Zone Poisoning: The How and Where of Non-Secure DNS Dynamic Updates

Maciej Korczyński, Michał Król, Orcun Cetin,
Carlos Gañán and Michel van Eeten

Delft University of Technology
Contact: maciej.korczynski@tudelft.nl

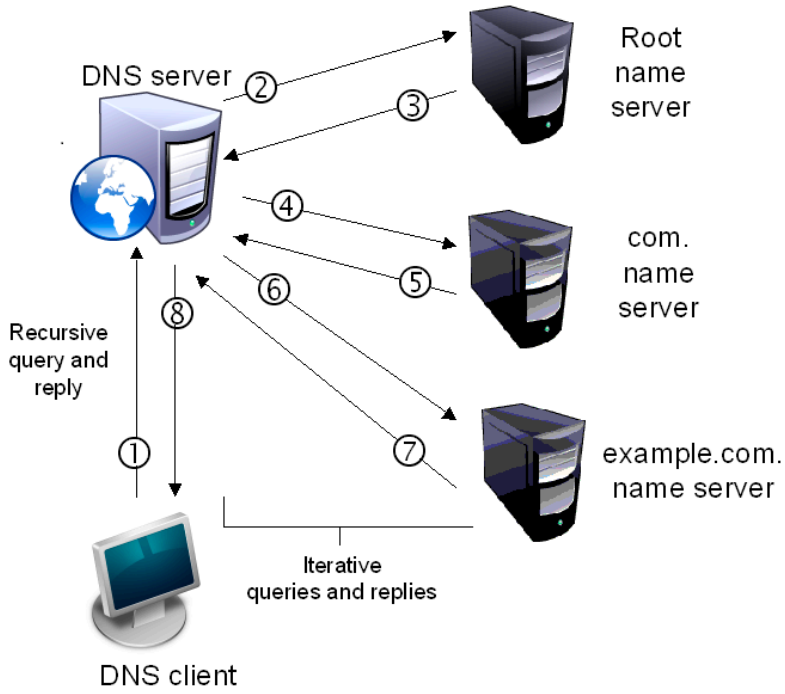
DNS-OARC 26, Madrid

15 May 2017

TU Delft

Attacks against DNS name resolution path

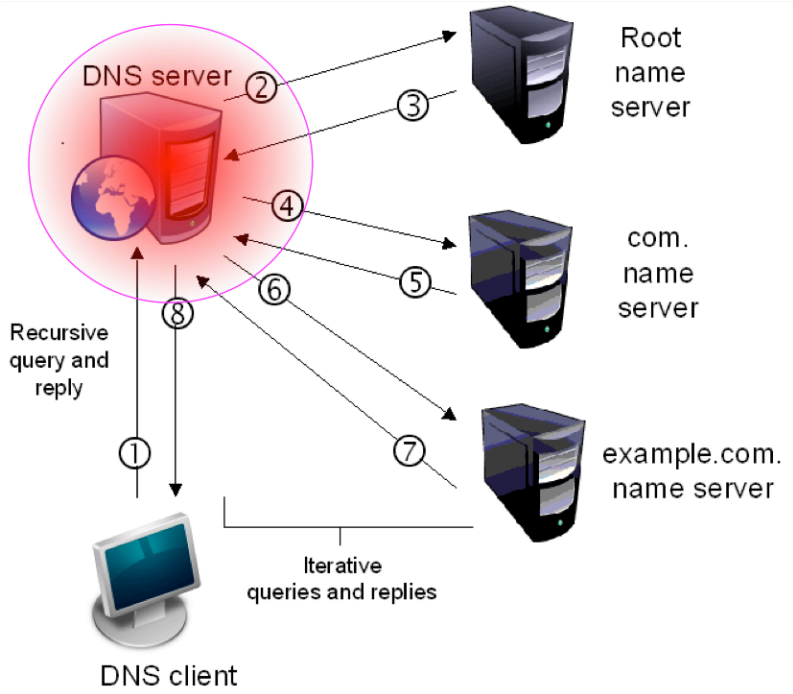
- Most attacks compromise the resolution path somewhere between the user and the authoritative name server for a domain



