Zone Poisoning and GDPR

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

Grenoble Institute of Technology, UGA
maciej.korczynski@univ-grenoble-alpes.fr

TechDay@ICANN63, Barcelona

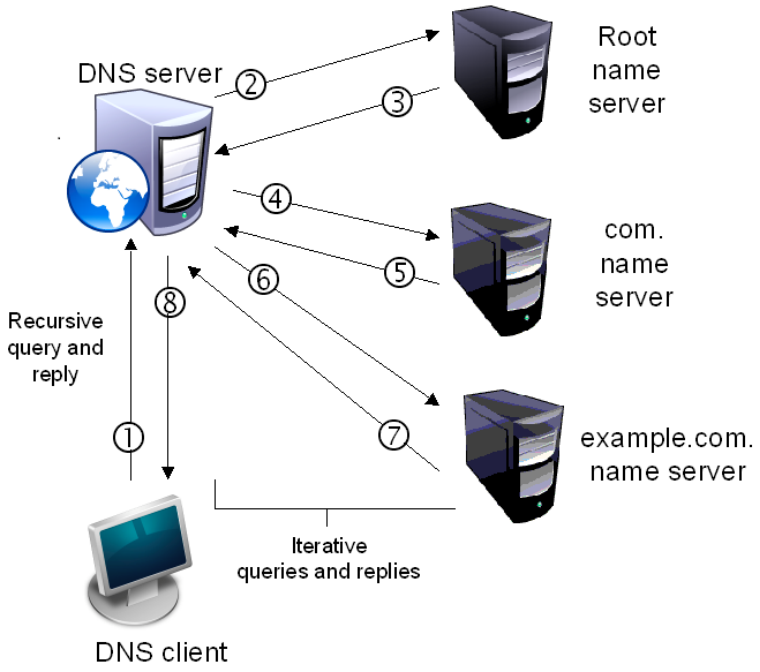
22 October 2018

Agenda

- Attacks against DNS name resolution path
- What is zone poisoning?
- Root problem: misconfigured *dynamic updates in DNS*
- Zone poisoning (requirements, specifics, threats, demo)
- Global measurement
- Affected domains and DNS servers
- Notifications
- Conclusions

Attacks against DNS name resolution path

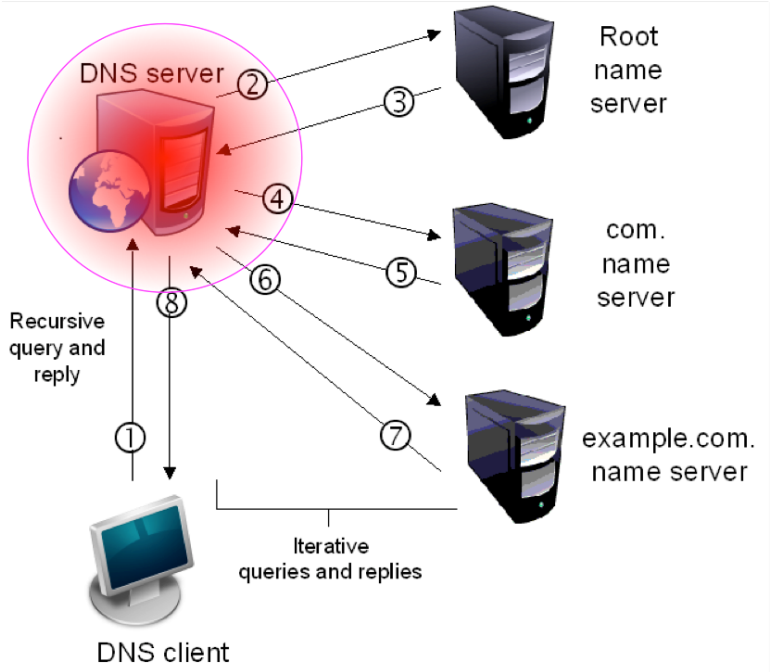
- Most attacks compromise the resolution path somewhere between the user and the authoritative name server for a domain



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

Attacks against DNS name resolution path

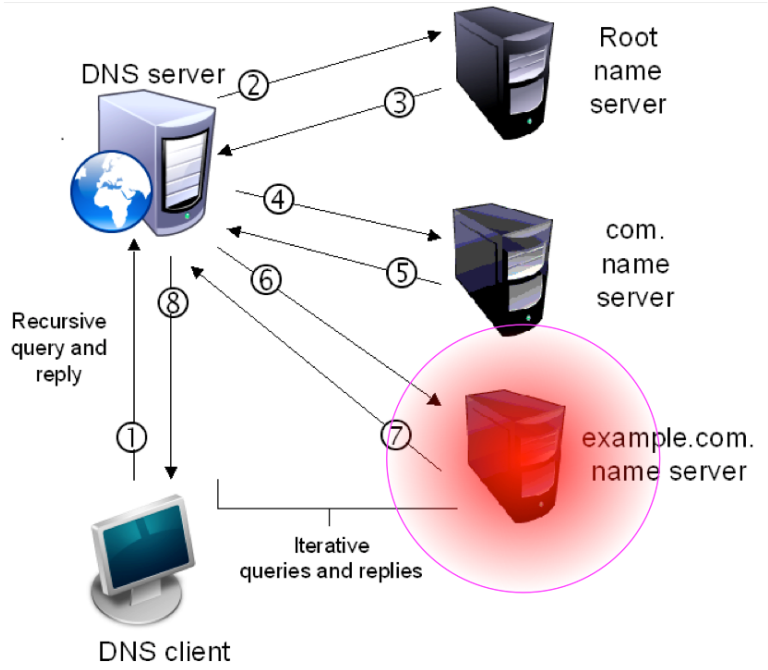
- Most attacks compromise the resolution path somewhere between the user and the authoritative name server for a domain
  - E.g. Traditional cache poisoning attacks or attacks against individual clients being directed to use a rogue DNS server *



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

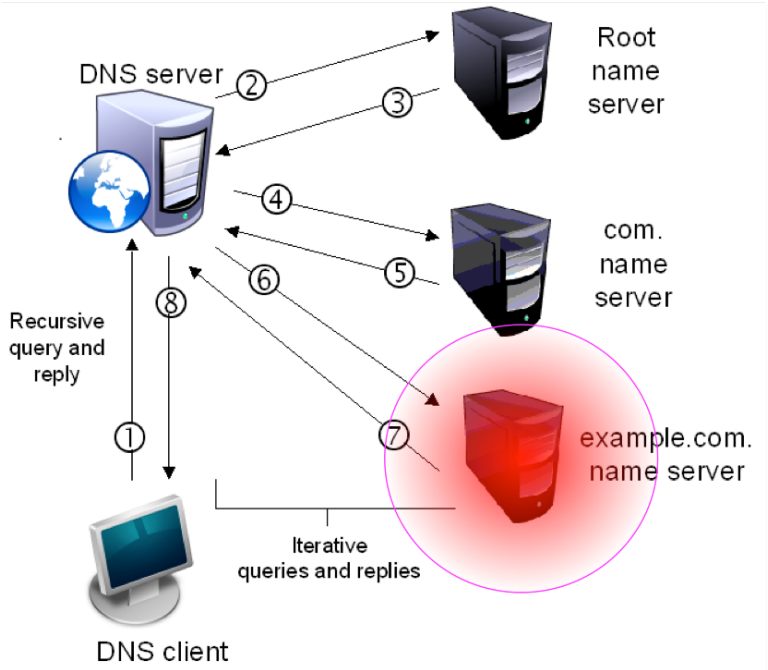
Attacks against DNS name resolution path

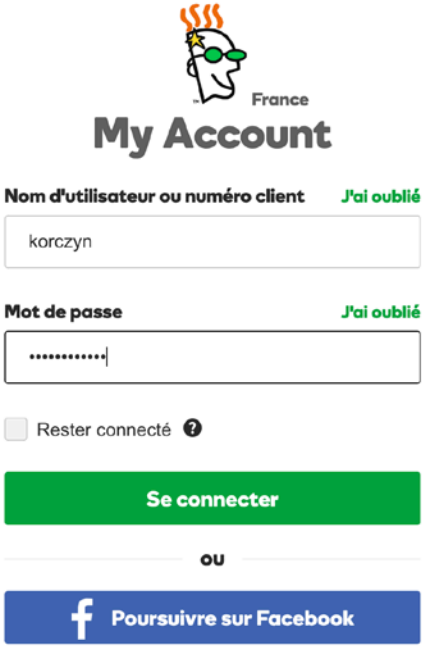
- What about attacks against the authoritative end of the path (authoritative DNS servers)?



Attacks against DNS name resolution path

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

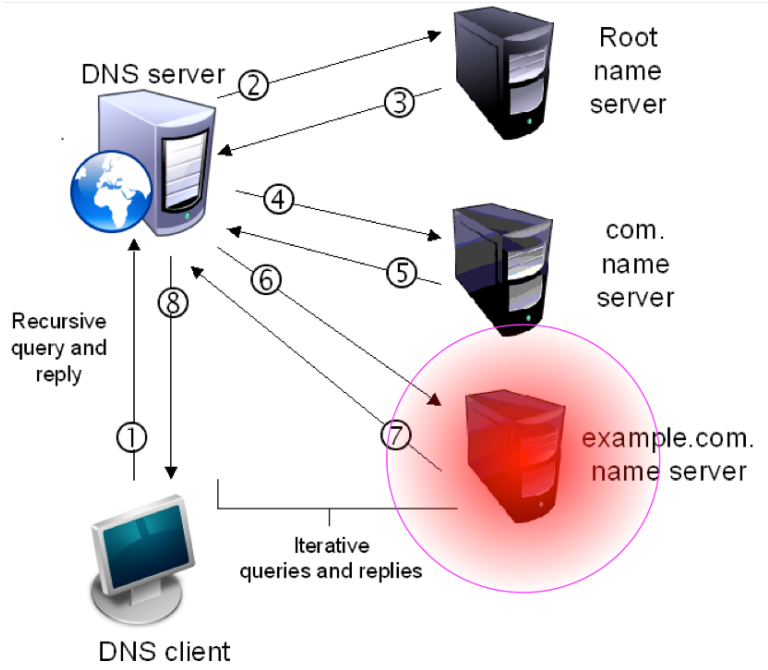




Attacks against DNS name resolution path

- What about attacks against the authoritative end of the path (authoritative DNS servers)?
  - 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
    - ...

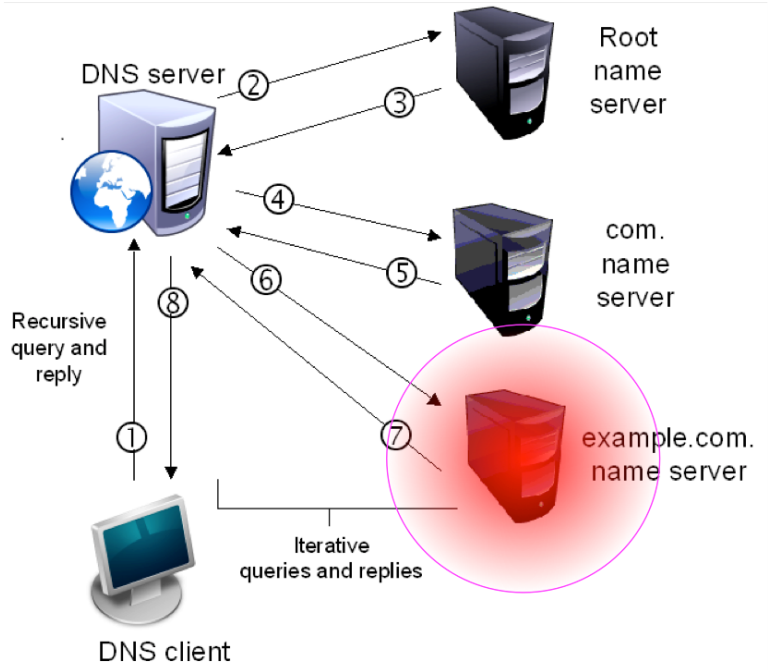


* Biasini, N., and Esler, J. Threat Spotlight: Angler Lurking in the Domain Shadows. http://blogs.cisco.com, March 2015.

