blackhat USA 2023

AUGUST 9-10, 2023

BRIEFINGS

MaginotDNS: Attacking the Boundary of DNS Caching Protection

Speaker(s): Zhou Li Contributor(s): Xiang Li and Qifan Zhang August 2023





About Us



Zhou Li Assistant Professor at UC Irvine Research interests: DNS, Graph Security analytics (GSA), ...



Xiang Li PhD at Tsinghua University





Qifan Zhang PhD at UC Irvine





Our MaginotDNS attack could poison a whole TLD, e.g., .com, at one round.

All domains under that TLD can be hijacked.







>DNS overview >DNS cache poisoning >MaginotDNS workflow >Attack demo >Large-scale scanning Discussion & conclusion







Domain Name System (DNS)

> DNS Overview

- □ Translating domain names to IP addresses
- □ Entry point of many Internet activities
- Domain names are widely registered











INCREASE year over year from Q4 2021^{1,2}



DNS Resolution

> Resolution Process

- □ Primarily over UDP
- □ Iterative and recursive
- Record caching















>DNS overview >DNS cache poisoning >MaginotDNS workflow >Attack demo >Large-scale scanning Discussion & conclusion







DNS Cache Poisoning









Massive DNS poisoning attacks in Brazil



🛛 2 minute read



Unpatched DNS Bug Puts Millions of Routers, IoT Devices at Risk





🎔 in 🖾 Share

72% of organizations hit by DNS attacks in the past year

MASOUERADE PARTY -DNS cache poisoning, the Internet attack from 2008, is back from the dead

A newly found side channel in a widely used protocol lets attackers spoof domains. DAN GOODIN - 11/12/2020, 6:30 AM







On-path DNS Cache Poisoning

Kashpureff Attack (on-path, 1997)

□ Method: returning forged responses from the authoritative

- Result: resolver accepting all records in the response
- Cause: lacking data verification (**bailiwick rules**)









DNS Bailiwick Rules

> Mitigating the Kashpureff Attack

- □ Record validation when storing cache entries
- Checking for "in bailiwick" in response data: answer records must be from the same domain as the requested name









After the Kashpureff attack, bailiwick checking is integrated into the resolver's implementation,

DNS cache poisoning on recursives from the on-path seems **impossible** to conduct from 1997.





Off-path DNS Cache Poisoning

Kaminsky Attack (Off-path, 2008)

□ Method: injecting forged responses with the birthday attack

Result: resolver accepting glue records in the response

Cause: lacking **source port randomization** (TXID only 16 bits)







If TXID matching, success!

Step 3: Response

ଟ୍ଟ www123.mybank.com A?

(empty)

mybank.com NS ns.mybank.com

Hans.mybank.com A 6.6.6.6



DNS Source Port/TXID Randomization

Mitigating the Kaminsky Attack

- □ Increasing the query guessing entropy
- □ 16-bit source port x 16-bit TXID = 32-bit space

□ Hard to brute force









After the Kaminsky attack, source port randomization is integrated into the resolver's implementation,

DNS cache poisoning on resolvers from the off-path became difficult to conduct from 2008.







>DNS overview >DNS cache poisoning >MaginotDNS workflow >Attack demo >Large-scale scanning Discussion & conclusion









Are bailiwick checking and port randomization good enough?

No. MaginotDNS breaks this guarantee with a new powerful cache poisoning vulnerability.





MaginotDNS Attack

> What is the MaginotDNS attack

- □ A new powerful DNS cache poisoning attack against CDNS resolvers
- Can be launched from either **on-path** or **off-path**
- Can poison arbitrary domains including TLDs, such as .com and .net

≻ Name

- Exploiting vulnerabilities of bailiwick checking to bypass itself
- □ Working like breaking the Maginot Line → MaginotDNS









What is the CDNS resolver?

A conditional DNS resolver with both recursive and forwarding query modes.





