The "Indefinitely" Delegating Name Servers (iDNS) Attack

Florian Maury, ANSSI

May 10, 2015

ANSSI

- is the French Network and Information Security Agency
- works under the authority of the French Prime Minister
- main missions regarding information systems security are:
  - prevention
  - defence
  - information

One of its priorities is Internet resiliency, including DDoS prevention

DNS reminders

Reminders about Delegations Inner-working

Glueless delegation example

```
;; AUTHORITY SECTION
france.fr.  IN NS ns2.produhost.net.
france.fr.  IN NS ns33.produhost.net.
```

Glued delegation example

```
;; AUTHORITY SECTION
ssi.gouv.fr.  IN NS dns1.certa.ssi.gouv.fr.
ssi.gouv.fr.  IN NS dns1.ssi.gouv.fr.
;; ADDITIONAL SECTION
dns1.ssi.gouv.fr.  IN A 213.56.166.96
dns1.certa.ssi.gouv.fr.  IN A 213.56.176.3
```

The iDNS Attack in a Nutshell

The iDNS Attack in a Nutshell

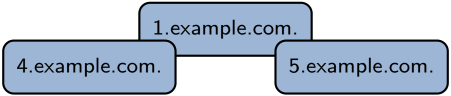
1.example.com.

Exploitation strategy:

- a dynamically-generated infinite glueless delegation chain

Vulnerable recursive servers will follow this chain for a long, possibly infinite, period.

The iDNS Attack in a Nutshell

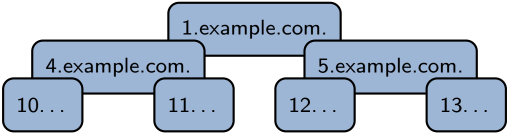


Exploitation strategy:

- a dynamically-generated infinite glueless delegation chain

Vulnerable recursive servers will follow this chain for a long, possibly infinite, period.

The iDNS Attack in a Nutshell

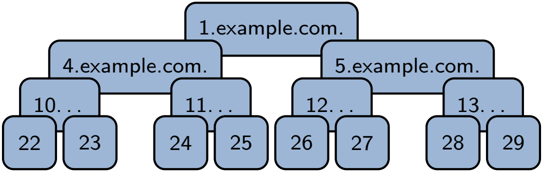


Exploitation strategy:

- a dynamically-generated infinite glueless delegation chain

Vulnerable recursive servers will follow this chain for a long, possibly infinite, period.

The iDNS Attack in a Nutshell

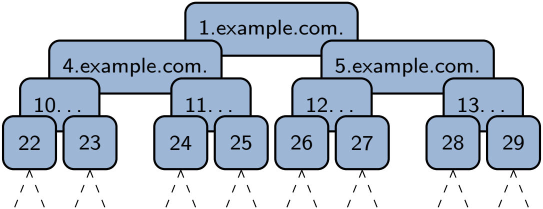


Exploitation strategy:

- a dynamically-generated infinite glueless delegation chain

Vulnerable recursive servers will follow this chain for a long, possibly infinite, period.

The iDNS Attack in a Nutshell

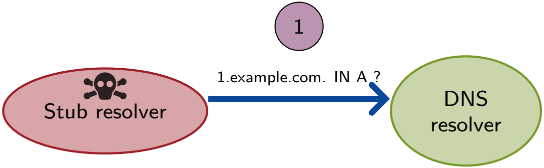


Exploitation strategy:

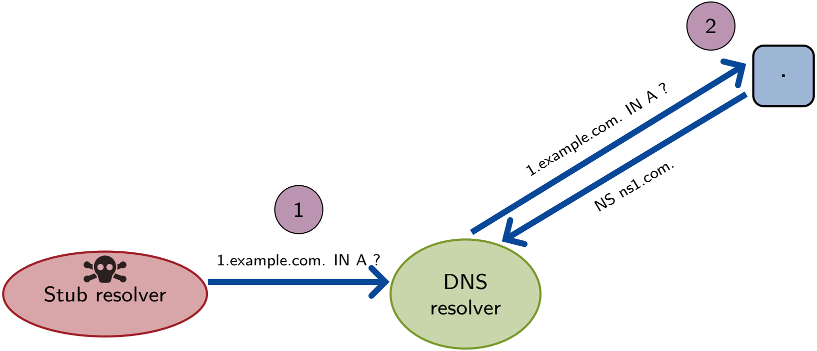
- a dynamically-generated infinite glueless delegation chain

Vulnerable recursive servers will follow this chain for a long, possibly infinite, period.

