



University
of Glasgow



Internet Protocols
Laboratory

Another Man's Treasure: Security and Privacy Risks of Junk DNS Queries

Elizabeth Boswell, Colin Perkins



What are junk queries?

- Not all DNS queries have a meaningful response
 - “What domain name resolves to 192.168.0.1?” → private address, so no meaningful answer
 - Sent by misconfigured software
- **Where do those junk queries go?**
 - Are answered by **AS112**

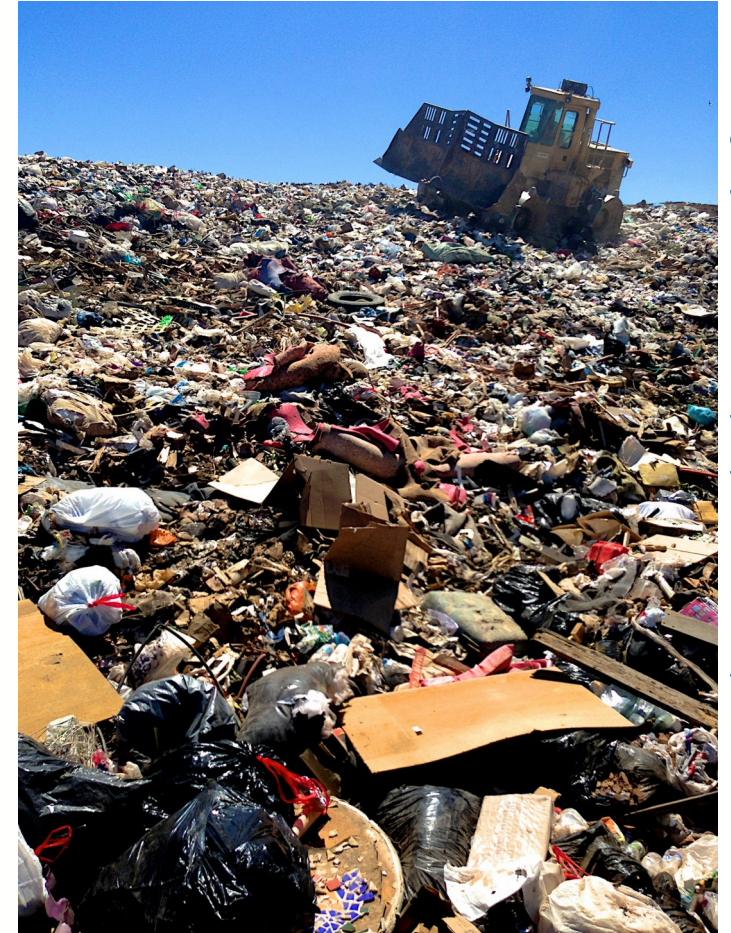
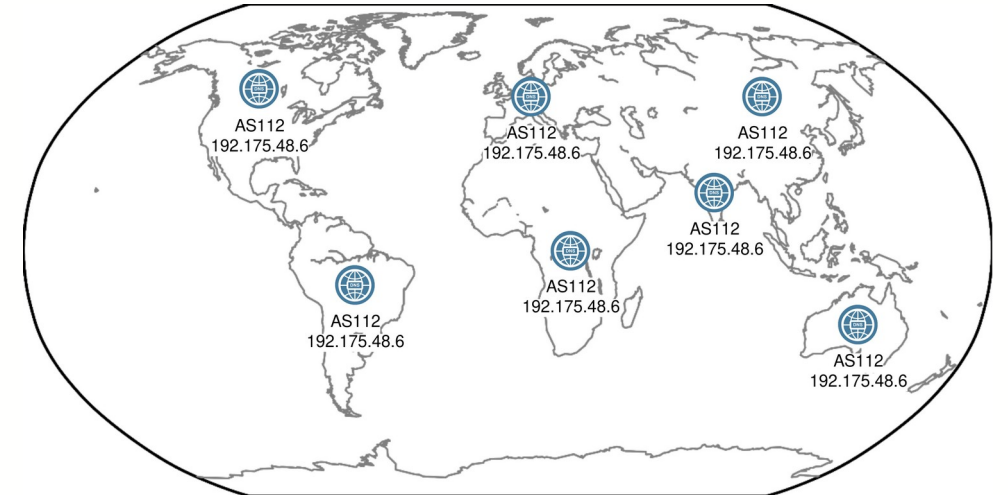


Image by Alan Levine, <https://pxhere.com/en/photo/213020>



What is AS112?