DNS Resolvers

> Worldwide > Multiple Roles **ODNS Recursive**, forwarder **RDNS** □ Hidden DNS (HDNS) **FDNS** RDNS Complex Interaction > CDNS □ One of HDNSes őçö DN □ Never been studied ە يت Clien







Attack Target: CDNS

Conditional DNS Resolver (CDNS)

- □ Forwarder + recursive resolver (shared cache)
- □ 2 query zones used for different resolution
 - \circ *Z_F*: domains for forwarding queries
 - \circ *Z_R*: domains for recursive queries

>Usage Scenarios

- **Enterprise**: splitting networks
- □ ISP: reducing heavy traffic cost







Attack Overview of MaginotDNS

Threat Model

- \Box Assuming we discovered a CDNS and inferred its $Z_F \& Z_R$
- Attacking the forwarding mode

> Why forwarding mode?

- □ Bailiwick checking of the recursive mode is well enforced
- □ But the forwarder mode is not
- □ Since they share the same global DNS cache
- We can exploit the weak forwarder mode to attack the well-protected recursive mode
 - $\circ \rightarrow$ Breaking the boundary of DNS cache protection







Software Analysis

Finding Vulnerable Software

- □ In depth **bailiwick checking implementation** analysis
- □ Via source code review, debugging, and testing
- □ 8 mainstream DNS software, e.g., BIND and Microsoft DNS





Inconsistent bailiwick checking implementations



Root Cause & Vulnerable Software

> General Bailiwick Checking Logic

□ Summarized by us

Root Cause

□ In the InitQuery function:

o Qry.zone is set to root → all records is in-bailiwick (root's subdomains)

> Vulnerable Software

DNS Software	Forwarding	Recursive	Vulnerable
BIND9	Enabled	Enabled	Yes
Knot Resolver	Enabled	Enabled	Yes
Microsoft DNS	Enabled	Enabled	Yes
Technitium	Enabled	Enabled	Yes





Algorithm 1: DNS resolution process				
input : A DNS Request from clients				
output: A DNS Reply to clients				
main()				
step 0: InitOuery (O, Request)				
sup 1: if SeachCache (Q. Cache) then				
goto final				
<pre>step_2: FindServers (Q, TgtSvrs)</pre>				
<pre>step_3: SendQuery (Q, TgtSvrs)</pre>				
<pre>step_4: ProcessResponse (Q, R)</pre>				
if ServerIsError (Q, R) then				
goto step 3				
if not MatchQuery (Q, R) then goto final				
Sanitize Records $(O R)$				
if IsReferral (<i>O</i> , <i>R</i>) then				
if not IsFwding () then				
UpdateOuery (O)				
goto step 2				
if ISCNAME (Q, R) then				
UpdateQuery (Q)				
goto step 1				
CacheRecords (<i>R</i> , <i>Cache</i>)				
final: ConstructReply (Reply)				
InitQuery (Q, Request)				
initialize Q.name, Q.type, Q.zone				
<pre>if IsFwding() then</pre>				
ModifyFwdQuery(Q)				
SanitizeRecords(<i>O</i> , <i>R</i>)				
for $RR \in R$ do				
if OutofBailiwick (<i>RR</i>) then				
remove <i>RR</i> from <i>R</i>				
UpdateQuery(Q , R)				
update Q.name, Q.type, Q.zone				



Bailiwick Checking (Done Right)







Bailiwick Checking (Done Wrong)

Forwarding zone: example.com

Recursive zone: {domains}-example.com









Attack Steps of MaginotDNS (On-path)

- Returning fake responses directly
- BIND, Microsoft DNS, Knot, and Technitium







Attack Steps of MaginotDNS (Off-path)

- Guessing source port & TXID
- Microsoft: new port vulnerability
- BIND9: using the SADDNS attack







Control the reply time

R



Off-path Attack on BIND9

Guessing Source Port

- □ We use SADDNS to infer the source port
- □ ICMP rate-limit side-channel (check the SADDNS paper for details)

> Brute-forcing TXID

- >Attack analysis
 - □ Source port range: 32,768 60,999 (28,232)
 - Query timeout: 1.2s, guessing 50 ports each round
 - □ Success rate after 3,600 rounds:
 - $0 1 [(28,232 50)/28,232]^{3,600} = 99.8\%$







Off-path Attack on Microsoft DNS

Guessing Source Port

- □ We found MS DNS only uses ~2,500 source ports for resolution
- □ 2,500 ports are all in the open state (SADDNS not working)

Brute-forcing all 2,500 ports

- Brute-forcing TXID
- > Attack analysis
 - □ Source port range: probing in advance (2,500)
 - Query timeout: 5s, guessing 20 ports each round
 - □ Success rate after 720 rounds:
 - $0 1 [(2,500 20)/2,500]^{720} = 99.7\%$











>DNS overview >DNS cache poisoning >MaginotDNS workflow >Attack demo >Large-scale scanning Discussion & conclusion







MaginotDNS Attack Demos

> On-path Attack

□ The result is determinative

> Off-path Attack

□ Microsoft: avg. 802s

BIND9: avg. 790s.



