Summarizing DNS & Security Academic Conference Papers in 2025

Chaoyi Lu

June 2026 @ ICANN 86

https://chaoyi.lu

Collecting papers

Academic conferences surveyed: 12

Security, tier-1

IEEE Symposium on Security and Privacy ***(IEEE S&P)***

NDSS *Network and Distributed System Security Symposium* ***(NDSS)***

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION ***USENIX*** *Security Symposium*

acm SIGSAC *ACM Conference on Computer and Communications Security* ***(CCS)***

Security, tier-2

Annual Computer Security Applications Conference ***(ACSAC)***

RAID *International Symposium on Research in Attacks, Intrusions and Defenses* ***(RAID)***

IEEE/IFIP International Conference on Dependable Systems and Networks ***(DSN)***

ESORICS *European Symposium on Research in Computer Security* ***(ESORICS)***

Networks, tier-1

ACM ***SIGCOMM***

ACM Internet Measurement Conference ***(IMC)***

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

USENIX Symposium on Networked Systems Design and Implementation ***(NSDI)***

THE WEB CONFERENCE ACM

The Web Conference ***(WWW)***

Having fun with numbers

20 papers about DNS/Security

2024: 23 papers

20 papers about DNS/Security

Measurement of DNS servicing and security (x7)

About DNS abuse (x3)

- [NDSS] The Guardians of Name Street: Studying the **Defensive Registration** Practices of the Fortune 500
- [CCS] Exposing the Roots of DNS Abuse: A Data-Driven Analysis of Key Factors Behind **Phishing Domain** Registrations
- [RAID] From Concealment to Exposure: Understanding the Lifecycle and Infrastructure of **APT Domains**

About DNSSEC (x2)

- [IMC] Decoding DNSSEC Errors at Scale: An Automated DNSSEC **Error Resolution** Framework using Insights from DNSViz Logs
- [IMC] Measuring the deployment of **DNSSEC Bootstrapping** Using Authenticated Signals

About DNS servicing (x1)

- [IMC] How I learned to stop worrying and love IPv6: Measuring the Internet Readiness for **DNS over IPv6**

Using DNS data for other measurements (x1)

- [USENIX Sec] Lost in the Mists of Time: Expirations in DNS Footprints of Mobile Apps

20 papers about DNS/Security

New DNS security threats / attack vectors (x6)

Amplification and DoS (x3)

- [USENIX Sec] Your Shield is My Sword: A Persistent Denial-of-Service Attack via the Reuse of Unvalidated Caches in **DNSSEC Validation**
- [CCS] Forward to Hell? On the Potentials of Misusing **Transparent DNS Forwarders** in Reflective Amplification Attacks
- [CCS] SocketFilled: A New **Cross Layer DoS Attack** Against UDP-based Services on Linux

Cache poisoning and snooping (x2)

- [USENIX Sec] DNS FLaRE: A Flush-Reload Attack on **DNS Forwarders**
- [CCS] RebirthDay Attack: Reviving DNS Cache Poisoning with the **Birthday Paradox**

Domain registry operations (x1)

- [USENIX Sec] Misty Registry: An Empirical Study of Flawed **Domain Registry Operation**

20 papers about DNS/Security

Detection of DNS abuse; DNS-related solutions (x7)

Detecting DNS abuse and threats (x3)

- [SP] MANTIS: Detection of **Zero-Day Malicious Domains** Leveraging Low Reputed Hosting Infrastructure
- [USENIX Sec] POPS: From History to Mitigation of **DNS Cache Poisoning Attacks**
- [SP] Resolution Without Dissent: In-Path Per-Query Sanitization to Defeat **Surreptitious Communication Over DNS**

Solutions about the DNS (x2)

- [SIGCOMM] DNSLogzip: A Novel Approach to Fast and **High-Ratio Compression for DNS Logs**
- [ESORICS] Formal Security Analysis of **DNSSEC+**

Solutions leveraging DNS (x2)

- [USENIX Sec] Transparent Attested DNS for **Confidential Computing Services**
- [SIGCOMM] Reliable and Decentralized **Certificate Revocation** via DNS: The Case for RevDNS

Measurement:
Obtaining data about the DNS

How's DNS Abuse Going?