Source: https://www.dns-oarc.net/files/pres/OARC-CENTRtech31.pdf

Attacks against DNS name resolution path

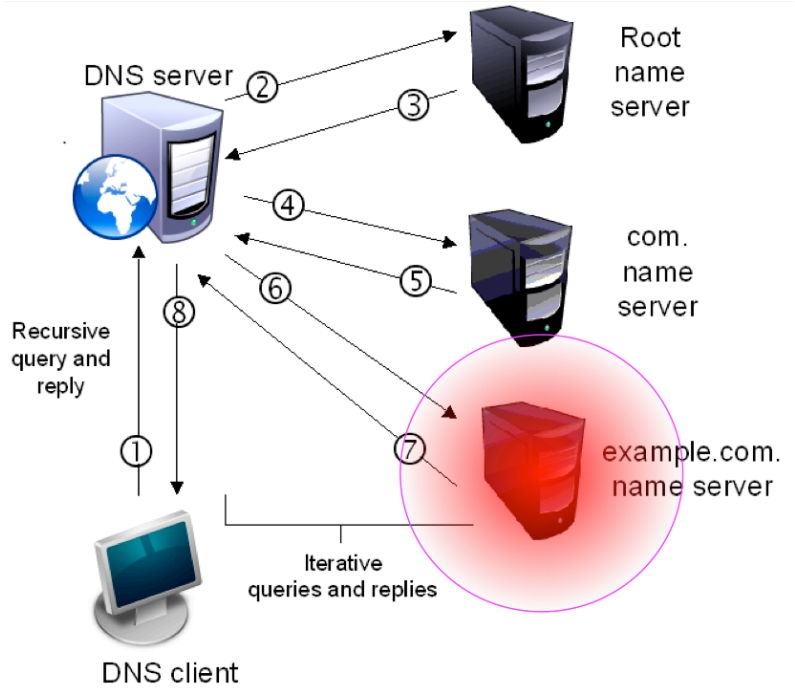
- Most attacks compromise the resolution path somewhere between the user and the authoritative name server for a domain
  - E.g. Traditional cache poisoning attacks or attacks against individual clients being directed to use a rogue DNS server *



* Dagon et al, Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority, in NDSS, 2008

Attacks against DNS name resolution path

- What about attacks against the authoritative end of the path?

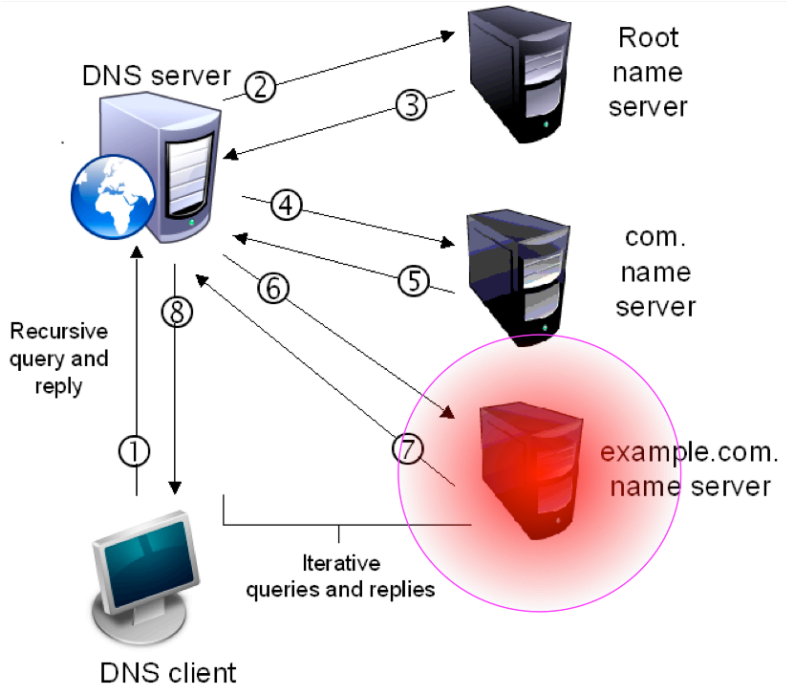


Attacks against DNS name resolution path

- What about attacks against the authoritative end of the path?
  - Domain Shadowing: is the process of using users domain registration logins to create malicious subdomains *

E.g.: legitimate.com

- secure.wellsfargo.legitimate.com
- bankofamerica.legitimate.com
- hsbc.com.legitimate.com
- …