Watch videos here.



Notes Note Note <t< th=""><th>Off-path-sattack 0 second secon</th><th>Control (Control (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro) (Contro)</th><th>LD: V</th><th>Thu / Thu / Thu / Thu / Thu / Thu / Thu / Thu / Thu /</th></t<>	Off-path-sattack 0 second secon	Control (Control (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro) (Contro)	LD: V	Thu / Thu / Thu / Thu / Thu / Thu / Thu / Thu / Thu /
B GC 2021 10/2113/037 FCB1 10/1 H0/260/ HELSEN (HLSE) B GC 2021 10/2113/037 FCB1 10/2 H0/260/ HLSEN (HLSE) B GC 2021 10/2114/037 FCB1 10/240/ H0/260/ HLSEN (HLSE) B GC 2021 10/2114/037 FCB1 10/240/ H0/260/ HLSEN (HLSEN (HLSE) B GC 2021 10/2114/037 FCB1 10/240/ HCSEN (HLSEN (HLSEN (HLSE)) B GC 2021 10/2114/037 FCB1 10/240/ HCSEN (HLSEN (HLSEN (HLSEN)) B GC 2021 10/2114/037 FCB1 10/240/ HLSEN (HLSEN (HLSEN (HLSEN)) B GC 2021 10/2114/037 FCB1 10/240/ HLSEN (HLSEN (HLSEN (HLSEN)) B GC 2021 10/2114/037 FCB1 10/240/ HLSEN (HLSEN (HLSEN (HLSEN)) B GC 2021 10/2114/037 FCB1 10/240/ HLSEN (HLSEN (HLSEN (HLSEN (HLSEN))) B GC 2021 10/2114/037 FCB1 10/240/ HLSEN (HLSEN (HLSEN (HLSEN (HLSEN))) B GC 2021 10/2114/037 FCB1 10/240/ HLSEN (HLSEN (HLSE	L sterr freed	(1.64/728) 6 (1.64/728) 6 (1.64	** attack cost 1940.99756s ************************************	Thu A Thu A Thu A Thu A





23:10:5 23:10:5 23:10:5 23:10:5 23:10:5 23:10:5 23:10:54 6 23:10:54 6 23:10:5

2021 :	(2/360)	dns	query : 2-BatHkHSX.idealeer.com	
2021 :	(2/360)	dns	response	
2021 :	(2/360)	dns	attack with fake com. 15%	
2021 :	(2/360)	dns	attack with fake com. 37%	
2021 :	(2/360)	dns	attack with fake com. 60%	
2021 :	(2/360)	dns	attack with fake com. 85%	
2021 :	(2/360)	dns	attack with fake com. 100%	
2021 :	to 202.2	112.2	238.57 : 1310720 pkts in 4.632276358s	
2021 :	(2/360)	dns	check	
2021 :	(2/360)	dns	check : com. NS gtld-servers.attack.	
2021 :	dns atta	ack s	succeeded with 2 guesses, cost 10.079395433	s

Log of Attacking Microsoft

2021	(661/3600)	dns	querying
2021	(661/3600)	dns	consuming 50 credits
2021	(661/3600)	dns	scanning port 40001-40050
2021	(661/3600)	dns	scanning port 40020 open (651.902104ms)
2021	(661/3600)	dns	replying
2021	(661/3600)	dns	replying 65535 (928.938966ms)
2021	(661/3600)	dns	checking
2021	(661/3600)	dns	checking NS gtld-servers.attack.
2021	(661/3600)	dns	attack successfully (13m12.992182401s)
2021	(661/3600)	dns	attack cost (13m12.99219492s)