[CCS] Exposing the Roots of DNS Abuse: A Data-Driven Analysis of Key Factors Behind Phishing Domain Registrations

Authors: Yevheniya Nosyk, Maciej Korczyński, Carlos Gañán, Sourena Maroofi, Jan Bayer, Zul Odgerel, Samaneh Tajalizadehkhoob, Andrzej Duda

Cybercriminals continually register new domain names for exploitation

- High concentration of malicious registrations in a handful of ***registrars*** and ***TLDs*** ➔ ***Why?***

A systematic analysis of factors driving abuse – how are they influencing malicious registrations?

Category	Feature	Malicious registration	Category	Feature	Malicious registration
Price	$1 ⬇️	+49%	**Registrar API**	Support registration via API	+401%
Free bundled services	Free web hosting	+88%	**Payment methods**	Accept cryptocurrency	+30%
	Free DNS	+205%		Accept bank transfers	-74%
	Free certificates	-81%	**Restrictions**	Verify email/mobile	-70%

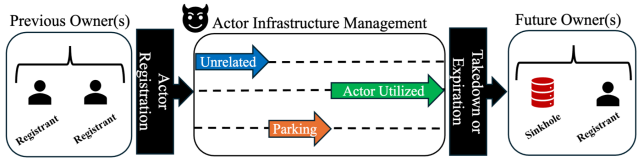
How's DNS Abuse Going?

[RAID] From Concealment to Exposure: Understanding the Lifecycle and Infrastructure of APT Domains

Authors: Athanasios Avgetidis, Aaron Faulkenberry, Vinny Adjibi, Tillson Galloway, Panagiotis Kintis, Omar Alrawi, Zane Ma, Fabian Monrose, Angelos D. Keromytis, Roberto Perdisci, Manos Antonakakis

Challenges in detecting APT domains

- Relation between infrastructure and APT actors is ***transitory***
- Attacks persist for years, allowing ***dynamic IP changes***



APT infrastructure identification

- 405 APT groups from OSINT (***31k*** domain IoCs)
- Get IPs from ***historical DNS logs***
- Feature extraction & classification - identifies ***3x more*** historically utilized IP infrastructure than threat reports

#f	Feature	Class	#f	Feature	Class
f_1	Detection and IP Fseen Delta	Temporal	f_{12}	IP Reputation	OSINT
f_2	Detection and IP Lseen Delta	Temporal	f_{13}	Number of Malicious Votes	OSINT
f_3	IP Lifetime	Temporal	f_{14}	Number of Harmless Votes	OSINT
f_4	Number of Historic Domains on IP	Infra.	f_{15}	Number of Malicious Analyses	OSINT
f_5	Mean Concurrent Domains on IP	Infra.	f_{16}	Number of Suspicious Analyses	OSINT
f_6	Median Concurrent Domains on IP	Infra.	f_{17}	Number of Undetected Analyses	OSINT
f_7	Number of IP Communicating Files	Infra.	f_{18}	Number of Harmless Analyses	OSINT
f_8	IP is Known Parking	OSINT	f_{19}	Num. of Domain Communicating Files	Domain
f_9	Nameserver is Known Parking	OSINT	f_{20}	Num. of Files Downloaded From Domain	Domain
f_{10}	IP is Known Sinkhole	OSINT	f_{21}	Number of Domain Subdomains	Domain
f_{11}	Nameserver is Known Sinkhole	OSINT	f_{22}	Number of Domain Certificates	Domain

Analysis results of APT infrastructure

- Most APT actors ***re-utilize*** a part (~26%) of infrastructure
- 73% of actor-utilized IPs ***no longer point to domains after APT disclosure*** – importance of historical data
- A significant portion of parking and sinkhole IPs are ***mistakenly flagged as malicious***
- APT actors first provision infrastructure on their domains ***~300+ days*** before the attack is reported; organizations need to keep their network logs for ***~2 years***

How's DNS Abuse Going?