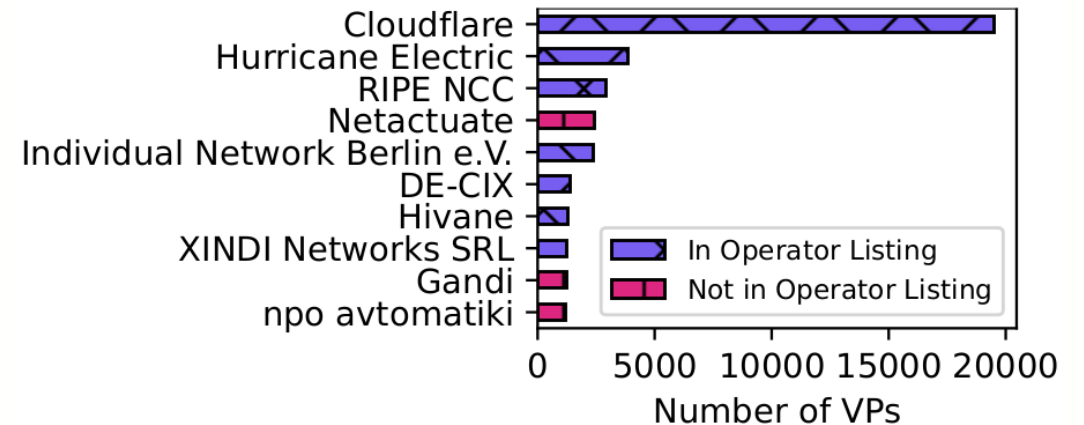
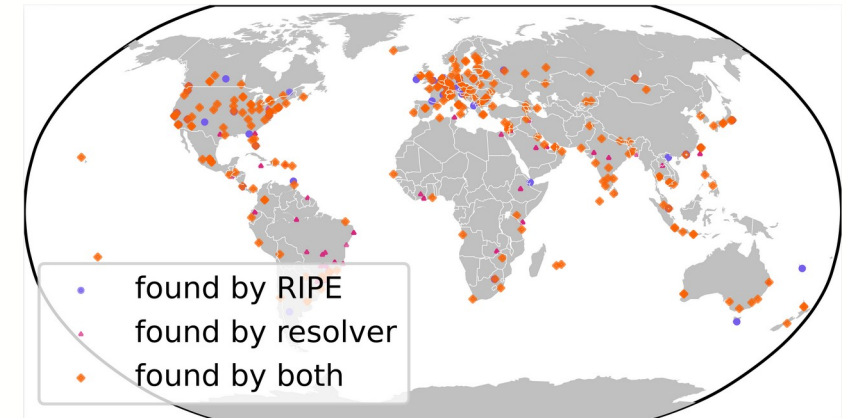
- **AS112:** anycast DNS deployment that captures junk queries
 - Diverts them from `.arpa/in-addr.arpa` nameservers
 - Nameserver for reverse mappings of RFC1918 private addresses and link-local IPv4 addresses, `home.arpa` and `service.arpa`
 - Reverse mapping: `203.0.113.23` → `23.113.0.203.in-addr.arpa`
 - Reverse DNS (rDNS) query: PTR query for the reverse mapping





Who runs AS112?

- Volunteer-run network
 - **Anyone** can add a site! Loosely coordinated by DNS-OARC
- We found **469 AS112 sites**, run by **97 operators**
 - **Cloudflare**: 216 sites





What queries go to AS112?

- AS112 is volunteer-run and uncoordinated
- Relies on **assumption** that AS112 traffic is harmless
- Our questions:
 - **What queries** are sent to AS112?
 - What could a **malicious operator** do with these queries?
- **Work in progress**, these are preliminary results



Our Dataset

- DNS-OARC Day in The Life 2025 data (8-10 April 2025)
 - **RIPE NCC site (Amsterdam):** ~542M requests, ~246K clients
 - **WIDE site (Osaka):** 2,252M requests, ~145K clients
 - **TIX site (Dar es Salaam):** ~4M requests, ~2K clients
 - In total: **2,799,058,875 requests, 393,183 clients**
- We found:
 - Reverse DNS queries
 - DNS Dynamic updates
 - Service Discovery queries
 - Lame-delegated queries



RFC1918 Reverse Mapping Queries

- Most requests are for **reverse mappings of RFC1918 private addresses**
 - **37.62%** PTR (rDNS) queries for RFC1918 addresses
 - **27.09%** are other queries for RFC1918 reverse mappings (excluding service queries)
 - **33.8%** other query types (e.g. A, SOA, NS)
 - **50.04%** of form `_.1.0.168.192.in-addr.arpa` (artefact of QNAME minimisation)
 - Queries for personal devices, **9.69%** contain substring “iphone”