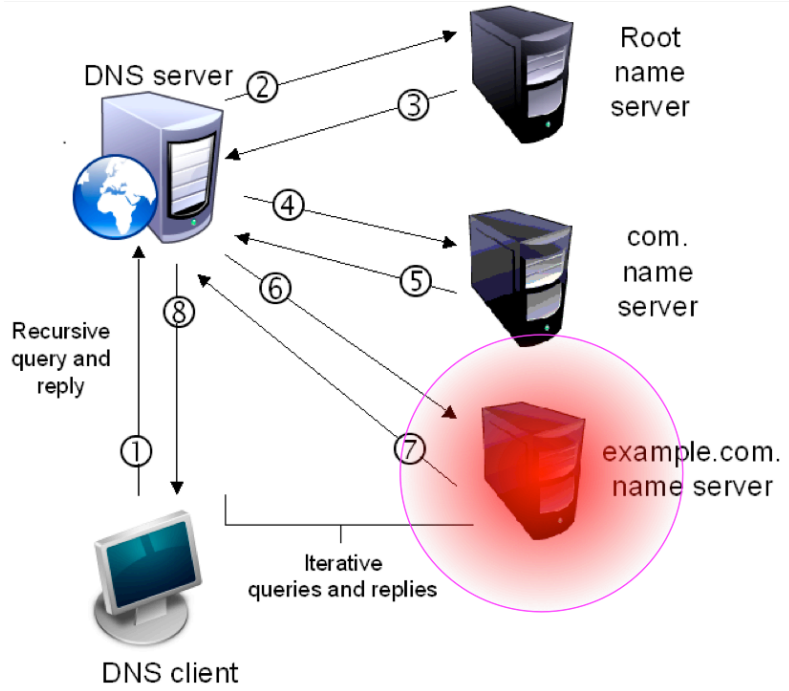


* Biasini, N., and Esler, J. Threat Spotlight: Angler Lurking in the Domain Shadows. http://blogs.cisco.com, March 2015.

Attacks against DNS name resolution path

- What about attacks against the authoritative end of the path?
  - A more ambitious vector is hacking the registrars directly *

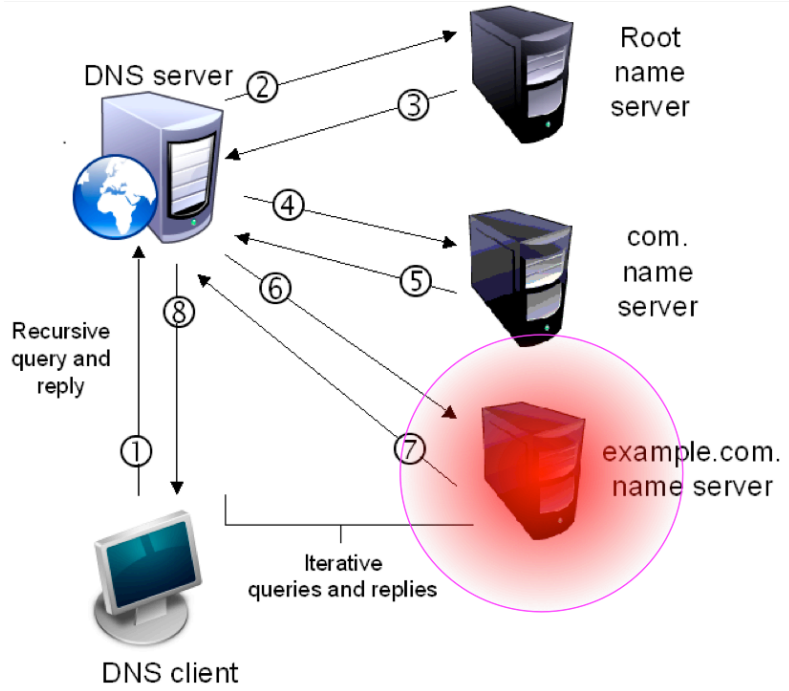
E.g. Twitter and New York Times websites replaced in August 2013



* Arthur, C. Twitter and New York Times Still Patchy as Registrar Admits SEA Hack. https://www.theguardian.com, 2013.