[NDSS] The Guardians of Name Street: Studying the Defensive Registration Practices of the Fortune 500

Authors: Boladji Vinny Adjibi, Athanasios Avgetidis, Manos Antonakakis, Michael Bailey, Fabian Monrose

Defensive registrations for protecting intellectual property or trademark

Original	TLD-squatting	Typo-squatting		Bitsquatting	Homophones	Homographs
icann.org	icann.info icann.com	icanm.org ican.org	icannn.org iacnn.org	8cann.org ifann.org	ikann.org icanne.org	1cann.org lcann.org

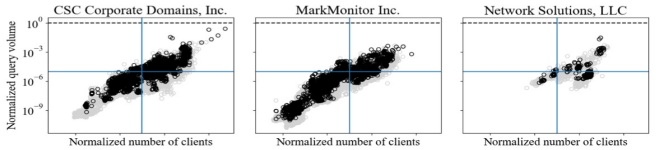
Level of engagement is still low

- Found **19K** defensive registrations
- Over 200 companies registered only **<10** domains
- **TLD squatting** accounts for ~40%

Top 10 registrants	
Amazon	709 (0.33%)
Arrow Electronics	473 (0.25%)
Microsoft	424 (0.13%)
Cigna	362 (0.08%)
American Express	305 (0.06%)
Alphabet	304 (0.13%)
Bank of America	303 (0.07%)
Elevance Health	297 (0.07%)

Most use online brand protection (OBP)

- Often miss domains with **significant traffic**
- Recommends using **passive DNS data** to identify heavily queried available domains



The old and new about DNSSEC

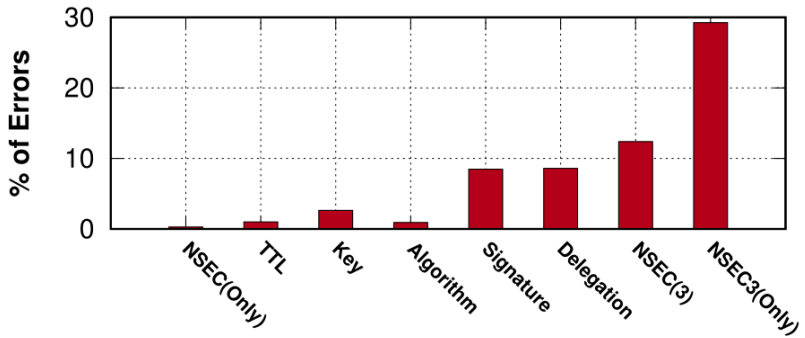
[IMC] Decoding DNSSEC Errors at Scale: An Automated DNSSEC Error Resolution Framework using Insights from DNSViz Logs

Authors: Md. Ishtiaq Ashiq, Olivier Hureau, Casey Deccio, Tijay Chung

DNSSEC misconfiguration and errors: missing records, wrong signature, and beyond

- Signed domains can become effectively **unresolvable** as a result
- **Real-world outages** show serious outcomes misconfigurations can bring

Which misconfigurations are often?