DNS Dynamic Updates

- DNS Dynamic updates change contents of zone, e.g. used by DHCP
- Sent to AS112 if:
 - Host uses private IP address, updates its reverse mapping
 - Local DNS doesn't serve the reverse mapping zone
- Studied in 2003 and 2006 [1,2]
- **5.80%** of requests are dynamic updates
 - Plus 0.57% TKEY queries to secure updates
- Malicious AS112 operator could learn local network configuration, and track individual users

[1] [1] Broido, A., Nemeth, E. and claffy, kc 2003. Spectroscopy of private DNS update sources. Proceedings the Third IEEE Workshop on Internet Applications. WIAPP 2003 (Jun. 2003), 19–29.

[2] [1] Broido, A., Shang, H., Fomenkov, M., Hyun, Y. and Claffy, K.C. 2006. The Windows of Private DNS Updates. ACM SIGCOMM Computer Communication Review. 36, 3 (2006).



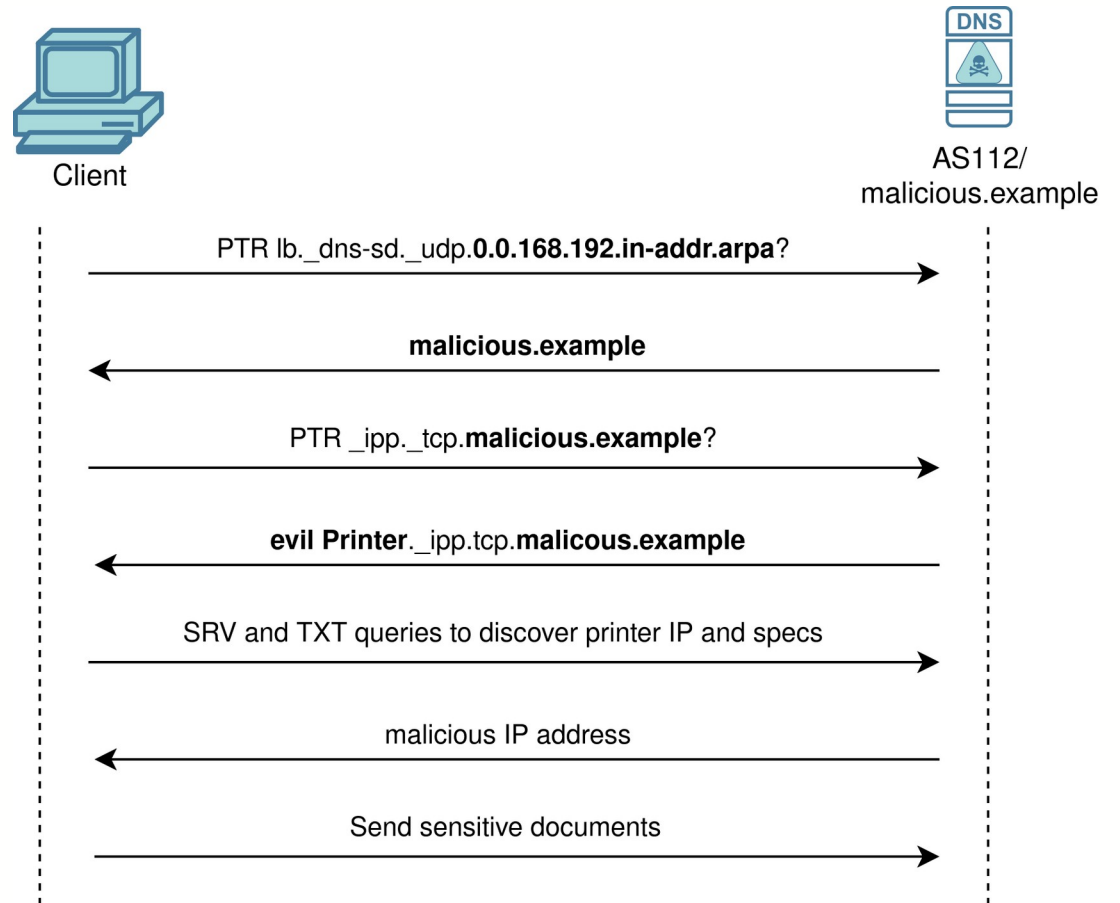
Service Discovery Queries and Service Queries (1/3)

- Interaction between AS112 and DNS-Based Service Discovery
 - Client discovers services by sending SRV/TXT queries of the form
 - `_<service name>._<protocol>.<local domain>` to the local DNS
 - e.g. `_ipp._udp.example.com`
 - Client has to first discover the `<local domain>`, through PTR queries of the form `lb._dns-sd._udp.<bootstrap domain>`
 - This bootstrap domain can be the reverse mapping of the local address
 - Queries go to AS112 if local address is RFC1918 private address, and local DNS does not serve this zone!