Attacks against DNS name resolution path

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

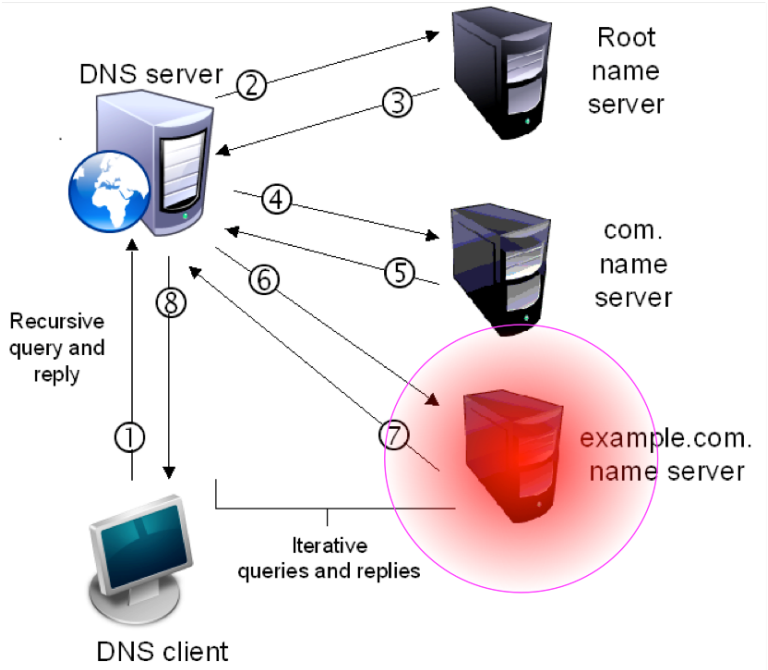
E.g. Twitter and New York Times websites replaced in August 2013



* 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

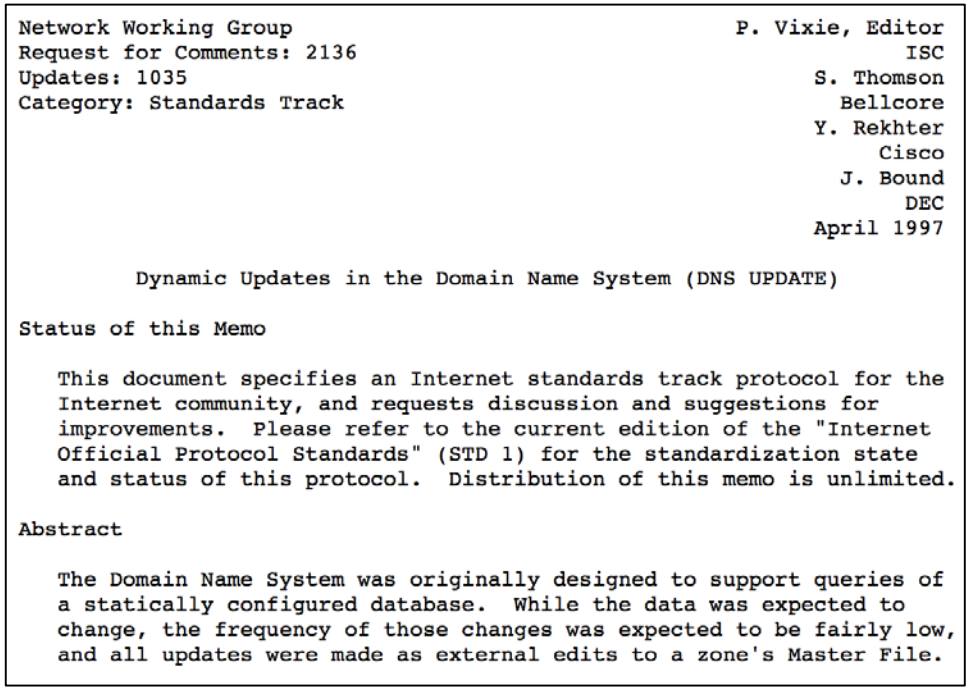
- We explore an attack against the authoritative end of the path: the zone file of the authoritative name server using **non-secure DNS dynamic update** protocol extension *



* "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

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 — P. Vixie, Editor, ISC
Request for Comments: 2136
Updates: 1035 — S. Thomson, Bellcore
Category: Standards Track — 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, and all updates were made as external edits to a zone's Master File.

