

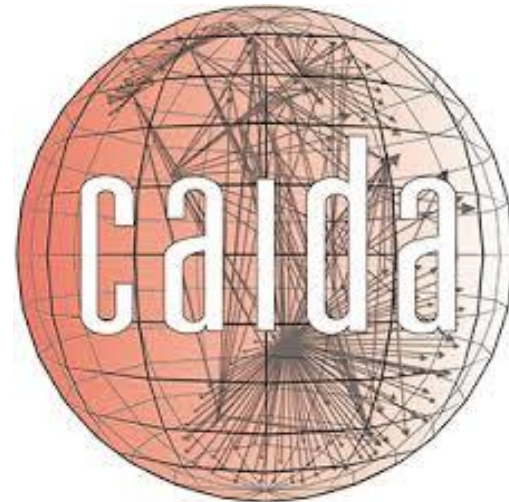
The background features several overlapping, flowing, ribbon-like shapes in shades of deep red and purple, creating a sense of movement and depth. These shapes are set against a dark gray background. The title text is centered within a white rectangular frame that overlaps these shapes.

# The Forgotten Side of DNS: Orphan and Abandoned Records

R. Somnese, M. Jonker, R. van Rijswijk-Deij, A. Dainotti, K. Claffy, and A. Sperotto



**Homeland  
Security**



**UNIVERSITY  
OF TWENTE.**

## Introduction

- Paper Accepted at WTMC (Workshop on Traffic Measurements for Cybersecurity) 2020, Genova, Italy.
- [https://www.caida.org/publications/papers/2020/forgotten\\_side\\_dns/](https://www.caida.org/publications/papers/2020/forgotten_side_dns/)
- Part of NWO-DHS MADDVIPR Project – A Joint Collaboration between University of Twente and CAIDA

# Introduction

- DNS zone administration is a complex task involving manual work and several entities.
- Within the context of the DNS, we typically identify three types of stakeholders: registries, registrars, and registrants.
- Due to the complexity of managing DNS information, misconfiguration and errors can occur, with an impact on the overall security and reachability of the DNS.
- In this work, we present an analysis on a specific misconfiguration, defined as orphan records.

# Glue Records

- A top-level domain (TLD) is a special type of zone that typically only has one task: to delegate authority for second-level domains.
- The delegation uses NS records that identify the name server for a domain.
- If the NS record for a domain points to a record that is inside the domain (called in-bailiwick), that name is included in the zone as a glue record to enable the resolution process to continue.
- Glue records are usually the only A/AAAA records admitted to TLD zone files.

# A Well-Formed Zone

- In normal operation, glue records are used only to break the circular dependency in the process of the resolution.

```
good.com      86400 IN NS ns1.good.com
ns1.good.com  3600 IN  A 1.2.3.5
```

# DOMAIN LIFECYCLE



Dad, where  
are you?



## Orphan Records?

- An orphan record is a former glue record for which the related domain no longer exists in the zone (the delegation has been removed)
- These records are supposed to be removed after a delegation is removed or changed.


# Orphan Records: A Decade Later

- This work reproduces and extends the analysis performed by Kalafut et al. in 2010.
- *A decade after the original analysis, what does the orphan records phenomenon look like?*
- We characterize the orphan records through a dataset of ~2K TLDs and over a wider time window of 25 months.
- We also discover a related type of misconfiguration, which we call "Abandoned Records".



# Abandoned Records?

- We define abandoned record as a former glue record for which the related domain still exists in the zone, but the delegation no longer requires that glue record.
- Abandoned records do not show up in the DNS resolution.
- They are returned in the additional section only when they are referred by a delegation of other domains of the zone.



example.com	86400	IN	NS	ns.external.org
ns1.example.com	3600	IN	A	1.2.3.4
ns1.expired1.com	3600	IN	A	3.2.5.4
ns1.expired2.com	3600	IN	A	8.4.5.6
active.com	86400	IN	NS	ns1.expired2.com
good.com	86400	IN	NS	ns1.good.com
ns1.good.com	3600	IN	A	1.2.3.5

TABLE 1: Example .com Zone File

■ *Orphan Records*

■ *Abandoned Records*

# A QUICK RECAP

# Results

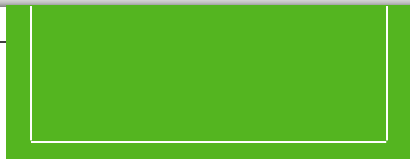
- We found 88K orphan and IM abandoned records (daily average).
- The .info zone is responsible for ~44K orphans and shows the highest percentage of orphans over the total number of records in the zone.
- We found many orphans also in .org and new gTLDs.
- Abandoned records are most prevalent in .com and .org.

