PoPS: Mitigation of DNS Cache Poisoning Attacks

Yehuda Afek[1]; Harel Berger[2]; Anat Bremler Barr[1]
[1]Tel Aviv University, [2]Ariel University

TEL AVIV UNIVERSITY

ARIEL UNIVERSITY

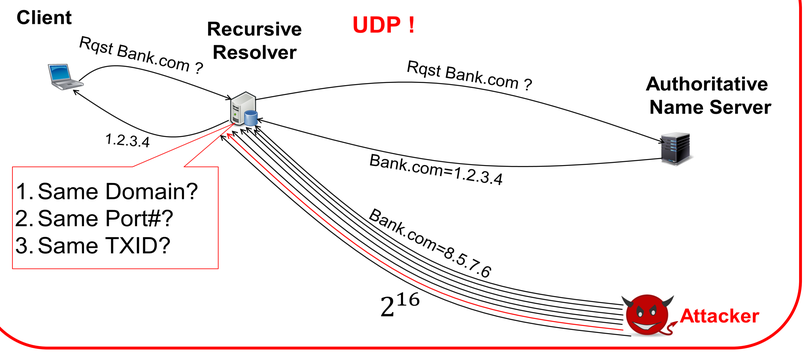
PoPS:
Detect and Mitigate <u>All</u> Statistical DNS Poisoning Attacks

- Blocks 99.993% of attacks with zero false negatives.
- Fast & efficient

DNS Cache Poisoning – Still a Big Problem

- Adversaries insert fake DNS records, redirecting users to malicious domains.
- Despite DNSSEC starting at 1997, adoption remains < 30% globally.
- Attacks use port and TXID inference, packet fragmentation, and improper validation of the bailiwick rule.
- Current industry practices mitigate vulnerabilities only after CVE disclosure.
- A critical need for a lightweight, easily deployable IDS/IPS.

Statistical DNS Cache Poisoning



Detection + Mitigation of *all* Statistical DNS Poisoning attacks

✓ We detect:
1. Standard Statistical attacks
2. Fragmentation attacks
3. Out-of-Bailiwick attacks

✗ We do not detect:
1. MITM poisoning attack
2. BGP hijacking attacks

Comparison to Other Tools (Suricata/Snort)

- 20%–50% of the time and only 5%–10% of the packets.
- Suricata/Snort produce 10×–20× more FN than PoPS.

SURICATA

PoPS

Detects and Mitigates with **zero FN** and **negligible FP**

Detection: **minimize FN** & **negligible FP, 0.0076%**
Mitigation: **zero FN** * & **zero FP**

==========

All together: **zero FN** & **negligible FP (0.0076%)**

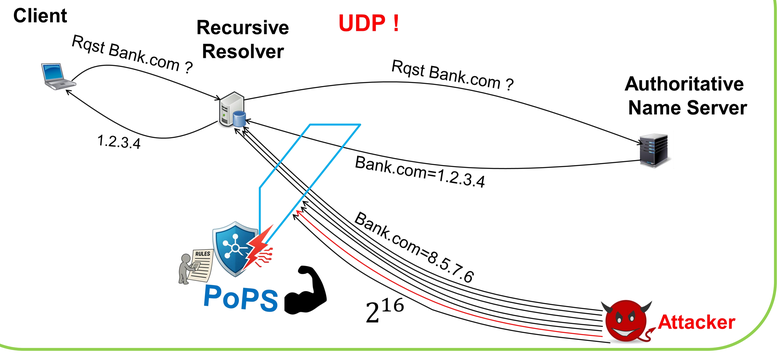
Approach

Two components:
1. ***Detection module*** - 3 simple rules targeting DNS cache poisoning attacks.
2. ***Mitigation module*** - uses the TCP fallback for handling suspicious traffic.

Detection Rules

1. Statistical attacks - detected >5 packets with same domain & varying port#/TXID, using a compact structure (~4 Kbit), flags an attack after 5 packets.
2. Fragmentation attacks - detected by spotting mis-association of fragments.
3. Out-of-bailiwick attacks - detected by glue RRs outside the target domain.

Detection Module



Proactive CVE Mitigation

- Blocks 14 DNS cache poisoning CVEs reported from 2002–2023.
- Protects major DNS software - BIND, Microsoft DNS, CoreDNS, etc.
- Minimizes patching needs for emerging CVEs.

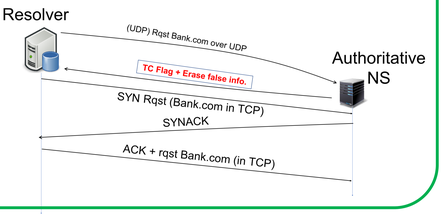
Mitigation Strategy

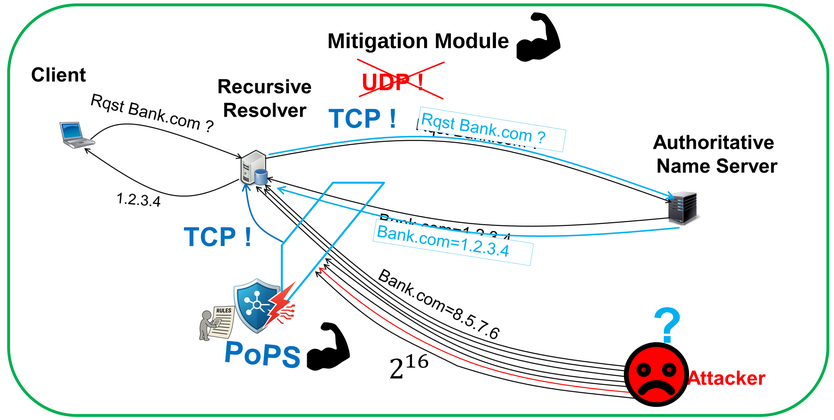
1. Sets the TC flag in DNS header -> TCP fallback, leveraging TCP's reliability.
2. Eliminate manipulated data from answer.
3. If fragment is obtained, drop it and follow the above.
4. If out-of-bailiwick packet, drop.

PoPS' Mitigation

On detecting a **suspicious response**:

1. Erase answer/auth/add records.
2. Set TC flag to true.
3. Forward packet to resolver.





Conclusions:

- PoPS detects attacks after 5 packets.
- 99.993% accuracy with 0 FN & ~0 FP.
- Fast & efficient compared to existing tools.
- Would have prevented all related CVEs.

For more information: