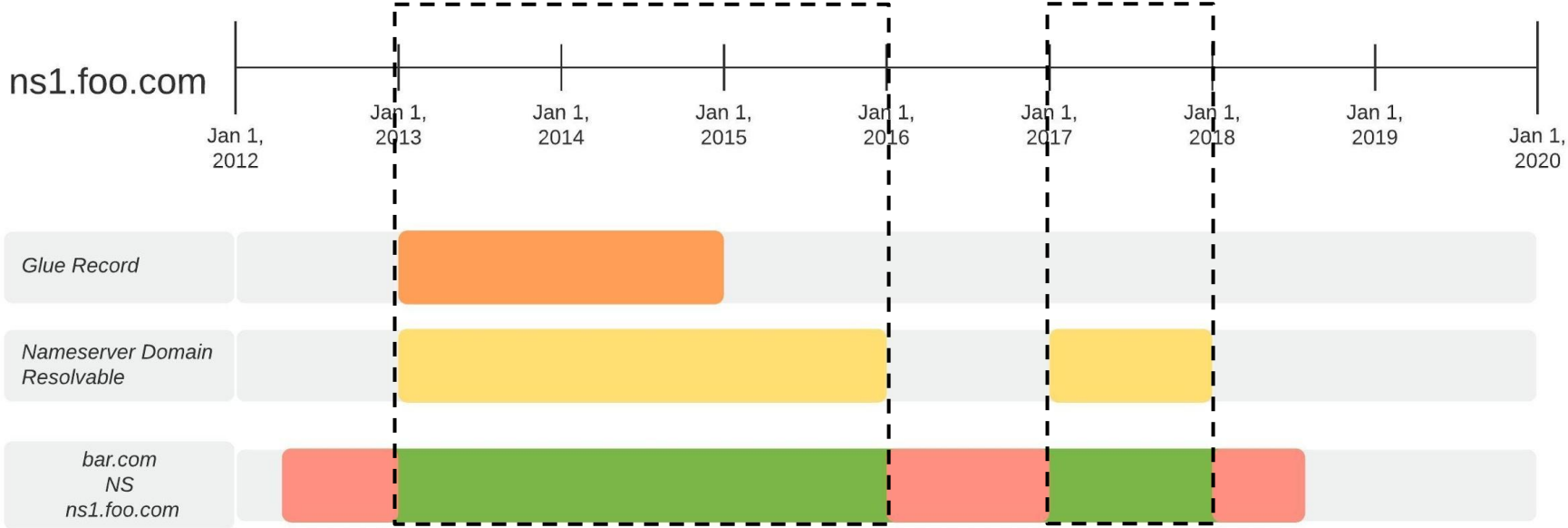
Nameserver Resolvable Time Periods



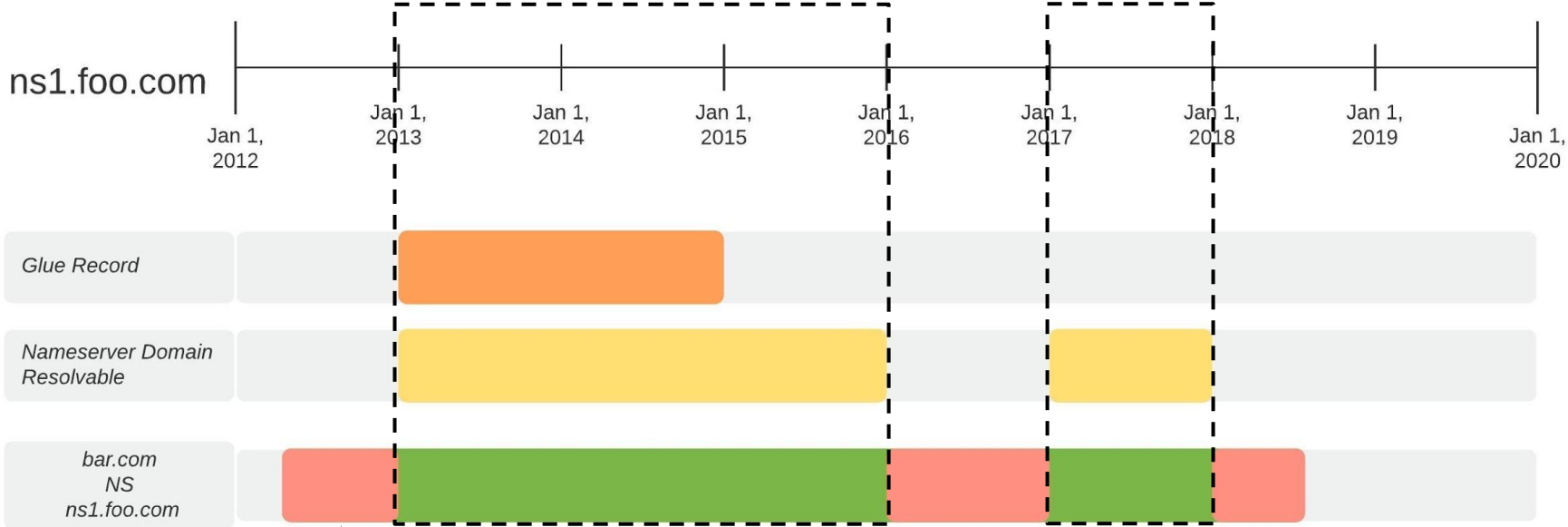
Nameserver Resolvable Time Periods



Nameserver Resolvable Time Periods



Nameserver Resolvable Time Periods

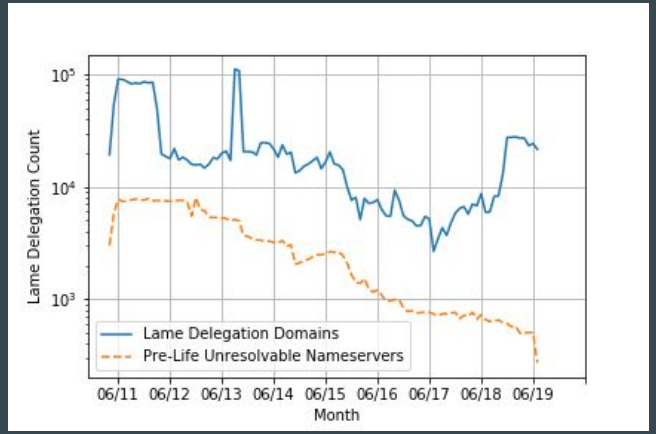


Pre-Life

- Domain delegates to a nameserver before it is first resolvable.

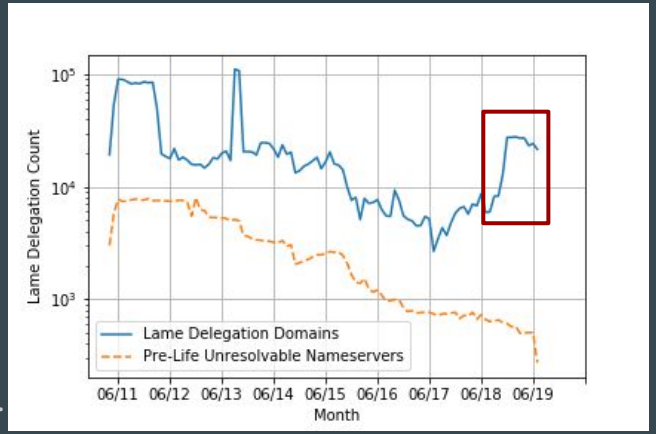
Pre-Life

- Domain delegates to a nameserver before it is first resolvable.
- Delayed registration of nameserver domain



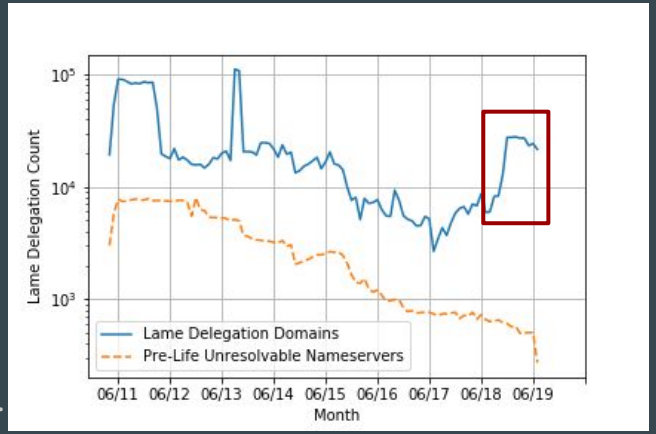
Pre-Life

- Domain delegates to a nameserver before it is first resolvable.
- Delayed registration of nameserver domain
- Typo when entering nameserver
  - ns5.dsndun.net instead of ns5.dnsdun.net
  - ~20,000 domains lame delegated for nearly a year in 2018-19.



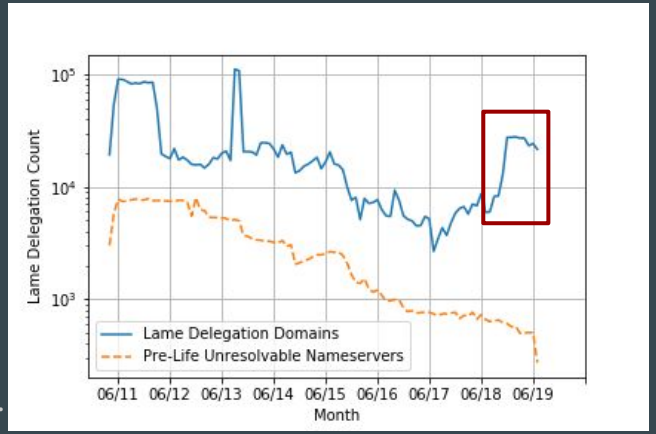
Pre-Life

- Domain delegates to a nameserver before it is first resolvable.
- Delayed registration of nameserver domain
- Typo when entering nameserver
  - ns5.dsndun.net instead of ns5.dnsdun.net
  - ~20,000 domains lame delegated for nearly a year in 2018-19.
  - Security risk: dsndun.net was registered by another actor soon after.

