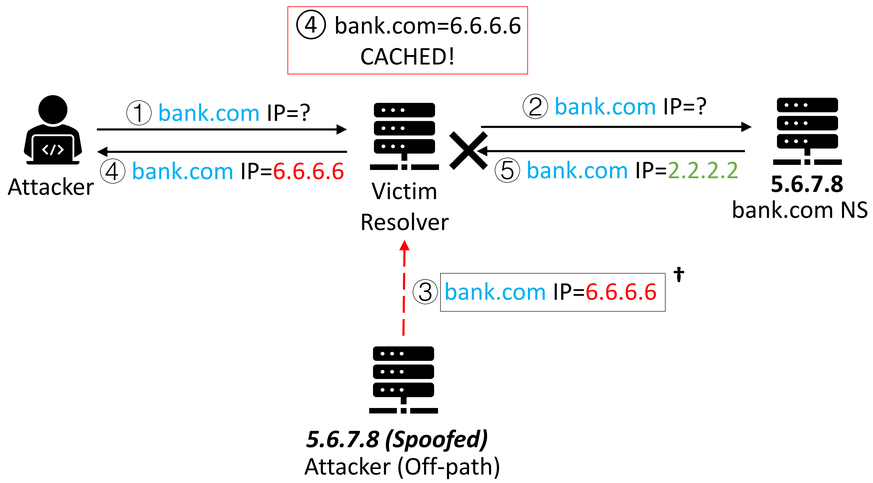
DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels

Keyu Man, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, Haixin Duan

I. Background: DNS Cache Poisoning Attack



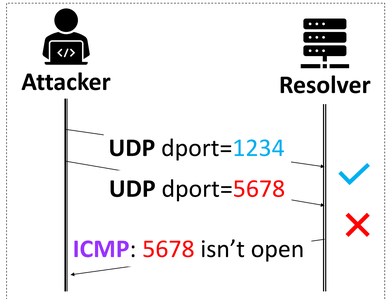
IMPACT: traffic hijacking->phishing & scamming, fake certificate issuance

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 guess TxID *16-bit entropy only on TxID*
Ephemeral (client) port opens to NS only *can't be inferred*	Infer with spoofed IP of NS
ICMP of spoofed packets *can't be received by the attacker*	(**III.**) Side Channel

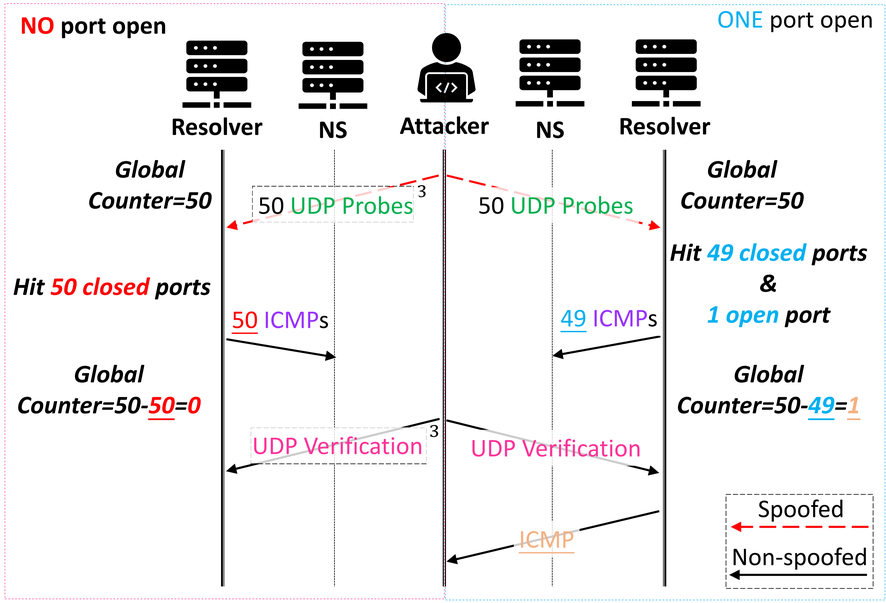
Contributions

- 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 attack is based on a **novel side channel** we discovered in the OS kernel

ICMP Global Rate Limit

- Limits global ICMP sending rate.
- A counter **shared** by all remote IPs.
  - Shared resource->Side channel arises!
- Send 1 ICMP->"counter--;".
- Can't send ICMP if counter=0.
  - Violates **non-interference** property.
- Linux: recover to max=50 in 50ms.
- The attacker can infer an open port is open by sending a sequence of packets (spoofed or not) and watch the difference in the observed response.

III. Side Channel



[3] *Interfere with each other on global counter*

UDP Probes: UDPs with different dst port # that need to infer

UDP Verification: UDP destined to known-to-close port (e.g., 1)

IV. Evaluation

Real world attacks:

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

[1] Serves an educational network with 70M queries/day

[2] Serves an entire country

```
$ dig @          test2.test.xiaofengtest.net +timeout=999

; <<>> DiG 9.11.5-P4-5.1ubuntu2.1-Ubuntu <<>> @          test2.test.xiaofengtest.net +timeout=999
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;test2.test.xiaofengtest.net.   IN      A

;; ANSWER SECTION:
test2.test.xiaofengtest.net. 300 IN     A       1.2.3.4

;; AUTHORITY SECTION:
test2.test.xiaofengtest.net. 3534 IN    NS      ns.test2.test.xiaofengtest.net.

;; ADDITIONAL SECTION:
ns.test2.test.xiaofengtest.net. 294 IN  A       54.177.157.64

;; Query time: 172 msec
;; SERVER:          #53(          )
;; WHEN: Thu Apr 02 20:54:05 UTC 2020
;; MSG SIZE  rcvd: 105
```

Screenshot of a successful attack

The victim resolver returns the poisoned record (1.2.3.4) from its cache

NS=Name Server