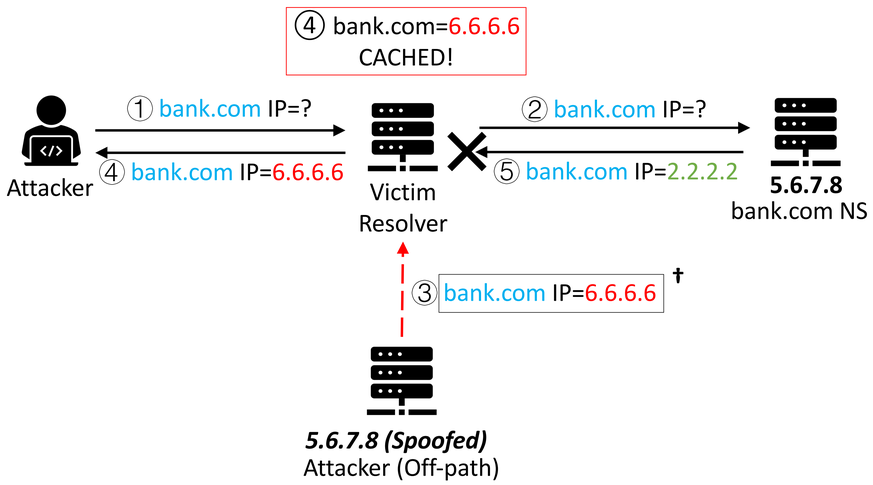
SADDNS: DNS is Side channel AttackeD!

Keyu Man, Xin'an Zhou, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan, Zhiyun Qian

I. Background: DNS Cache Poisoning Attack

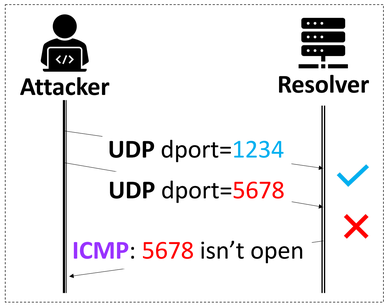


IMPACT: traffic hijacking->phishing & scams, fake certificate issuance, etc.

II. Challenges

† *

IP	**Src:** 5.6.7.8	**Dst:** *(resolver)*
UDP	**Src Port:** 53	
	Dst Port: Randomized (16 bit)	
DNS	**TxID:** Randomized (16 bit)	
	Question: bank.com A ?	
	Answer: bank.com A 6.6.6.6, TTL=**999**	



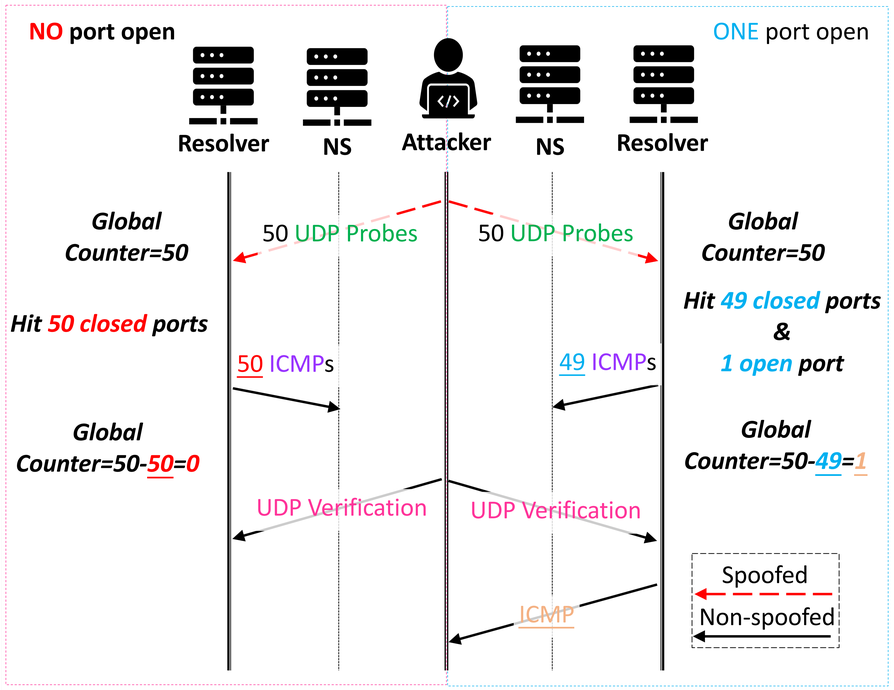
Challenges	Our Solutions
Guess two random fields *32-bit entropy*	Infer port # * before guessing TxID *16-bit entropy only on TxID*
Ephemeral (client) port opens to NS only *can't be easily inferred*	Infer with spoofed IP of NS
Response of spoofed packets *can't be received by the attacker*	(**III.**) Side Channel