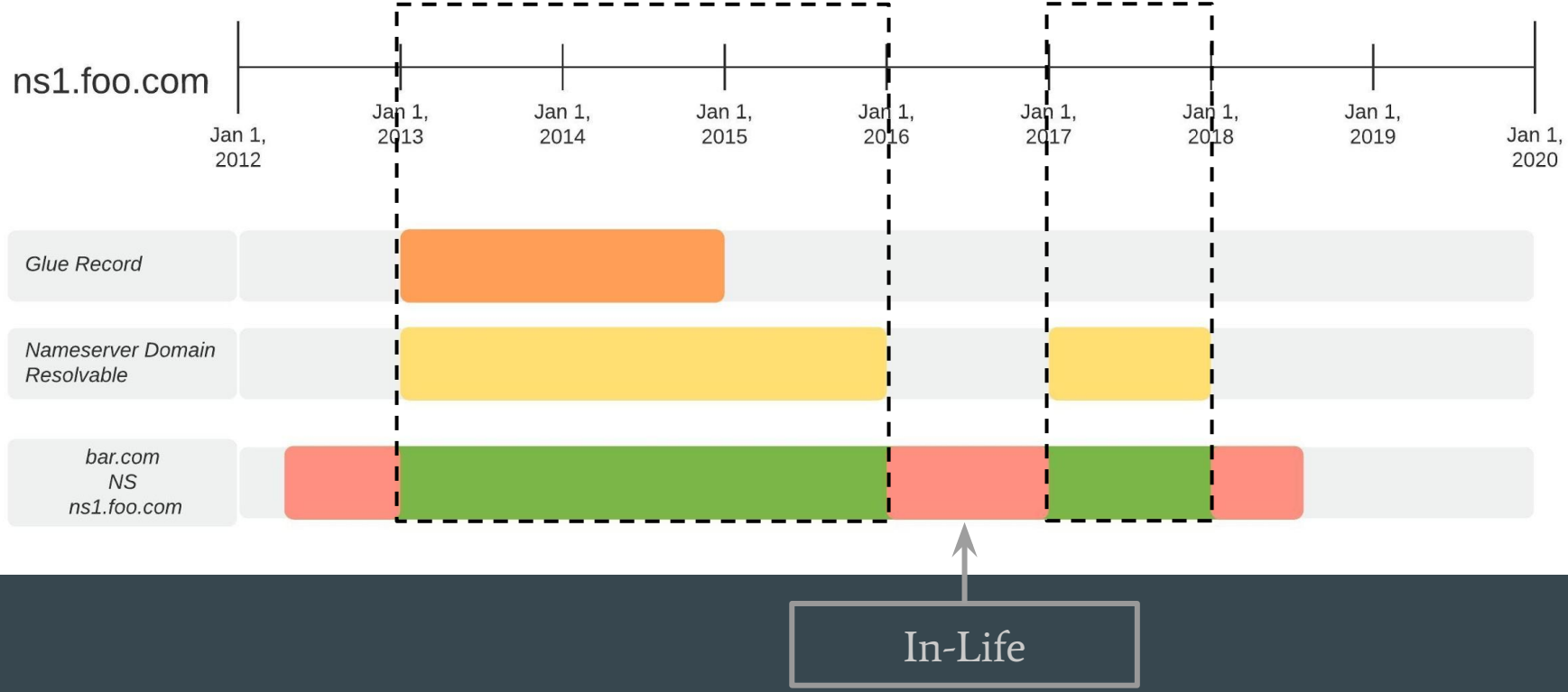


Pre-Life

- Domain delegates to a nameserver before it is first resolvable.
- Delayed registration of nameserver domain
- Typo when entering nameserver
  - ns5.dsndun.net instead of ns5.dnsdun.net
  - ~20,000 domains lame delegated for nearly a year in 2018-19.
  - Security risk: dsndun.net was registered by another actor soon after.
  - Functioning alternate nameservice can hide delegation issues.

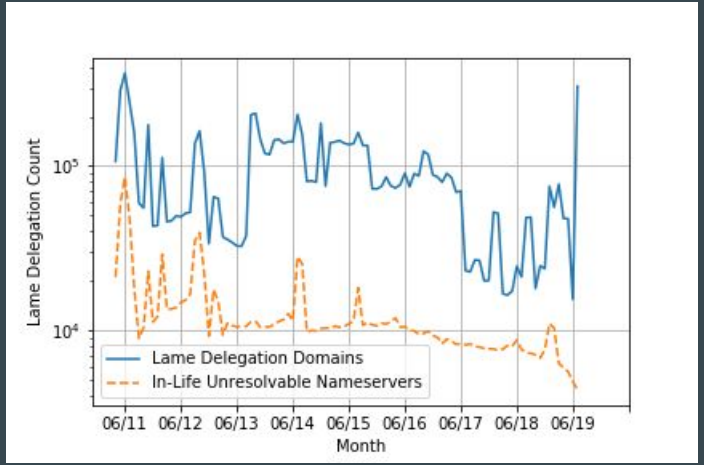


Nameserver Resolvable Time Periods



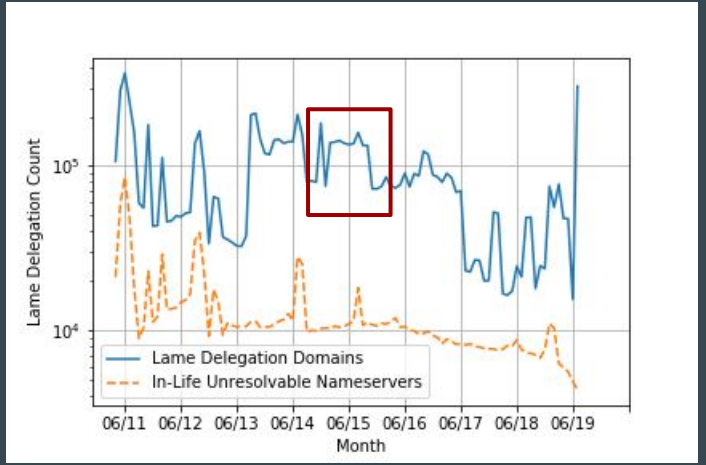
In-Life: Conficker Working Group Saga

- Nameserver is briefly unresolvable.
- Misconfiguration
- Delay in nameserver domain renewal.