Log of Attacking BIND9





Off-path Attacks on BIND9 & Microsoft DNS

		off-path	attack	of BIN	D	Carrier and the second se
THE OWNER		ALL DESCRIPTION OF	Statements and the	a photolog root	1. Constructions	dis stinit over our 175 distrine
			street officers of man lines	a 00-00-00 0001	· 1945/72461	Attacker
	In set sets in which has been, but tradely arrests privately.		Arrive 18 (868 261	A BOOM STATE	1.1044/10465	the Lansau 18 credity MULCIUNCI
-	to be and the table of the second s		from a set but	+ 99.64138 2823	1 Classification (The same part which which characters whereas a
	and the second s	1	And in the second second	A DOUBLE DESC	1 Classification 1	and attain good county-worker total represent
	the local state of the second of the second state of the second st	100	And In the lot	* #9-10108.700X	1-1040/12000	sha artain uses cont 580. Machine
0.00			Title II and Do	8.85159188.2823	1 TRANSCOMP.	den ettigen ment sitt. 2606236
	Parameter allante and the second car at at at the second car in	G	particular in the second lists	a pression part.	1.1204/324041	and party
	ar her after so-at to at "anter the second program		COLUMN TWO DOLD	1. 101.011.00 2021	 Contract Contract 	dia and bott short while
	a be an a second and the second s	1	party in and his	1 09.00.00 PMD	A COMPANY OF STREET	dia atan port 18681-58088 closer 1284,25862804)
	an out the most property and relies and employing arranged attacks.	and the second sec	and 201	· • • •• • • • • • • • • • • • • • • •	1.1206772863	Ava allock failed time.covers1
	the days into the late and the first the work of a late of the	Completent Sectors	0w0 -004	A REALISTIC COLL	1.10040/228081	ges within over that the DOULER
	at an our sector of during the spin and a markle sciently	a print satura last	Party in the local	A THE RELATE CALLS.	1 LODGE TO BE	dia matrix
	an our little as in in the lease of a standard stranger of the little as	a print option is not i	the state of the state	1, 10, 60, 60, 10, 11,	1.1003/19981	dra concer de scentra
	an and an an in the second second second second second by	a providence per	salar in the day	4 20180300 2003	1.1010/378983	des sue poly while while
	the second	a set of the tax of the local set.	Contract of the second second	A DECEMBER OF STREET	A LODGE COMMENTS	des sone port office that entrance (TTE Semillion)
	en det alle de la del ferrie de la desta de la dest	A ALL MADE AND AND	Links in that for	A 10-04704-1011	COLUMN TRACK	dra attuit utan tiri VII. IMPORt
	the new place who are proved for the public and the provider of the latter	Carter demark liet.	station in these first	A DAMAGE DATE.	1.10032719981	the street hear and provide
		a sub references to the	the lot of	A 18-86-81 2003	1.1040/12481	dire autority
	the first second as any initial The second privates and all	a and second and	States in the local	A DESIGNATION OF THE	- 1000/100000	dis termine in confits
	an and an an an an an and an	a plant speak and	states in their last	· A TALANCES DATE	1 1002/12004	the loss part sheet child closet (187, 396261es)
	an in the state of the set with the before all sets of the S	a and the set of a	PARTY PARTY Det	+ 18 68:81 7871	1 1000/12000	der alltets Andel 1387-430873es1
	the first provide and the same one other attacks attacks attacks. The	a station and the	Contract Contract Contract	A 10104-01-2021	1.1352/33483	des attack date test 187,000000
	이는 것은 것 같은 것을 것 것 것 같은 것 것 같이 것 같이 것 같이 것 같이 것 같이 것 같		West for the second	6 10:00 EL 2021	1.1052/39881	The attack over the Skillers
	to be the second second second with the second	States and the second	States of the local lines.	a terminal part.	1 CONSTRUCTION	dry presses 10 predity
	and the second second second reaching the second	A DECEMBER OF STREET	the second second	A 18 18 18 18 1911	1.1003/12008	des sign part piets-child
	en an ann an an an an Anna an A	a set of the set of the	Libe is and for	+ 18184183 2021	1.052/11841	den stad 2021 0000-0000 tilsen 1591.0005000)
	the next side of the set of a factor of the set of a set of the se	the set of resident states	And the second second	+ 1/2 APR 11 2011	1.1555/12884	ans ettant fatian (188-6581/046)
	이 이는 것이 안 같은 것은 것이가 것을 가지만한 것이라는 것이다.		the first	a particular conta	A LINE TOWN	die attach over the William
	an out-only spinster, and taking the product because second a	C STATE OF BAR AND	OPPORT NO HAR DO	A DEPOSITE ONLY	1. USACIDESI.	dia duale
	an dah ber dana da Per Yang ber berter atau dari dari dari dari dari dari dari dari	the state over the state of	And the second	A 18 BURNER, 2003	HARPER	the paperse in conducts
	We start we want the start of t	an the at	tack sei	IDE WHERE	SAUN	NVGA-1011 - MARI - MARI
	the second s	and the second second	and the second second	And in case of the local division of	Sector Sector	Statement of the statem
			Carlos inc	and all the second second	100	
				A PERSON A PERSON A	ALC: NO.	and the second s