Service Discovery Queries and Service Queries (2/3)

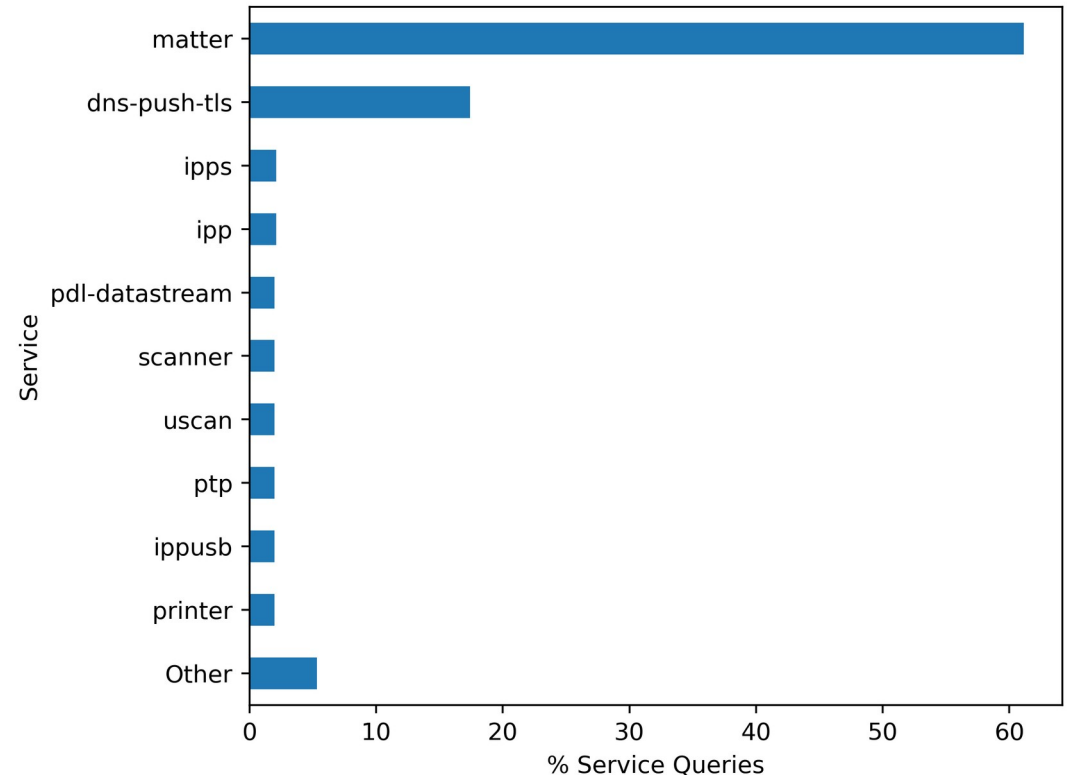
- **18.17%** of requests are Service Discovery Queries
- Malicious operator could misuse these queries to spoof the service
 - Return a bogus local domain, then return bogus IP address for the service
 - Fails if service is authenticated





Service Discovery Queries and Service Queries (3/3)

- **6.71%** of requests contain a service name
 - 320 services
 - “matter” was the most common (61.13%)
- Can be used to spoof local services if service is not authenticated





Lame-delegated Queries

- 0.35% of requests are for domains not delegated to AS112, with public TLDs
- Malicious operator could respond and **spoof the site**
 - 38,447 domains; 43% of queries are for strepsils[.]top (malware/phishing domain!)
- Why are these queries going to AS112?
 - Historical zone files and WHOIS for ~20k domains (from VirusTotal and DNS Coffee)
 - ~95% were **delegated to AS112** in the zone files (lame delegation)
 - Of these, ~75% use the same registrar (Hosting Concepts B.V.), 24.90% contain “bet|poker|gambl|win|slot|casino|kasino”
- Has anyone heard of this?



Conclusions

- ~2.8B requests from three AS112 sites
 - Found dynamic updates, service queries and lame delegated queries
- AS112 does not only receive “harmless” reverse DNS queries

Elizabeth Boswell, University of Glasgow

e.boswell.2@research.gla.ac.uk

<https://www.gla.ac.uk/pgrs/elizabethboswell/>