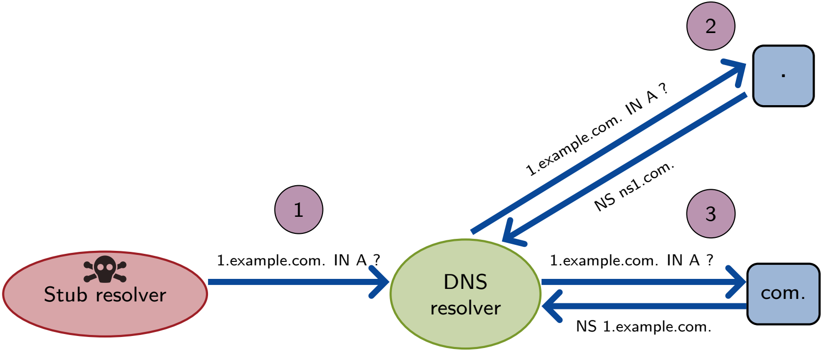
Denial of Service Attack
against
Recursive Nameservers



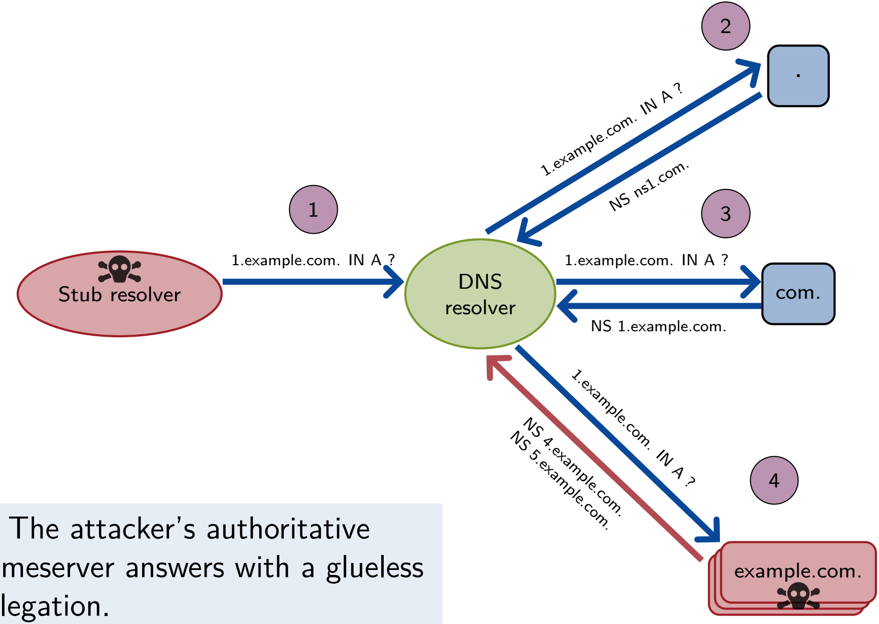
1: An authorized stub resolver queries an arbitrary domain name.



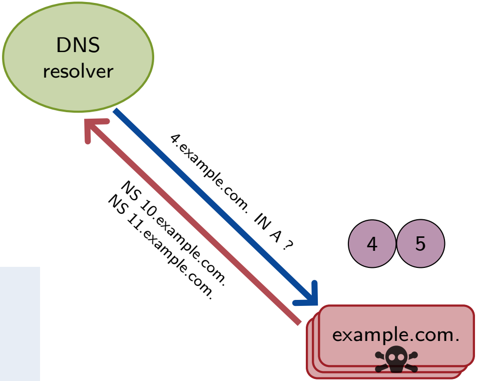
2,3: The resolver follows the referrals, as usual, until it reaches the attacker-controlled domain name.



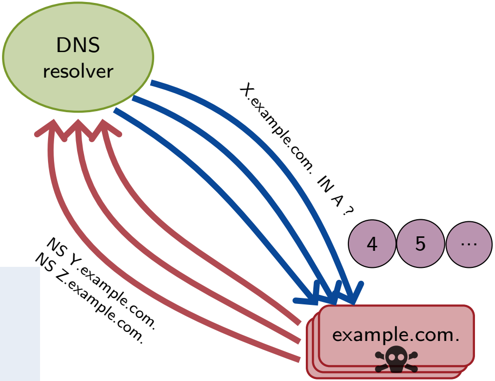
2,3: The resolver follows the referrals, as usual, until it reaches the attacker-controlled domain name.