NSEC(3) errors are the most prominent

- ***Non-zero NSEC3 iteration count*** – an outstanding issue
- Missing non-existence proof

Delegation & signature errors

- Invalid KSK algorithm in DS record
- Signature missing / expired

Key inconsistencies

- Different DNSKEY across different authoritative servers

The old and new about DNSSEC

[IMC] Measuring the Deployment of DNSSEC Bootstrapping Using Authenticated Signals

Authors: Q Misell, Florian Steurer, Johannes Zirngibl, Anja Feldmann, Tobias Fiebig

Current solutions for automating DNSSEC configuration and key rollovers

- CDS/CDNSKEY RRs – allows automatic rollover of DS records in the parent
- Authenticated bootstrapping – enables automatic DNSSEC configuration on domain names

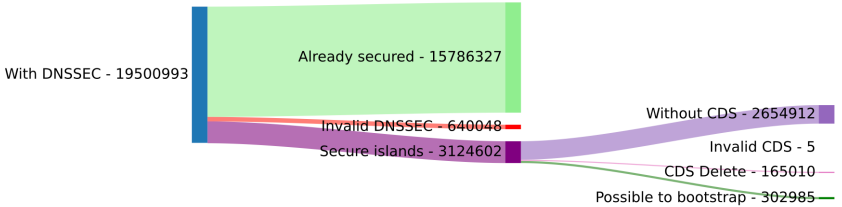
DNSSEC and CDS deployment

- Only **5.5%** of all scanned zones are correctly signed
- CDS is gaining primary support from ***smaller operators***, especially ***Swiss*** – likely due to financial incentives

#	DNS Operator	Dom. w. CDS Num	%	#	DNS Operator	Dom. w. CDS Num	%
1	Google Domains	4 624 357	46.6	11	Gandi	34 486	3.6
2	WIX	1 326 336	18.1	12	Webland	26 416	76.3
3	Cloudflare	1 232 531	4.4	13	green.ch	24 674	16.8
4	Simply.com	218 590	96.8	14	WebHouse	18 766	60.0
5	GoDaddy	111 078	0.2	15	Váš Hosting	13 066	98.3
6	cyon	60 981	48.1	16	HostFactory	12 897	68.4
7	Gransy	54 690	98.9	17	INWX	11 303	7.8
8	METANET	54 522	70.5	18	OpenProvider	10 312	79.5
9	Porkbun	34 989	3.2	19	AWARDIC	8 898	99.9
10	netim	34 586	40.9	20	3DNS	8 112	75.6

Authenticated bootstrapping (AB) potential

- AB is ***not*** widely implemented, but is implemented correctly in almost all cases it is
- ***Low DNSSEC deployment*** remains a barrier for further DNSSEC



Getting ready for IPv6?

[IMC] How I learned to stop worrying and love IPv6: Measuring the Internet Readiness for DNS over IPv6

Authors: Tobias Fiebig, Anja Feldmann

IPv6 adoption in DNS is not universal – is it time to require IPv6 for DNS?

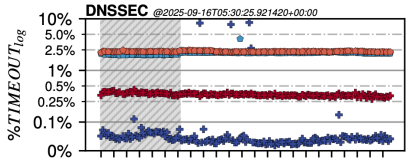
- RFC 3901 (Best current practice since 2004): rules out IPv6-only DNS servers; **IPv6 is optional**
- Recent study: **<60%** of all DNS zones support IPv6-only resolution

Research question: Is DNS resolution impaired by IPv6?

- Dataset: daily resolution result of Top 10M domains *(under different MTU/PMTUD scenarios)*

Resolution errors

- DNS timeout: IPv6 > IPv4, due to IPv6 misconfigurations
- SERVFAIL: lower for DNSSEC zones



IPv4 vs IPv6 fragments

- Slight difference in the share of fragmentation
- IPv4/IPv6 fragmentation are ***comparably functional***
- The expectation that in IPv6 DNS resolution there are notably fewer fragments ***does not hold***

Summary & recommendations

- ***No indications of negative impact*** of using IPv6 for DNS resolution under broken MTU/PMTUD scenarios
- "It is time to recommend that IPv6 **SHOULD** be used in the DNS"

DNS threats:
New attack vectors & methods

DoS: DNSSEC Debugging

[USENIX Security] Your Shield is My Sword: A Persistent Denial-of-Service Attack via the Reuse of Unvalidated Caches in DNSSEC Validation