Attacks against DNS name resolution path

- We explore an attack against the authoritative end of the path: the zone file of the authoritative name server using **non-secure DNS dynamic update** protocol extension *



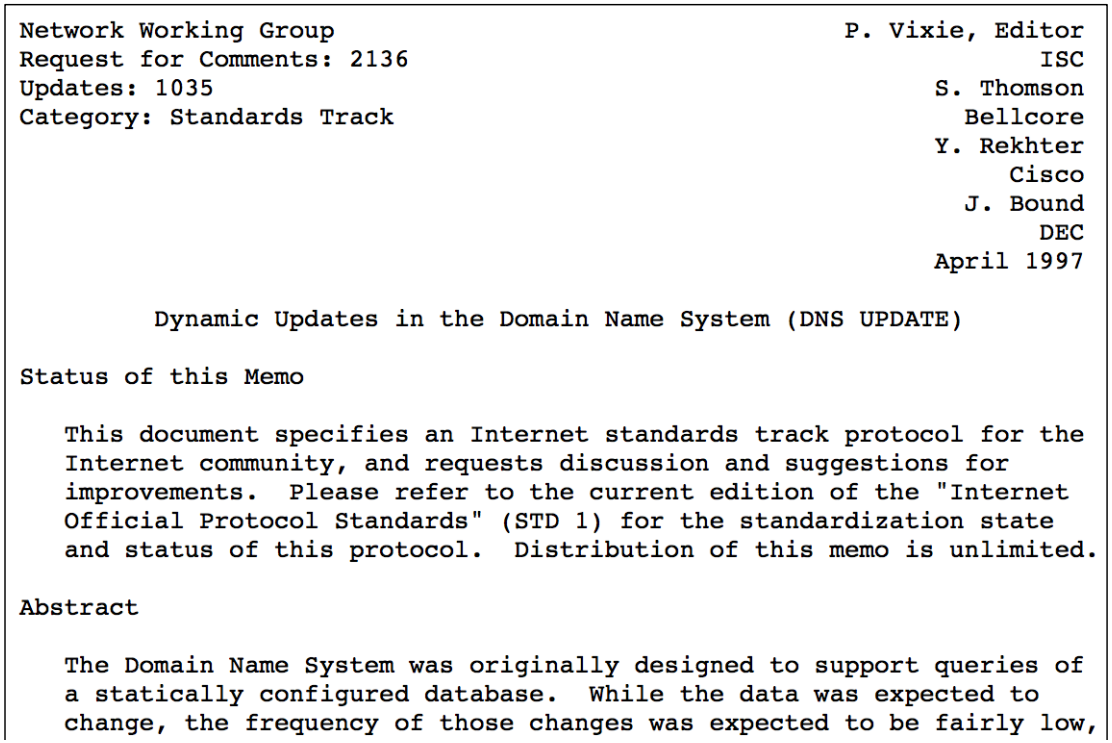
* "Zone Poisoning: The How and Where of Non-Secure DNS Dynamic Updates", Maciej Korczyński, Michal Król, and Michel van Eeten, *ACM SIGCOMM Internet Measurement Conference (IMC'16)*, pages 271-278, Santa Monica, November 2016

Agenda

- Dynamic updates in DNS
- Secure dynamic updates
- Implementations
- Zone poisoning (requirements, specifics, and threats)
- Scanning setup
- Affected domains
- Notifications
- Conclusions

Dynamic updates in DNS

- Complies with the standard DNS message
- Can add/delete any type of resource record (A, AAAA, CNAME, NS, etc.)
- Propagates between slave and master servers
- Server verifies if:
  - Prerequisites set by the requestor are met (e.g. RR exists)
  - Restrictions are met (if any)



Network Working Group
Request for Comments: 2136
Updates: 1035
Category: Standards Track

P. Vixie, Editor
ISC
S. Thomson
Bellcore
Y. Rekhter
Cisco
J. Bound
DEC
April 1997

Dynamic Updates in the Domain Name System (DNS UPDATE)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Domain Name System was originally designed to support queries of a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low,

TU Delft

Secure dynamic updates

- Security considerations in the original RFC 2136

```
8 - Security Considerations

   8.1. In the absence of [RFC2137] or equivilent technology, the
   protocol described by this document makes it possible for anyone who
   can reach an authoritative name server to alter the contents of any
   zones on that server.  This is a serious increase in vulnerability
   from the current technology.  Therefore it is very strongly
   recommended that the protocols described in this document not be used
   without [RFC2137] or other equivalently strong security measures,
   e.g. IPsec.
```

- Security measures (RFC 2137 -> RFC 3007)
- DNS Security Extensions
  - Public-key authentication
  - Resource heavy
- Secret Key Transaction Authentication for DNS (TSIG)
  - Shared secret
  - HMAC-MD5
  - Lightweight

Implementations

- BIND
  - Disabled by default
  - "allow-update" with a list of allowed hosts (with available option "any")
  - TSIG supported since 8.2

Implementations

- BIND
  - Disabled by default
  - "allow-update" with a list of allowed hosts (with available option "any")
  - TSIG supported since 8.2

```
zone "example.com" {
     type master;
     file "db.example.com";
     allow-update { 192.2.2.200; }; // just our DHCP server
};
```

Implementations

- BIND
  - Disabled by default
  - "allow-update" with a list of allowed hosts (with available option "any")
  - TSIG supported since 8.2

```
zone "example.com" {
     type master;
     file "db.example.com";
     allow-update { 192.2.2.200; }; // just our DHCP server
};
```

- Microsoft DNS
  - By default updates only via extended TSIG
  - Non-secure updates also allowed
  - Secure updates not available for standard primary zones

Zone poisoning

- Requirements:
  - Non-secure updates allowed
  - The attacker knows the name of a zone and its NS
- Specifics:
  - Single packet attack
  - No need to get response
  - Difficult to detect
- Threats:
  - Running fake website/mail server
  - Reputation abuse (`paypal.user.example.com`)
  - Subdomain delegation

Zone poisoning

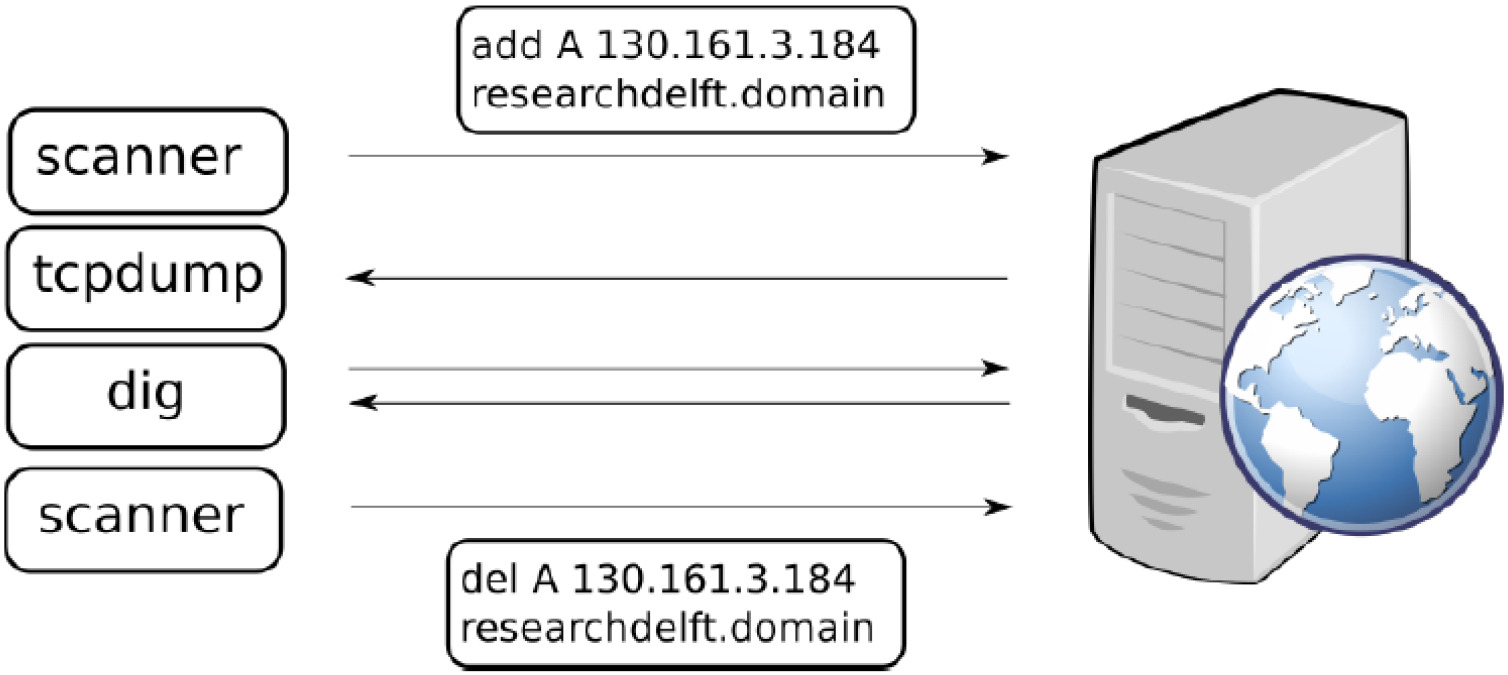
- Requirements:
  - Non-secure updates allowed
  - The attacker knows the name of a zone and its NS
- Specifics:
  - Single packet attack
  - No need to get response
  - Difficult to detect
- Threats:
  - Running fake website/mail server
  - Reputation abuse (paypal.user.example.com)
  - Subdomain delegation

```
:~$ nsupdate
> server 192.2.2.101
> zone example.com
> update add paypal.example.com 86400 A 10.10.10.10
> send
```