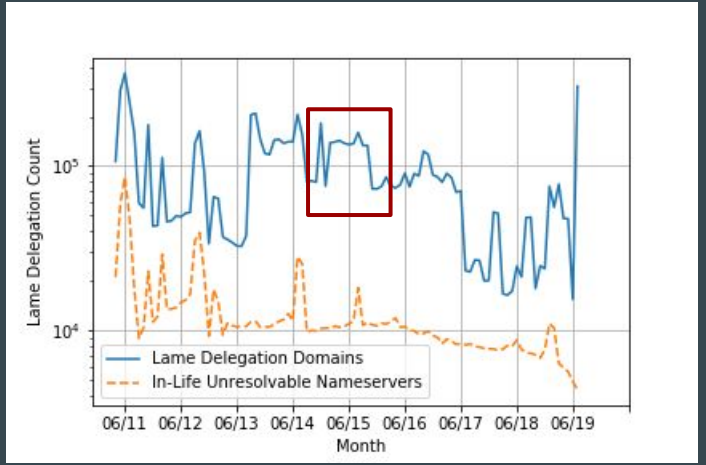
In-Life: Conficker Working Group Saga

- Nameserver is briefly unresolvable.
- Misconfiguration
- Delay in nameserver domain renewal.
- Conficker Working Group Saga
    - *.cwgsh.[com, net, org] used as sink nameservers for Conficker Worm domains



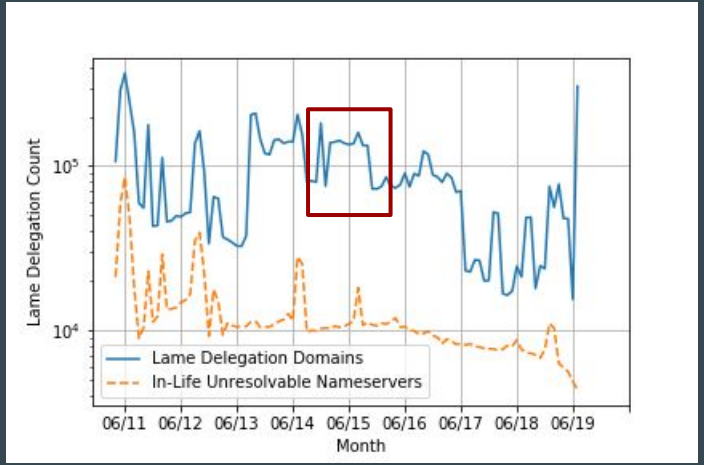
In-Life: Conficker Working Group Saga

- Nameserver is briefly unresolvable.
- Misconfiguration
- Delay in nameserver domain renewal.
- Conficker Working Group Saga
  - *.cwgsh.[com, net, org] used as sink nameservers for Conficker Worm domains
  - Allowed to expire. Registered by other actors.



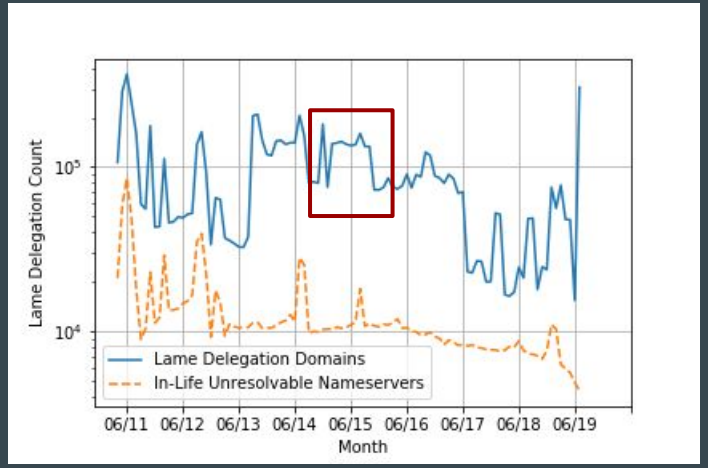
In-Life: Conficker Working Group Saga

- Nameserver is briefly unresolvable.
- Misconfiguration
- Delay in nameserver domain renewal.
- Conficker Working Group Saga
  - *.cwgsh.[com, net, org] used as sink nameservers for Conficker Worm domains
  - Allowed to expire. Registered by other actors.
  - Major effort to move domains off cwgsh to conficker-sinkhole.com