Authors: Shuhan Zhang, Shuai Wang, Li Chen, Dan Li, Baojun Liu

CD **bit enables troubleshooting for DNSSEC**

- CD=1 returns **unvalidated** data and signatures
- Resolvers are caching and **reusing** this data (🤯)

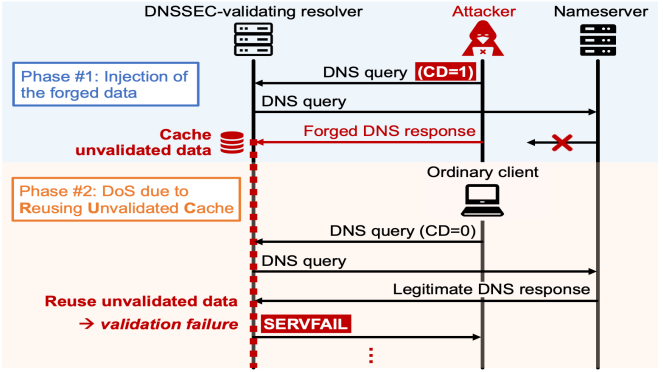
Ordinary query: CD=0 (default)	Troubleshooting query: CD=1
Resolver: validation fails	***Resolver: no validation***
`DNS response: SERVFAIL` `(no answer)`	`DNS response: NOERROR` `foo.com DNSKEY tx8EZ…` `foo.com RRSIG DNSKEY (expired)`
🤔 Where is the problem??	😉 I know! The RRSIG of foo.com's DNSKEY has expired.

Reuse Unvalidated Caches (RUC) for DoS attacks

- Attacker sends CD=1 queries to resolvers
- Attacker forge DNS response – **unvalidated and cached**
- Ordinary queries for victim domain fail (**SERVFAIL**) due to RUC

Evaluation & mitigation

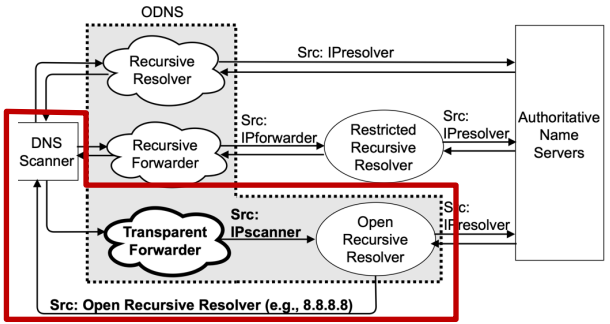
- 5 DNS software, 28 public DNS services, 65% open resolvers
- Calls for tight restrictions for reusing unvalidated data



DoS: Amplification

[CCS] Forward to Hell? On the Potentials of Misusing Transparent DNS Forwarders in Reflective Amplification Attacks

Authors: Maynard Koch, Florian Dolzmann, Thomas C. Schmidt, Matthias Wählisch

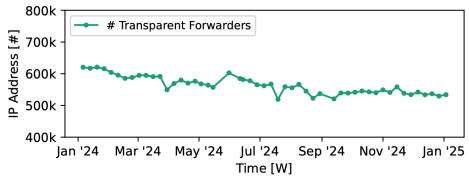


Transparent forwarders: forward queries *w/o* rewriting source IP

- Account for **30%** of the open DNS infrastructure
- **Not receiving or caching** responses from upstream resolvers
- **Not discoverable** by scanning campaigns (e.g., Censys)

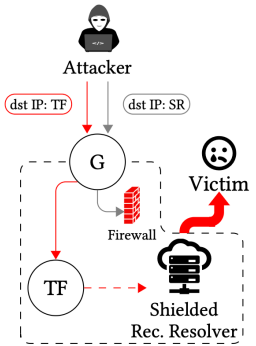
530K transparent forwarders found

- Most (fingerprint-able ones) are routers
- Creates attack traffic more efficiently because they don't process responses