4: The attacker's authoritative nameserver answers with a glueless delegation.



5: The resolver follows this referral, which leads it to query once more the attacker's authoritative nameserver.



Repeat indefinitely.

Summary

Attack traits:

- enabled from a single query
- RFC-compliant individually innocent-looking messages
- sometimes self-sustained

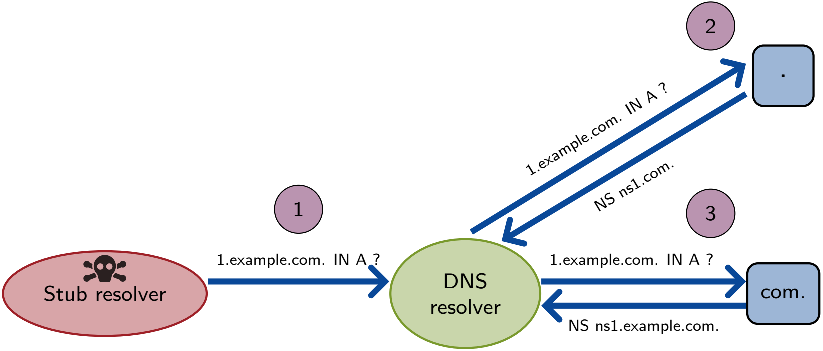
Impact:

- **Temporary or permanent DoS of the resolver**

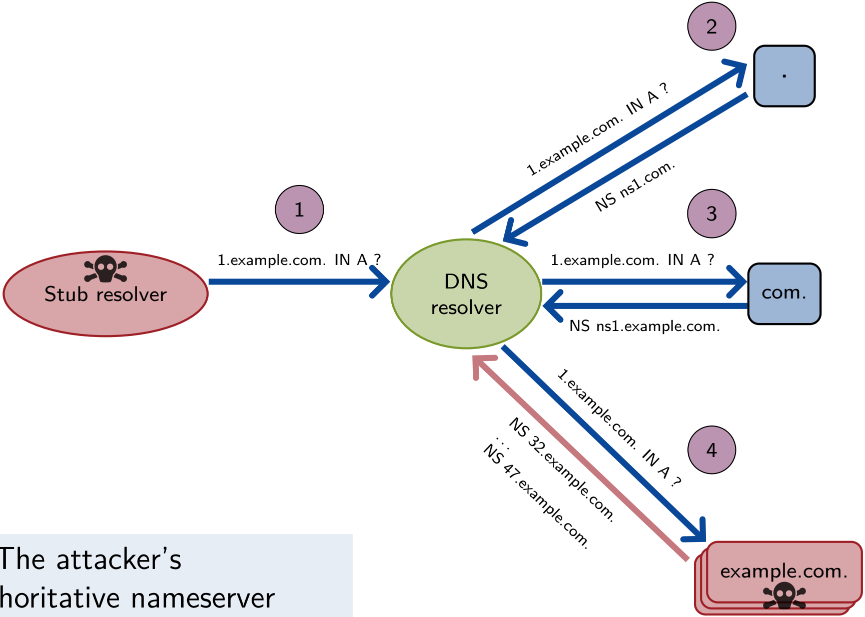
DDoS Variant of the iDNS Attack

Attack Payload Sample

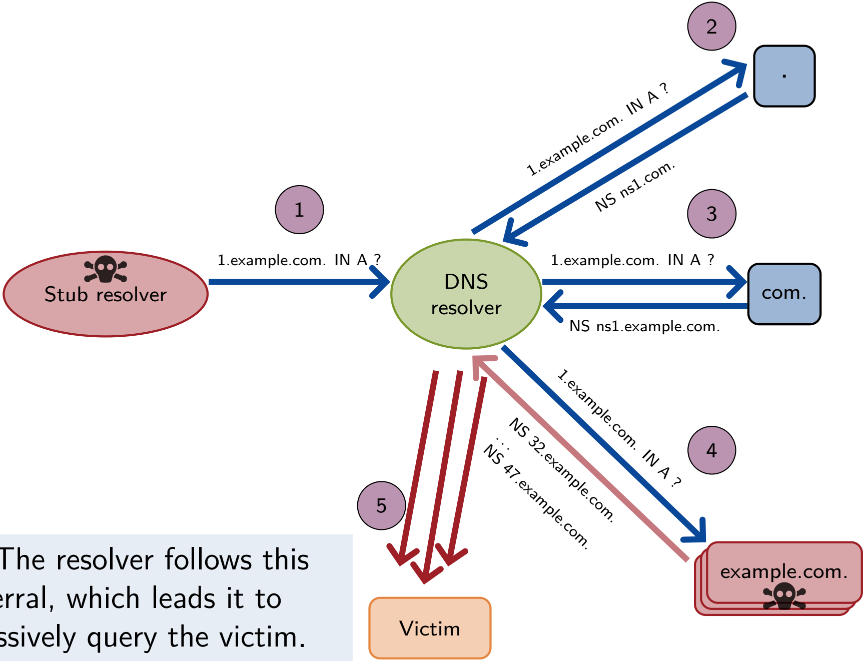
```
$ dig @AttackerAuthServ A 1.example.com.

...

;; AUTHORITY SECTION
1.example.com.  IN NS 32.example.com.
1.example.com.  IN NS 33.example.com.
...
1.example.com.  IN NS 47.example.com.
;; ADDITIONAL SECTION
32.example.com.  IN A  192.0.2.1
33.example.com.  IN A  192.0.2.2
...
47.example.com.  IN A  192.0.2.16
```



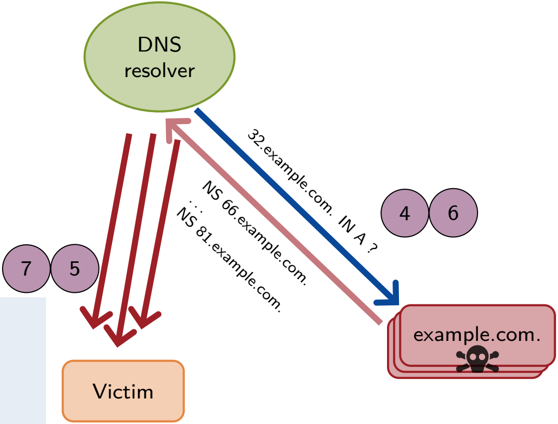
1,2,3: Attack begins as previously.



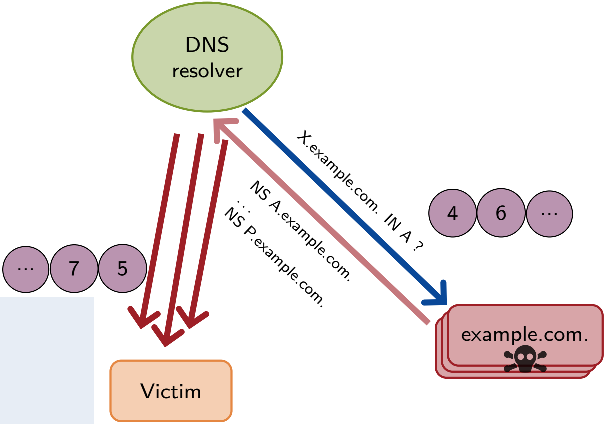
4: The attacker's authoritative nameserver answers with a massive glued delegation.



5: The resolver follows this referral, which leads it to massively query the victim.



6: Gratuitious queries may be sent to attacker's authoritative nameserver.



Repeat indefinitely.

Summary

Attack traits:

- enabled from a single query
- uses only RFC-compliant messages
- exploits well-configured servers
- sometimes self-sustained

Impact:

- **offers a Packet Amplification Factor (PAF) of 10+**

Operational Impact Study

Impacted Systems and Software

Vulnerable software:

- **BIND** $<$ 9.9.6-P1 and $<$ 9.10.1-P1
    - some BIND auth-only deployments are also affected
- **Unbound** $<$ 1.5.1
- **PowerDNS Recursor** $<$ 3.6.2
- **Efficient IP** $<$ 5.0.4.p1 or $<$ 5.0.3.p4
- **MaraDNS** $<$ 1.4.15, $<$ 2.0.10
- **Deadwood** $<$ 3.2.06
- **Infoblox NIOS** $<$ 6.8.13, $<$ 6.10.11, $<$ 6.11.7 and $<$ 6.12.2

Operational Impacts

Impact varies from one implementation to another.

Temporary DoS:

- high CPU consumption
- high memory consumption
- cache exhaustion
- network load (pps)

Permanent DoS:

- crash/killed

Network Collateral Damage

Some recursor implementation may survive: partial DoS.

However, some network devices may be overwhelmed by the generated network load.