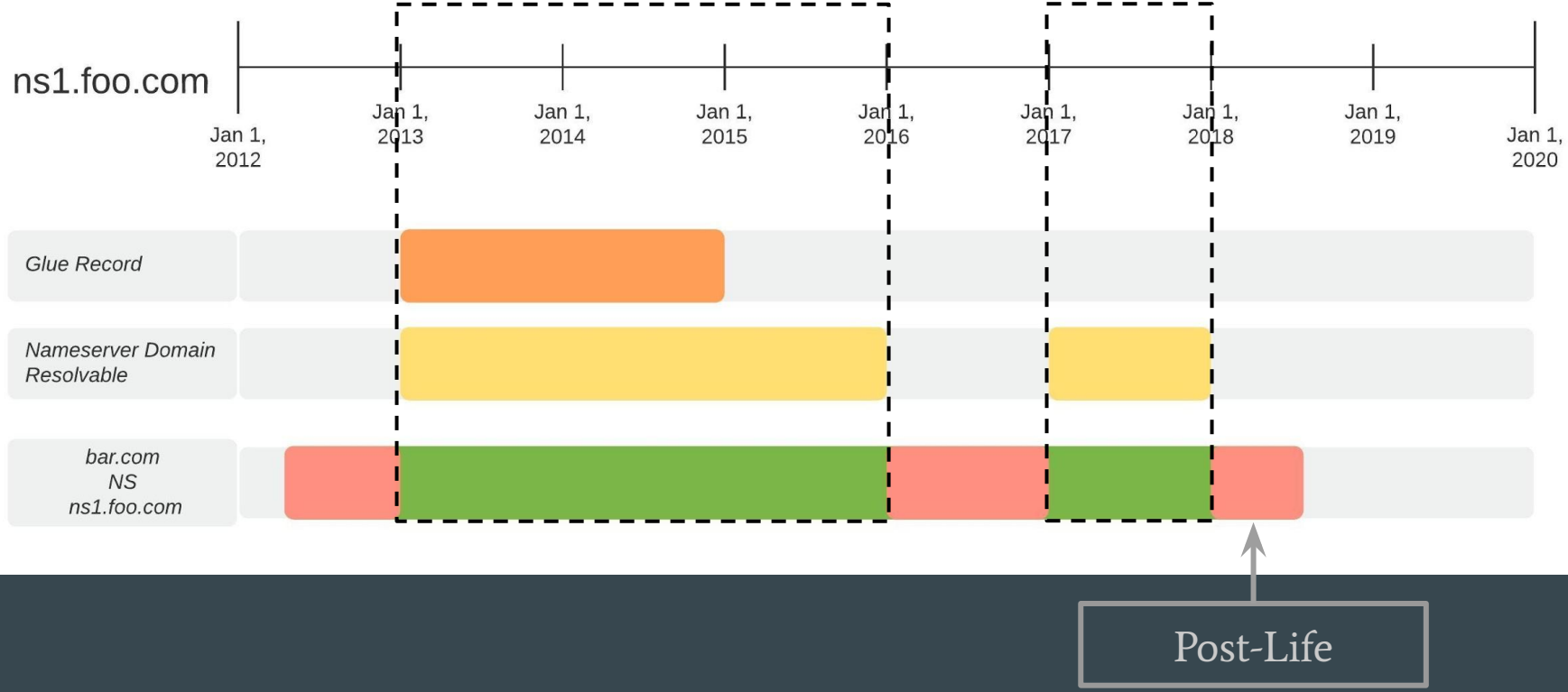


In-Life: Conficker Working Group Saga

- Nameserver is briefly unresolvable.
- Misconfiguration
- Delay in nameserver domain renewal.
- Conficker Working Group Saga
  - *.cwgsh.[com, net, org] used as sink nameservers for Conficker Worm domains
  - Allowed to expire. Registered by other actors.
  - Major effort to move domains off cwgsh to conficker-sinkhole.com
  - Registration for conficker-sinkhole.com lapses. Renewed during the grace period.