Transparent forwarders can be exploited to access "shielded resolvers" and for more powerful amplification

- Shielded resolvers: behind firewall/gateway ➔ **looser rate limits**
- Some still support **ANY** ➔ **can be triggered via transparent forwarder**



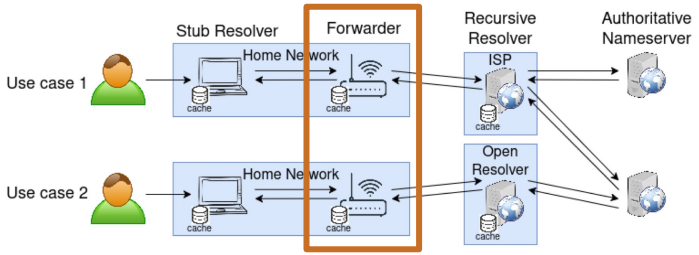
Cache Snooping

[USENIX Security] DNS FLaRE: A Flush-Reload Attack on DNS Forwarders

Authors: Gilad Moav, Yehuda Afek, Anat Bremler-Barr, Amit Klein

DNS forwarders are very close to users

- Commonly found in home routers and on Linux systems
- They are often the first devices queried by users



DNS FLaRE: side-channel that determines whether a user has accessed a website

- Whether a user has accessed a website ↔ whether the website domain presents in forwarder cache

- Step 1: flush and clear the forwarder cache
- Step 2: wait for a given time interval
- Step 3: infer cache by measuring response time

Browser / OS	Chromium	Safari	Firefox
Windows	HTTP, DNS ✓	N/A	✗
Mac OS	HTTP, DNS ✓	✗	✗
Linux	HTTP ✓	N/A	HTTP ✓
Linux	HTTP ✓	N/A	HTTP ✓

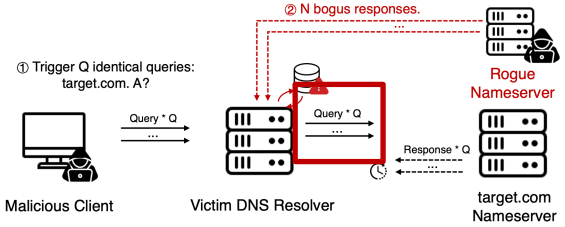
Reviving the Old Cache Poisoning

[CCS] RebirthDay Attack: Reviving DNS Cache Poisoning with the Birthday Paradox

Authors: Xiang Li, Mingming Zhang, Zuyao Xu, Fasheng Miao, Yuqi Qiu, Baojun Liu, Jia Zhang, Xiaofeng Zheng, Haixin Duan, Zheli Liu, Yunhai Zhang, Dunqiu Fan

The DNS Birthday cache poisoning attack (2002)

- On repeated queries, resolver issues multiple queries to authoritative
- Attacker only needs to **hit the TxID in one of them** (*birthday paradox!*)
- Mitigated by **query aggregation**: no repeat for the same `<qname,qtype>`



An ECS implementation bypassing query aggregation

- Caching and query aggregation based on `<qname,qtype,subnet>`
- Affects **6** types of recursive and forwarder DNS software
- Birthday Paradox says success rate reaches 99.6% after 1,800 rounds

Software	Avg. Round Taken	Avg. Time Taken	Success Rate
Unbound	263	593s	20/20
PowerDNS Recursor	328	237s	20/20
CoreDNS	20	245s	20/20

Testing on public/open DNS servers

- 45 public DNS services: **14** vulnerable
- Open DNS resolvers: ~**15%** vulnerable

Mitigation

- Resolvers verify ECS consistency
- Cache poisoning defenses: 0x20 encoding, DNSSEC, etc.