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
- Previous state restored on all servers
- Website reference in the added record
- Opt-out mechanism
- Notifications

Datasets

- Alexa top 1 Million domains
- Other datasets
  - DNSDB (Farsight Security*)
  - Project Sonar Data Repository**
  - Zone files

* https://www.farsightsecurity.com
** https://scans.io

Affected domains and name servers

- 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)
- Second global scan (February 2017)

- All campaigns:
  - 5 Billion packets
  - **752,511** A RR
  - **7,333** name servers
  - **418,573** domains (2nd level domains and subdomains)

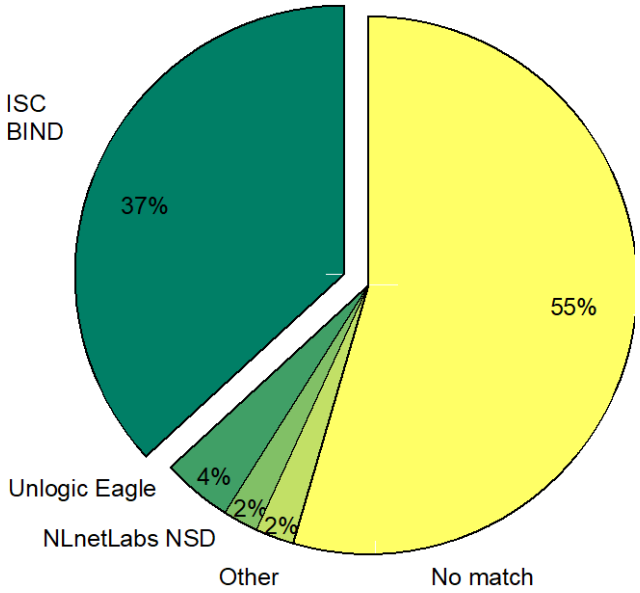
Affected domains

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

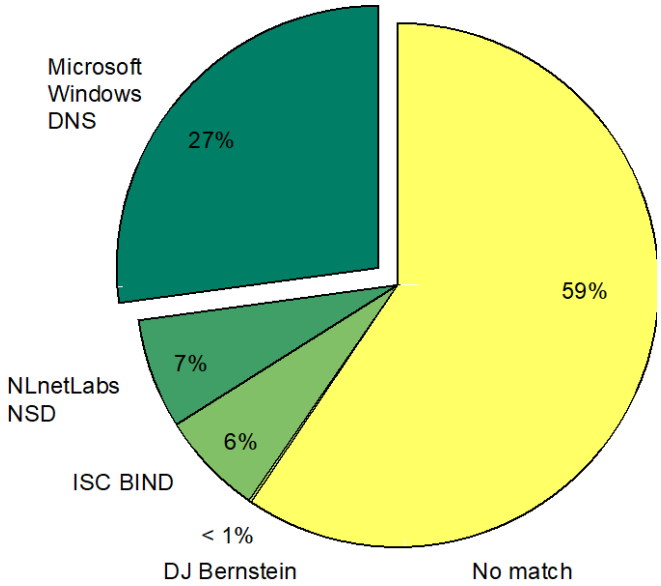
Affected domains

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

Servers: implementation distribution



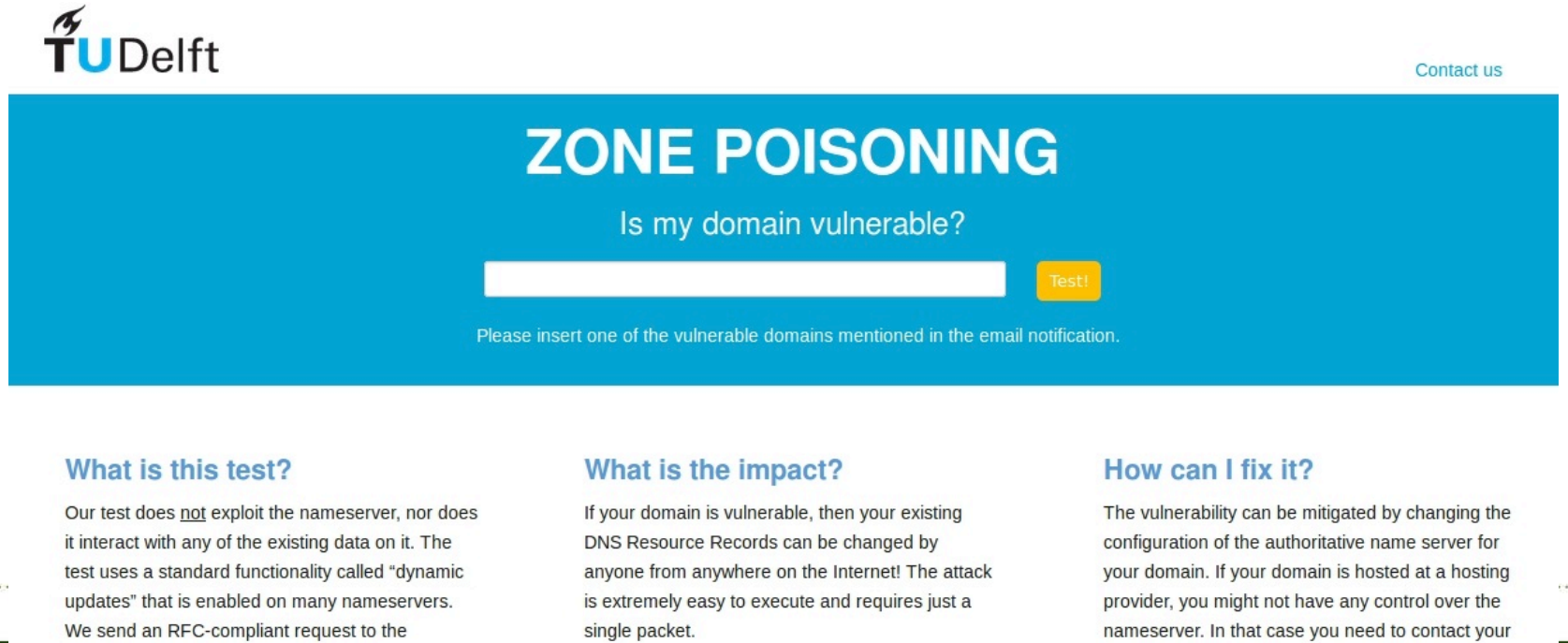
All servers



Vulnerable servers

Notifications

- After the first global scan we sent notifications to:
  - DNS service providers (DNS SOA records)
  - Generic email addresses (`abuse@domain, hostmaster@domain`)
  - Website owners (domain WHOIS)
  - network operators (IP WHOIS)
- Notifications with demonstrative content (external link demonstrating an existence of the vulnerability) vs. standard vulnerability notification



Notifications

- Obtaining WHOIS data at scale is a problem
- Contact information is extremely unreliable
  - 40% of emails to domain owners, failed to be delivered (registrant WHOIS)
- RFC standards are widely ignored
  - 70% of the emails sent to the persons responsible for the name servers (DNS SOA RNAME), affected by zone poisoning, failed to be delivered
  - 84% of the messages to generic emails (`hostmaster@domain`, `abuse@domain`) generated a delivery failure.
- Network operators are more reachable
  - 8,6% generated a delivery failure.