Some obvious potential victims:

- out-of-the-box stateful firewalls
- NAT-based load balancers

Disclosure Plan & Feedback

Disclosure Plan (1)

Original disclosure plan:

- Google and OpenDNS first contacted for operational feedback
- reporting to ISC, NLNet Labs, and NetherLabs
- embargo of two months
- synchronous disclosure on December 8, 2014

Disclosure Plan (2)

Early releases:

- ISC advisories to premium clients a week before common disclosure
- NetherLabs early "performance patch"
  - a "slow domain" reported independantly by a customer

Feedback

Some GNU/Linux distributions were informed too late

Mitigation Strategies

Mitigation Strategies Matrix

	BIND	Unbound	PowerDNS Recursor	Microsoft DNS	OpenDNS
Depth limit					
Breadth limit					
Overall query time limit					
Overall query count limit					
Maximum in-flight query count					

Details

Mitigation Strategies Matrix

Legend: 🟩 Implemented 🟦 Not implemented	BIND	Unbound	PowerDNS Recursor	Microsoft DNS	OpenDNS
Depth limit	🟩	🟩	🟩	🟦	🟩
Breadth limit	🟦	🟩	🟦	🟦	🟩
Overall query time limit	🟦	🟦	🟦	🟩	🟩
Overall query count limit	🟩	🟩	🟩	🟦	🟦
Maximum in-flight query count	🟦	🟦	🟩	🟦	🟩

Details

Mitigation Strategies Matrix

Legend: 🟥 Hardcoded/Fixed values 🟨 Config options available 🟦 Not implemented ? ⇒ unknown value	BIND	Unbound	PowerDNS Recursor	Microsoft DNS	OpenDNS
Depth limit	🟨 7	🟨 5	🟥 15	🟦	🟥 ?
Breadth limit	🟦	🟥 16	🟦	🟦	🟥 ?
Overall query time limit	🟦	🟦	🟦	🟨 8s	🟥 ?
Overall query count limit	🟨 75	🟥 32	🟥 50	🟦	🟦
Maximum in-flight query count	🟦	🟦	🟥 1	🟦	🟥 1

Details

Contribution Summary
&
Thoughts about the DNS

Contribution Summary

The iDNS attack:

- exploits a logic flaw in DNS resolvers
- affects several popular implementations
- causes temporary or permanent DoS of affected systems
- causes potential DDoS of third party systems
- can only be fixed by patching

Patched release for BIND, Unbound and PowerDNS Recursor on December 8, 2014

Thoughts about the DNS (1)

The issue was documented.

RFC 1034 (published in 1987)

"Bound the amount of work (packets sent, parallel processes started) so that a request can't get into an infinite loop or start off a chain reaction of requests or queries with other implementations EVEN IF SOMEONE HAS INCORRECTLY CONFIGURED SOME DATA."

Tony Finch pointed that out, on DNS-OARC mailing-list.

Thoughts about the DNS (2)

Implementing DNS recursive servers is HARD:

- over 220 RFCs specifying the DNS; several active IETF WG
- performance needs ⇒ use of unsafe, low-level languages

Room remains for interpretation in many of these RFCs. When the specification fails, developers get creative.

Thoughts about the DNS (3)

DNS is fragile:

- Kaminsky attack (2008)
- block DNS messages ⇒ easier DNS cache poisoning (2013)
- DNSSEC-related bugs (since 2005)
- DNS rebinding (since 1996)
- ...

Extreme precautions should be taken when modifying the protocol.

Q & A

Implemented Mitigation Strategies (1)

ISC BIND:

- limit depth – option max-recursion-depth (default: 7)
- limit total query count – option max-recursion-queries (default: 75)

Unbound:

- limit breadth (16)
- limit depth – option target-fetch-policy (default: 5)
- limit total query count (32)

Back

Implemented Mitigation Strategies (2)

PowerDNS:

- limit depth, CNAME and alike included (15)
- limit in-flight queries per query per destination (1)
- limit total query count (50)

MaraDNS:

- limit depth (83)
- limit in-flight queries (8?)

Back

Implemented Mitigation Strategies (3)

Microsoft:

- limit overall query time – command Set-DnsServerRecursion -Timeout (default: 8s)
- limit specific query time – command Set-DnsServerRecursion -AdditionalTimeout (additional) (default: 4s)

OpenDNS:

- limit in-flight queries per query per destination (1)
- limit depth (?)
- limit breadth (?)
- limit overall query time (?)

Back