Special Cases Found in TLD Zone Files

[USENIX Security] Misty Registry: An Empirical Study of Flawed Domain Registry Operation

Authors: Mingming Zhang, Yunyi Zhang, Baojun Liu, Haixin Duan, Min Zhang, Fan Shi, Chengxi Xu

Domain lifecycle - from creation, management, to deletion - is operated with the EPP protocol

- EPP implementations and operational practices can vary between registries

Finds several vulnerable EPP implementations that result in domain takeover:

Redundant domain creation

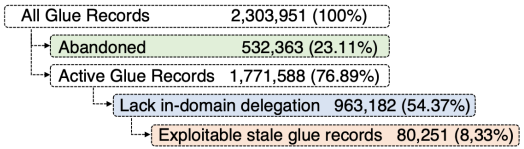
- For IDN scripts with variants, registries can create them automatically

测试.example *(simplified Chinese)*

測試.example *(traditional Chinese)*

Stale glue records

- Registries indiscriminately add all DNS host objects into zone files



"Relic" domains

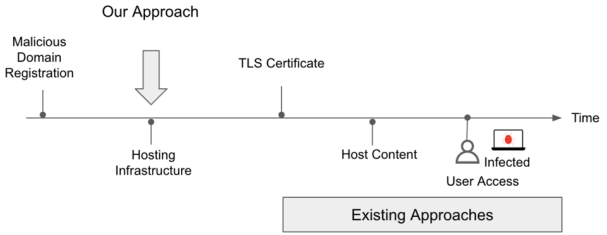
- EPP available, but delegation in zone files remains
- Attackers can control the domains **permanantly** without pay – abuse for illicit activities

Detection & solution

Detecting/Mitigating DNS Threats & Abuse

[SP] MANTIS: Detection of Zero-Day Malicious Domains Leveraging Low Reputed Hosting Infrastructure

Authors: Fatih Deniz, Mohamed Nabeel, Ting Yu, Issa Khalil



How to detect *short-lived, disposable* domains for attacks?

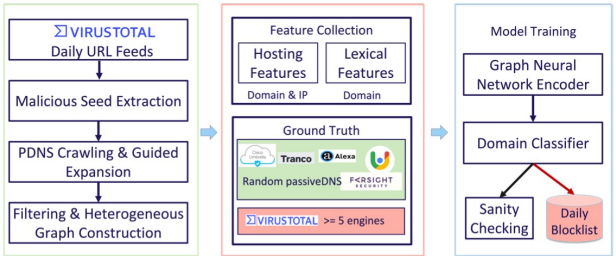
- Existing detection mechanisms are either too ***late*** or easily ***evaded***

Observation: attackers often reuse hosting infrastructure to launch their attacks

- ***Passive DNS*** data can be utilized to quickly find domains hosting on the same IPs
- Domains using the same IPs as attack domains can be correlated using a graph
- ***Graph Neural Networks (GNN)*** can be trained to classify malicious domains

Features used for domain classification

- Lexical: suspicious keywords, length, and specific character patterns, etc.
- Domain hosting: access frequency, presence of multiple IPs and NSes, etc.
- IP features: # apex domains, duration of appearance in PDNS records, etc.



Detecting/Mitigating DNS Threats & Abuse

[USENIX Security] POPS: From History to Mitigation of DNS Cache Poisoning Attacks

Authors: Yehuda Afek, Harel Berger, Anat Bremler-Barr

Taxonomy of DNS cache poisoning attacks: bullseye and statistical

- Bullseye: attacker only generates **1** packet Statistical: attacker generates **multiple** packets

Paper	Type	#Pkts	POPS
Schuba et al. [12] 1993	-	1	-
V. Sacramento [41] 2002	S	2^{16}	Rℓ1
Klein, Amit [42] 2007	S	>100	Rℓ1
Kaminsky, Dan [13] 2008	S	$200 \cdot q$	Rℓ1
Herzberg et al. [18] 2012	S	2^{16}	Rℓ1
Herzberg et al. [18] 2012	S_{Frag}	2^{16}	Rℓ2
Herzberg et al. [43] 2013	B_{Frag}	1	Rℓ2
Herzberg et al. [44] 2013	S_{Frag}	$\sim 2^{11}$	Rℓ2
Herzberg et al. [45] 2013	S, S_{Frag}	2^{16}	Rℓ1
Zheng et al. [46] 2020	B_{Frag}	1	Rℓ2
Man et al. [47] 2020	S	2^{16}	Rℓ1
Dai et al. [48] 2021	S_{Frag}	64	Rℓ1
Klein et al. [49] 2021	S	2^{16}	Rℓ1
Jeitner et al. [50] 2022	S	2^{16}	Rℓ1
Jeitner et al. [50] 2022	S	2^{16}	Rℓ1
Li et al. [17] 2023	S_{OoB}	2^{16}	Rℓ3
Heftring et al. [51] 2023	S_{Frag}	2^{16}	Rℓ2
Li et al. [22] 2024	S	2^{16}	Rℓ1

What techniques have major attacks used?

- Excessive guessing of TXID/Port (S)
- Fragmentation (Frag)
- Out-of-bailiwick data injection (OoB)

POPS: cache POisoning Prevention System as an IDS module

- Rℓ1: Alert when # of responses with only 1 field differs passes a threshold
- Rℓ2: Alert when seeing the first fragment of any DNS response
- Rℓ3: Alert when the QNAME is outside authority of the responding server

Mitigation after alert: move to TCP by setting TC=1

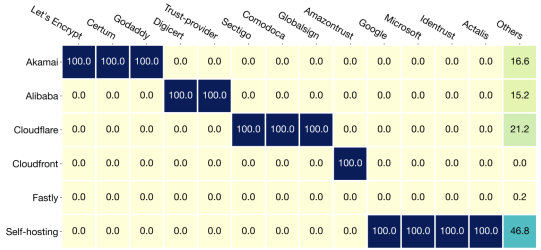
Solutions based on the DNS

[SIGCOMM] Reliable and Decentralized Certificate Revocation via DNS: The Case for RevDNS

Authors: Protick Bhowmick, Dave Levin, Taejoong Chung

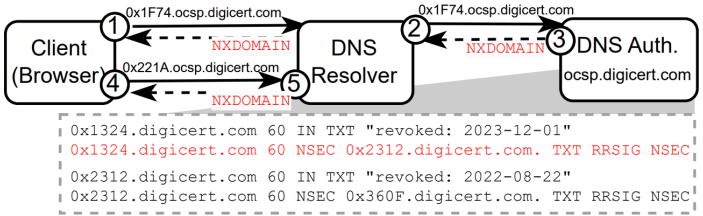
Online Certificate Status Protocol (OCSP): no longer sustainable

- Clients can query a ***CA's OCSP responder*** for certificate revocation status
- Often delegated to external operators, e.g., CDNs



RevDNS: a DNS-based revocation scheme that drops CDN dependence with real-time guarantee

- CA serves OCSP responses through their authoritative servers
- Revoked serial numbers live in ***DNSSEC-signed TXT records***
- NSEC proofs allow ***aggressive negative caching***
- Requires only ***the CA to deploy DNSSEC*** at its servers



Evaluation

- Zone size: extra 700MB for 1.4M revoked certs using ECDSA
- Caching efficiency: resolvers answer ***99.8%*** without bothering a CA

CA	# of Certs		OCSP Resp. (B)	Zone Size (MB)
	Total	Revoked		ECDSA 256
LetsEncrypt	612,524,633	655,216	503	345
Google	148,668,485	524,759	471	273
Godaddy	107,581,381	1,464,592	1,777	712
Digicert	87,409,159	1,171,433	471	608

Summarizing DNS & Security Academic Conference Papers in 2025

Chaoyi Lu

June 2026 @ ICANN 86

https://chaoyi.lu