Ethical considerations

- Single packet sent
- No modifications on existing records
- No data on persons collected
- Previous state restored on all servers
- Website reference in the added record
- Opt-out mechanism
- Notifications

Scanning setup



Datasets

- Alexa top 1 Million domains
- Random sample of 1% of the domain space
  - DNSDB (Farsight Security *)
  - Project Sonar Data Repository
  - Zone files

#	1% Sample	Alexa 1M
Domains	2,865,393	947,823
NS	510,850	487,515
IPs of NS	438,478	418,251
Domain-NS-IP	27,499,061	7,368,659

* https://www.farsightsecurity.com

Affected domains

- First campaign (April 2016):
  - Random sample
    - 2,626 A resource records
    - 188 name servers
    - 1,877 domains (0.065%)
  - Alexa 1M
    - 881 added A RRs
    - 560 name servers
    - 587 domains (0.062%)

- First global scan (October 2016)
  - 579,096 A RRs
  - 5,738 name servers
  - 309,687 domains

- Second global scan (February 2017)
  - 679,930 A RRs
  - 5,576 name servers
  - **381,966** domains

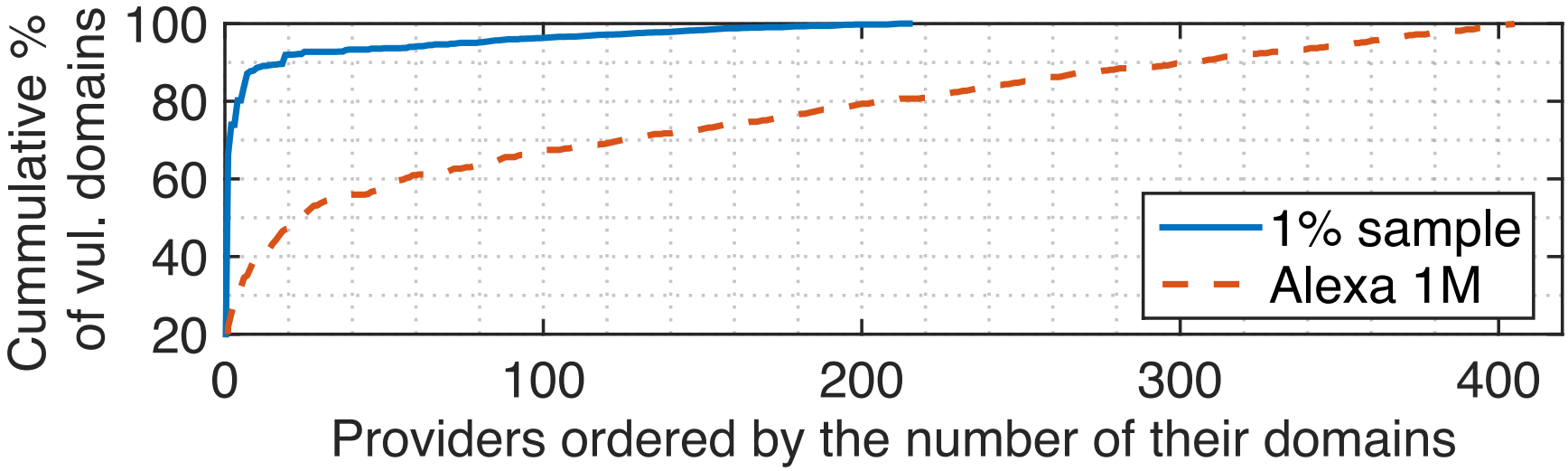
Affected domains

Type	in #	in %
Business	181	31
Entertainment	92	15.7
Educational	90	15.3
Governmental	56	9.5
News services	41	7
Adult	13	2.2
Financial services	9	1.5
Health care	8	1.4
Other	95	16.2
Total	587	100

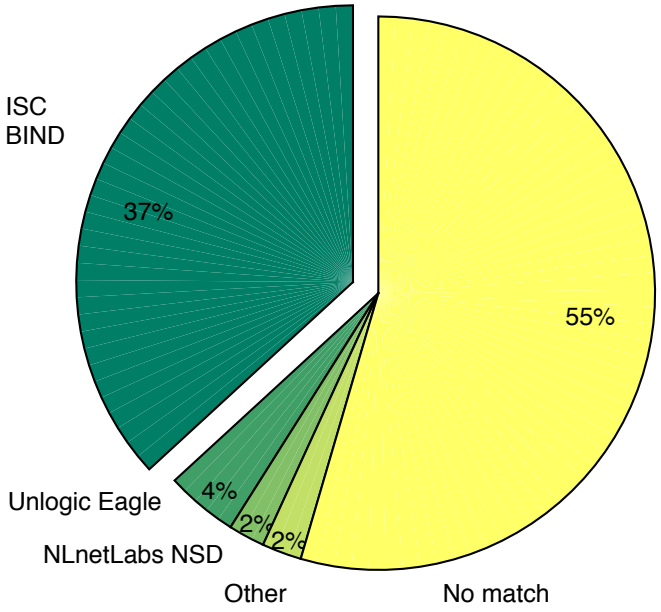
Affected domains

Type	in #	in %
Business	181	31
Entertainment	92	15.7
Educational	90	15.3
Governmental	56	9.5
News services	41	7
Adult	13	2.2
Financial services	9	1.5
Health care	8	1.4
Other	95	16.2
Total	587	100