BIND9

Microsoft DNS











>DNS overview >DNS cache poisoning >MaginotDNS workflow >Attack demo >Large-scale scanning Discussion & conclusion







Finding Vulnerable CDNSes

Differentiating Forwarder & Recursive

- □ Based on the DNS resolution mechanism
- □ Forwarders do not cache intermediate NS records

Finding CDNSes

- □ New methodology
 - 1. Targeting one resolver
 - 2. Testing a group of domains, sending **NS&NR** queries
 - 3. For some domains, no NS responses (forwarding)
 - 4. For others, we get NS responses (recursive) ----
 - 5. The resolver does both forwarding & recursive resolution
 - 6. \rightarrow CDNS identified







Vulnerable CDNS Population

Measurement

- □ We collected **1.2M resolvers**
- Removing not-applicable ones, such as violating NR or multiple caches
- □ Applying our method to identify **154,955 CDNSes**
- □ Using **software fingerprints** to locate **54,949 vulnerable CDNSes**
 - \circ Resolvers with DNSSEC or 0x20 are filtered out

CDNSes identified by probing	154,955	41.8%
– Version identifiable (in CDNS)	117,306	31.7%
-by version.bind	59,419	16.0%
- by fpdns	57,887	15.6%
– OS identified for BIND (in CDNS)	19,995	5.4%
– DNSSEC validation (in CDNS)	34,424	9.3%
- 0x20 encoding (in CDNS)	1,119	0.3%

Vulnerable CDNSes	54,949	14.8%
– On-path attack possible [*]	54,949	14.8%
– BIND	24,287	6.6%
– Microsoft DNS	30,662	8.3%
– Off-path attack possible [*]	48,539	13.1%
– BIND (OS exploitable)	17,877	4.8%
– Microsoft DNS	30,662	8.3%
– Recursive-default	10,445	5.0%
– Forwarding-default	36,581	9.9%







>DNS overview >DNS cache poisoning >MaginotDNS workflow >Attack demo >Large-scale scanning Discussion & conclusion







Discussion & Mitigation

> Vulnerability Disclosure

- **Confirmed** and **fixed** by **all affected software**: BIND9, Knot, Microsoft, & Technitium
- **4 CVE-ids** published & **Bounty** awarded by Microsoft

Root Cause

- **Problematic forwarding bailiwick checking implementations (**gry.zone <- root)
 - Why? Forwarder needs flexibility

Mitigation Solution

- \Box gry.zone should be set to the forwarded domain in Z_F (query zone restriction)
- □ Then only records under forwarded domain are acceptable (cache split)
- □ Have been adopted by affected software





Black Hat Sound Bytes

> Bailiwick checking is not bullet-proof!

□ We thought it's perfect after **26 years** since it's born.

> Inconsistent DNS implementations are common...

- □ Forwarder vs. resolver
- BIND, Knot, Microsoft,
- □ Partially caused by the vague RFCs

> There might be more vulnerabilities we don't even know ...

- □ We need **automated tools** (e.g., fuzzers) customized to analyze DNS software
- \Box My group is working on that \odot











Paper



Thanks for listening! Any questions?

Zhou Li, <u>zhou.li@uci.edu</u> Xiang Li, <u>x-l19@mails.tsinghua.edu.cn</u> Qifan Zhang, <u>qifan.zhang@uci.edu</u>





Tool