# Orphan and Abandoned Records Lifetime

- For Orphan records, we found that ~19% survive just one day.
- However ~4% (21640) of all the orphan records we found persisted for more than 760 days.
- These 21640 orphans represent the hard core of orphan records in zone files, proving that this is a long-term misconfiguration.
- Same considerations apply to abandoned records, with the exception that, on average, abandoned survive longer.

# What's the Harm?

- Orphan records are working **A** DNS records that can still be in use.
- They can be referred by other domains as **NS** records (in case of legitimate usage) or they can host malicious content (e.g. malicious website).
- Registries should remove these records, or at least forbid the registration of the parent domain.
- An attacker, indeed, could potentially register the parent domain and hijack the orphan record traffic.
- All the domains that point to that orphan as **NS** will then be Hijacked!



Orphan records											
Ref by	ru	org	asia	CZDS	se	name	mobi	us	ca	info	Total
aero	0	0	0	0	0	0	0	36	4	0	40
asia	0	0	26	23	0	0	0	0	0	11	60
biz	0	17	12	93	4	0	2	62	101	96	387
ca	0	16	0	5	0	0	0	2	10320	24	10367
com	0	1337	41	276	34	2	19	3923	6223	1111	12966
CZDS	3	194	11	404	0	0	1	44	208	292	1157
fi	0	0	0	0	0	0	0	0	0	38	38
info	0	101	5	126	4	1	7	291	219	453	1207
mobi	0	8	4	99	0	0	30	7	149	5	302
name	0	0	0	28	2	68	0	0	9	0	107
net	0	277	10	139	19	0	3	1566	874	136	3024
nu	0	14	0	0	18	0	0	0	1	0	33
org	0	288	6	133	14	2	3	4695	1038	160	6339
ru	43	26	0	3	0	0	24	0	0	14	110
se	0	0	0	0	110	0	0	0	0	2	112
us	0	33	5	22	0	0	0	3287	67	20	3434
Total	46	2311	120	1351	205	73	89	13913	19213	2362	39683

DOMAIN  
POTENTIALLY  
HIJACKABLE

# Orphan DNSSEC signed records

- Normally, glue records are not signed, since the TLD is not authoritative for the domain.
- If the domain is deregistered, the orphan glue records are implicitly (and unintentionally) promoted by the registry to records that are part of the TLD zone.
- This means that in DNSSEC-signed zone, orphans will be DNSSEC-signed.
- Registries sign and provide warranty about the authenticity of junk records.

# Abandoned, not harmful?

- While the security risks related to orphan records are clear, Abandoned records, at first look, are instead not harmful. They can not be exploited by registering the domain, because the domain exists.
- However, we discover a relationship between orphan and abandoned.
  - ~28% of orphan records were previously abandoned records.
  - ~2% of orphans become abandoned ⇒ Evidence of registered Orphans!



# Origin of Orphan records

- ~54% (30K) orphan records had no associated WHOIS information, meaning they were potentially available for registration.
- Most of the orphan and abandoned records for which we found WHOIS information were registered with GoDaddy and Namecheap.
- Orphan and abandoned records come to exist due to how EPP (Extensible Provisioning Protocol) communication between registry and registrar takes place.

# EPP and Orphan records

- EPP defines three main object types: domains (NS records), contacts, and hosts (the glue records).
- In EPP, the creation of host and domain resources are two independent operations.
- The EPP specification does not define who, between registry and registrar, is responsible to clean up glue records if they are no longer required.
- This leads to the creation of orphan records.

# Registry, Registrar: Take action

- In 2010, Verisign cleans up .com and .net zone file removing all the orphan records.
- Still, after 10 years, some TLDs are been affected by the orphan records misconfiguration.
- The problem was also addressed by ICANN Security and Stability Committee in 2010 (SAC 048).
- We advise TLDs to revise their EPP policies and implementations and to clean up their zone.

# Afilias Case

- We reached out to Afilias, which is responsible for the technical management of .info, .org and many other TLDs affected by the orphan's misconfiguration.
- They are in the process of taking action for removing orphan records from their zone.
- <http://www.circleid.com/posts/20200811-afilias-to-protect-tlds-against-potential-orphan-glue-exploits>

# Cooperate with us

- We would collect data from the registries' perspective on the number of queries received by orphans.
- We can help you in the detection and removal of orphan and abandoned records from your zones.
- We can help us to expand our coverage of ccTLDs DNS measurement under the OpenINTEL project. <https://openintel.nl/>

# Conclusion

- Orphan records revealed to be a long term misconfiguration of the DNS TLD zones.
- After a decade from the original study, orphan records are still there.
- We extended scope and the scale of previous work and also discovered "abandoned records" that can be considered as a ringing bell of the creation of orphans.
- We invite all the registry to act to prevent the creation of these records.

QUESTIONS?