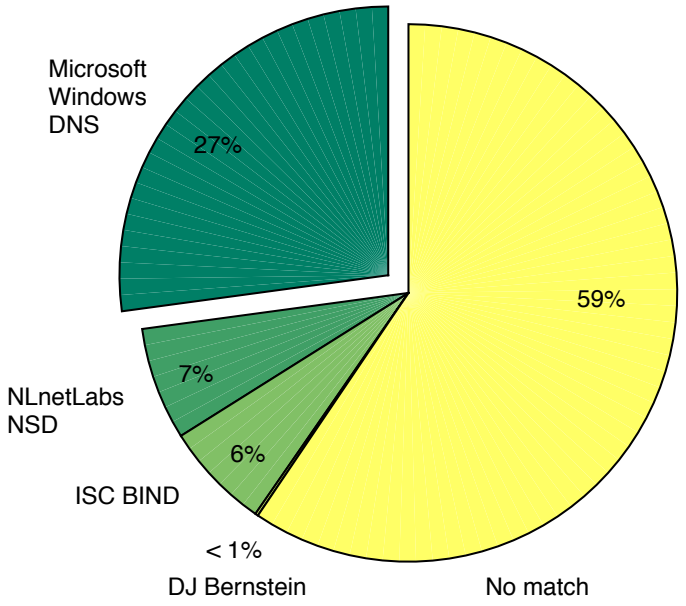
Domain distribution over providers



Implementation distribution



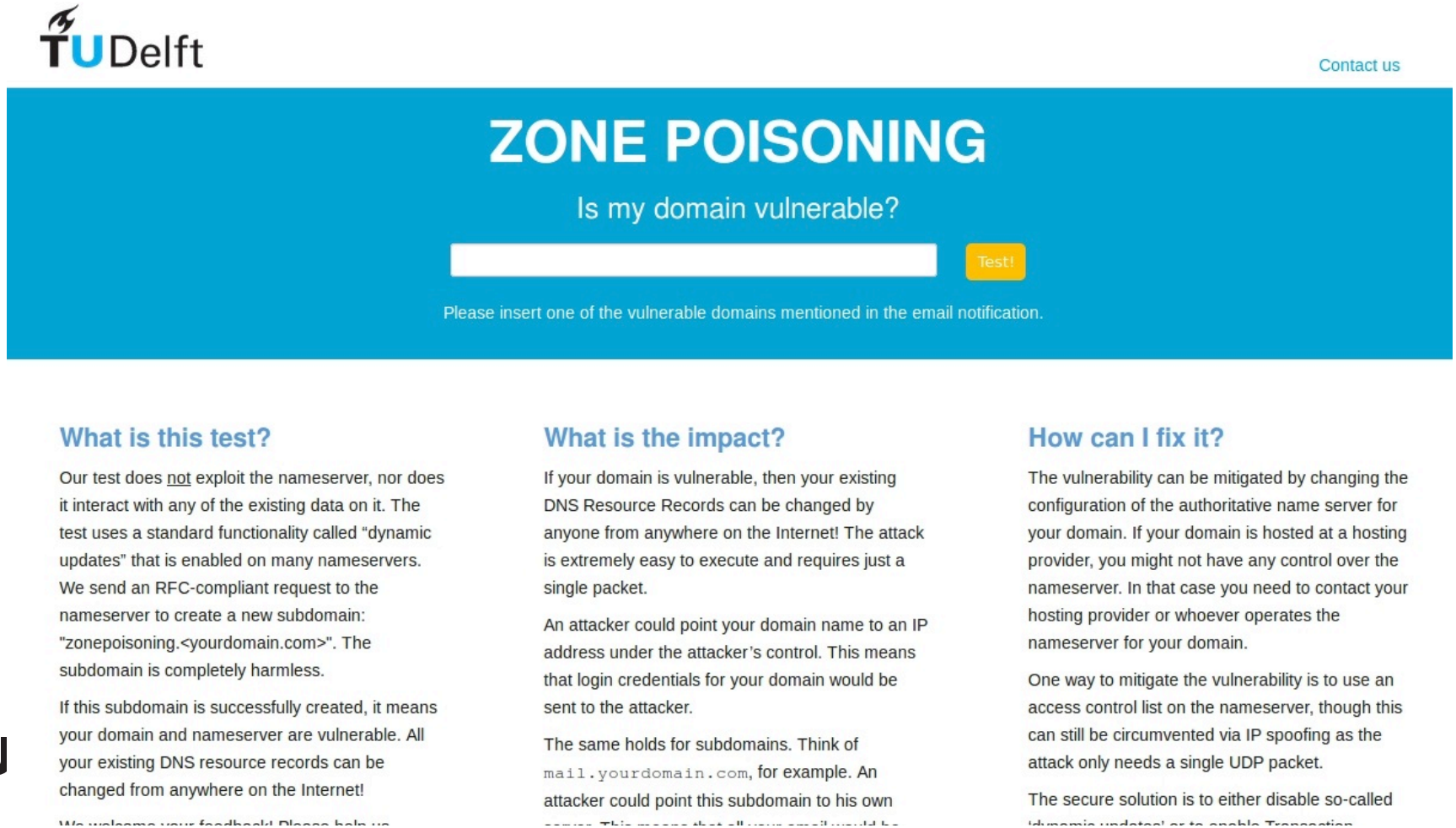
All servers



Vulnerable servers

Notifications

- After the first global scan we sent notifications to DNS service providers, website owners, network operators
- Notifications with demonstrative content (external link demonstrating an existence of the vulnerability) vs. standard vulnerability notification



Notifications *

- Contact information is extremely unreliable
- RFC standards are widely ignored

  (SOA RNAME, `abuse@domain, hostmaster@domain`)
- Network operators are more reachable
- Notifications did lead to more remediation than in the control groups
- Overall remediation rates were low
- Remediation did not improve when a website was provided with a live demonstration of the vulnerability

* "Make Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning", Orcun Cetin, Carlos Ganan, Maciej Korczyński and Michel van Eeten, *WEIS 2017*, La Jolla CA, June 2017

Notifications *

- Contact information is extremely unreliable
- RFC standards are widely ignored

  (SOA RNAME, `abuse@domain, hostmaster@domain`)
- Network operators are more reachable
- Notifications did lead to more remediation than in the control groups
- Overall remediation rates were low
- Remediation did not improve when a website was provided with a live demonstration of the vulnerability

- Please help us to remediate the problem!

* "Make Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning", Orcun Cetin, Carlos Ganan, Maciej Korczynski and Michel van Eeten, *WEIS 2017*, La Jolla CA, June 2017

Ongoing work

- Notifications
- Measurements and analysis
  - Short-lived domains
  - Propagation analysis
  - Global scan of subdomains
  - Exploitation

Conclusions

- Overlooked and still existing problem (since 1997)
- Relatively low percentage of affected hosts but multiple important services
- Zone poisoning: simple and scalable
- Not many complaints received
- Simply by forcing TCP the efficiency of the attack decreases
- Help us to remediate the problem

Acknowledgments

Authors thank Paul Vixie and Farsight Security for sharing DNSDB, Jeroen van der Ham (NCSC), Jelte Jansen, Moritz Muller and Marco Davids (SIDN) for their constructive and valuable comments.

This work was supported by SIDN, the .NL Registry and by NWO.

Questions?

maciej.korczynski@tudelft.nl

TU Delft