Contributions

- We **revived** DNS cache poisoning attack (**dead** since 2008)!
- **All** popular OSes and DNS software are vulnerable
  - Linux, Windows, BIND, Unbound, dnsmasq…
- Affected DNS servers in the wild
  - 34% open resolvers
  - 12/14 popular public resolvers
    - *Google, Cloudflare, OpenDNS…*
- The first side-channel-based DNS cache poisoning attack.

III. Side Channel

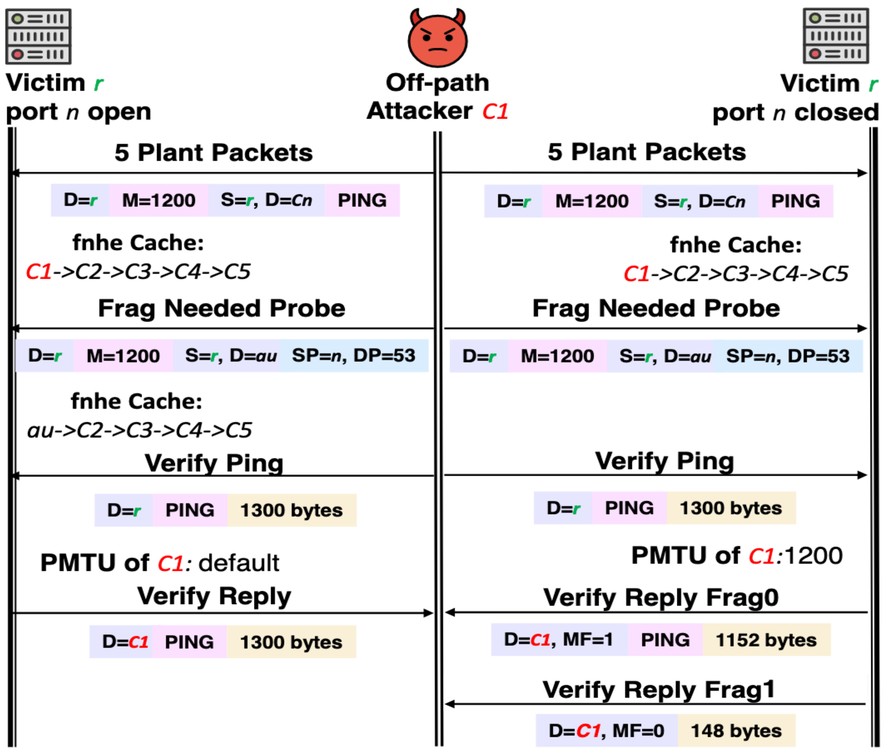
Revolution



UDP Probes: UDPs with guessed dst port #
UDP Verification: UDP destined to a known closed port (e.g., port 1)

- ICMP transmission reduce counter by 1
- Empty counter = no ICMP transmission

Resurrection



D=Destination IP, **S**=Source IP, **M**=PMTU, **SP**=Source Port, **DP**=Destination Port, **MF**=More Fragment, **Cn(C1-C5)**=Colliding IPs, **au**=Authoritative Name Server

- **F**orwarding Info Base **N**ext **H**op **E**xception Cache (**fnhe**) stores PMTU
- FILO queue

IV. Evaluation

Real world attacks:

Revolution		
Victim Resolver	Tsinghua	Commercial
# of backend servers	2	4
# of NS	2	1
Jitter	3ms	2ms
Delay	20ms	30ms
Loss	0.2%	0.6%
Success Time	15 mins	2.45 mins
Success Rate	5/5	1/1

Resurrection	
Victim Resolver	Controlled
# of backend servers	1
# of NS	2
Jitter	3ms
Delay	40ms
Loss	0.2%
Success Time	6.83 mins
Success Rate	20/20