Nameserver Resolvable Time Periods



Post-Life

- Nameserver stop beings resolvable
    - Domain expires. Not renewed.
- Nameserver was never resolvable

Post-Life: TLD Anomaly

Unresolvable Nameservers by TLD	
Nameserver TLD	**# Post-Life Unresolvable NS (% of Total in TLD)**
.com	85,899 (1.00%)
.net	24,997 (1.45%)
.org	17,438 (1.77%)
.info	10,207 (0.86%)
ccTLDs	4,920 (0.73%)
ngTLDs	14,474 (0.29%)
.biz	181,211 (48.1%)

Post-Life: TLD Anomaly

Unresolvable Nameservers by TLD	
Nameserver TLD	**# Post-Life Unresolvable NS (% of Total in TLD)**
.com	85,899 (1.00%)
.net	24,997 (1.45%)
.org	17,438 (1.77%)
.info	10,207 (0.86%)
ccTLDs	4,920 (0.73%)
ngTLDs	14,474 (0.29%)
.biz	181,211 (48.1%)

- **48%** of all nameservers ending *.biz* are never resolvable.

Post-Life: TLD Anomaly

Unresolvable Nameservers by TLD	
Nameserver TLD	**# Post-Life Unresolvable NS (% of Total in TLD)**
.com	85,899 (1.00%)
.net	24,997 (1.45%)
.org	17,438 (1.77%)
.info	10,207 (0.86%)
ccTLDs	4,920 (0.73%)
ngTLDs	14,474 (0.29%)
.biz	181,211 (48.1%)

- **48%** of all nameservers ending *.biz* are never resolvable.
- The *.biz* registry has no visibility since nameservers are referenced in other TLDs. So not a *.biz* issue.

Example of .biz post-life unresolvable nameserver

White County, Georgia Official Domain: *whitecounty.net*

Example of .biz post-life unresolvable nameserver

White County, Georgia Official Domain: *whitecounty.net*

whitecounty.net
NS
ns1.hemc.net
ns2.internetemc.com

nameserver change
on July 01, 2019

whitecounty.net
NS
ns1.hemc.net
ns2.internetemc1aj2tkdy.biz

internetemc1aj2tkdy.biz
is NOT registered

Example of .biz post-life unresolvable nameserver

White County, Georgia Official Domain: *whitecounty.net*

whitecounty.net
NS
ns1.hemc.net
ns2.internetemc.com

nameserver change
on July 01, 2019

whitecounty.net
NS
ns1.hemc.net
ns2.internetemc1aj2tkdy.biz

internetemc1aj2tkdy.biz
is NOT registered

Functioning alternate nameservice can hide underlying delegation issues.

Lame Delegations through EPP

- Undocumented registrar practice to get around EPP constraints.

Lame Delegations through EPP

- Undocumented registrar practice to get around EPP constraints.
- Lame Delegations not due to domain owner actions but registrar actions.

Lame Delegations through EPP

- Undocumented registrar practice to get around EPP constraints.
- Lame Delegations not due to domain owner actions but registrar actions.
- Creates lame delegations and security risks!
- Tens of thousands of domains affected
- Actors exploiting these vulnerable domains!

Lame Delegations: Active Measurement

Lame Delegations: Active Measurement

- Queried 49M domains as part of measurement campaign
  - Entire .net (13.1M domains), and .org (10M domains)
  - Random sample of 13M domains from .com, and ngTLDs

Lame Delegations: Active Measurement

- Queried 49M domains as part of measurement campaign
  - Entire .net (13.1M domains), and .org (10M domains)
  - Random sample of 13M domains from .com, and ngTLDs
- Measurement done from a vantage point connected to Netherlands NREN

Lame Delegations: Active Measurement

- Queried 49M domains as part of measurement campaign
  - Entire .net (13.1M domains), and .org (10M domains)
  - Random sample of 13M domains from .com, and ngTLDs
- Measurement done from a vantage point connected to Netherlands NREN
- For every `(domain, nameserver)` pair
  - Target NS queries to up to 5 IP resolutions for nameserver

Lame Delegations: Active Measurement

- Queried 49M domains as part of measurement campaign
  - Entire .net (13.1M domains), and .org (10M domains)
  - Random sample of 13M domains from .com, and ngTLDs
- Measurement done from a vantage point connected to Netherlands NREN
- For every `(domain, nameserver)` pair
  - Target NS queries to up to 5 IP resolutions for nameserver
- Allows us to identify partially lame domains!

Active Measurement Results

	.com	ngTLDs	.net	.org	**Total**
Domains Queried	**13 M**	**13 M**	**13.1 M**	**10 M**	**49.1 M**
Fully Lame	8.7%	9.6%	10.5%	9.2%	9.5%
Partially Lame	11.8%	19.8%	13.5%	11.7%	14.3%

Active Measurement Results

	.com	ngTLDs	.net	.org	**Total**
Domains Queried	**13 M**	**13 M**	**13.1 M**	**10 M**	**49.1 M**
Fully Lame	8.7%	9.6%	10.5%	9.2%	9.5%
Partially Lame	11.8%	19.8%	13.5%	11.7%	14.3%

- Lame Delegations even in popular domains
  - archive.org -- Alexa 200 domain -- has a lame delegation

Active Measurement Results

	.com	ngTLDs	.net	.org	**Total**
Domains Queried	**13 M**	**13 M**	**13.1 M**	**10 M**	**49.1 M**
Fully Lame	8.7%	9.6%	10.5%	9.2%	9.5%
Partially Lame	11.8%	19.8%	13.5%	11.7%	14.3%

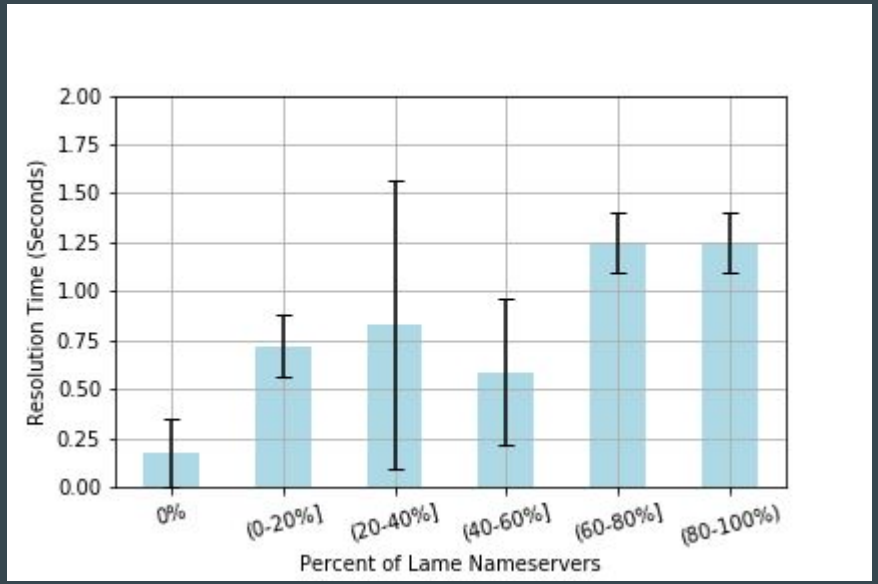
- Functioning alternate nameservice can hide broken delegations from domain owner.

Fully Lame Delegated Nameservers: By TLD

Lame Nameservers by TLD		
Nameserver TLD	**# Queried NS**	**Fully Lame NS**
.com	176,897	57,137 (32.3%)
.net	97,160	30,896 (31.8%)
.org	38,825	14,792 (38.1%)
.info	2,690	731 (27.2%)
ccTLDs	65,041	16,585 (25.5%)
ngTLDs	40,792	19,213 (47.1%)
.biz	14,311	10,533 (73.6%)

Increase in Resolution Time

- Lame delegated domains show 3.7x increase in resolution time.



More Details and Analysis in Paper...

Summary

Summary

- Lame delegations still prevalent in DNS today
  - 15% of domains actively queried have a lame delegation
  - Redundancy can mask lame delegations from domain owner

Summary

- Lame delegations still prevalent in DNS today
  - 15% of domains actively queried have a lame delegation
  - Redundancy can mask lame delegations from domain owner
- Lame delegations are also created due to systematic issues unrelated to domain owner misconfiguration
  - Unintended consequences of registrar practices

Summary

- Lame delegations still prevalent in DNS today
  - 15% of domains actively queried have a lame delegation
  - Redundancy can mask lame delegations from domain owner
- Lame delegations are also created due to systematic issues unrelated to domain owner misconfiguration
  - Unintended consequences of registrar practices
- Impacts of lame delegations
  - Cause unnecessary query load
  - Increase resolution time
  - Can put domains at risk of hijack

Thanks!

gakiwate@cs.ucsd.edu