* "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

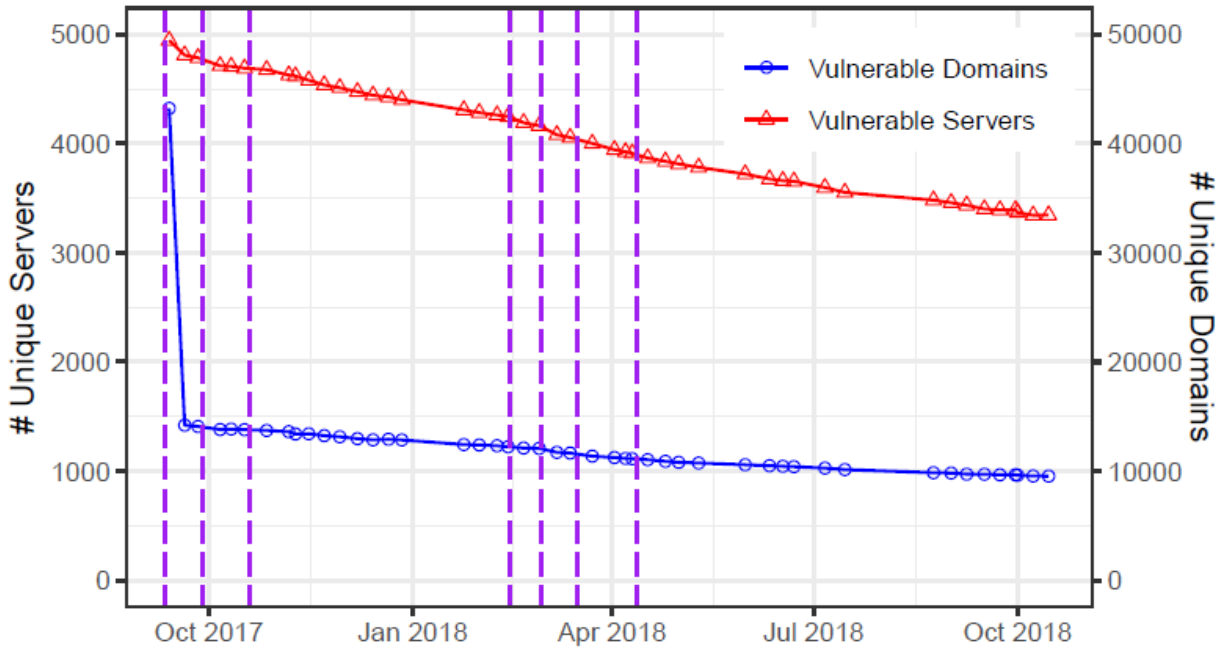
Notifications

- Notifications did lead to more remediation than in the control groups (11% - 18% in comparison to 5% in control group)
- 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

- Ongoing study: notifications to CERTS
- 7 notifications campaigns:
  - 1st -- 3rd campaign targeted to TF-CSIRTs (Task Force on Computer Security Incident Response Teams)
  - 4th -- 7th campaign targeted to National CERTs



Notifications

pierogi.ip-eend.nl/certs

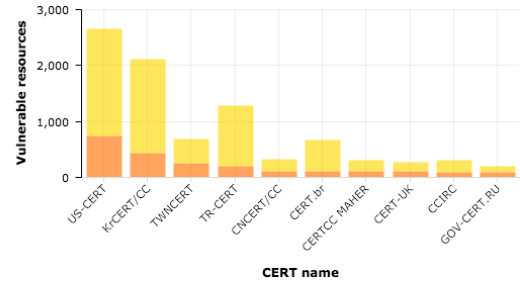
DNS Poisoning: Vulnerable DNS servers

Zone Poisoning | AS overview | CERT overview | Country overview | About us

Vulnerable DNS servers per CERT

Currently, there are more than 2,238 vulnerable DNS servers which put 10,059 domains at risk of being exploited.

Top10 CERTs with the largest amount vulnerable servers



CERT name	Vulnerable servers	Vulnerable domains
US-CERT	733	1924
KrCERT/CC	428	1675
TWNCERT	247	428
TR-CERT	192	1086
CNCERT/CC	110	224
CERT.br	103	561
CERTCC MAHER	101	191
CERT-UK	100	171
CCIRC	95	214
GOV-CERT.RU	82	107

How is your CERT doing?

The following table shows the results of our last scan (14th October, 2018).

Show 10 entries

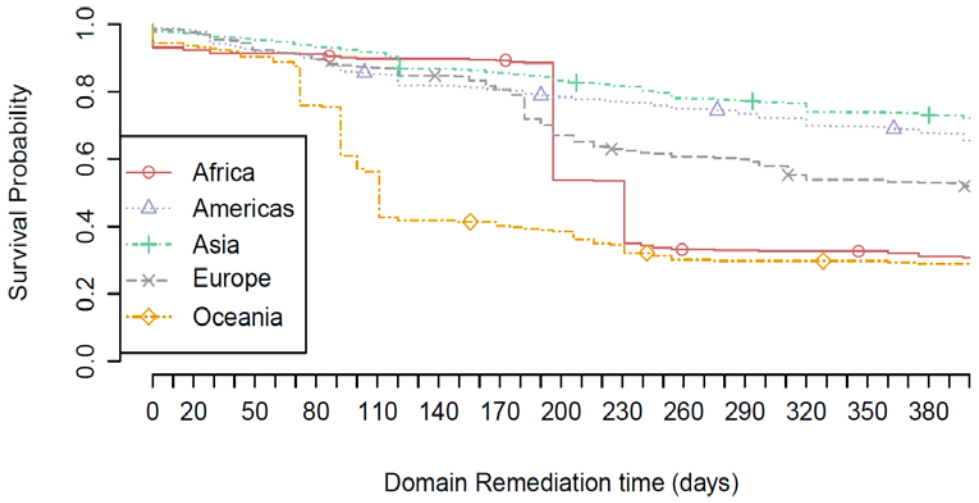
Search:

CERT	Vulnerable servers	Fixed servers	Fixed domains	Vulnerable domains
VNCERT	22	2	9	177
VenCERT	4	0	0	15
UZ-CERT	2	2	5	2
US-CERT	733	212	517	1924
TWNCERT	247	79	175	428
tunCERT	0	1	1	0
TR-CERT	192	46	147	1086
ThaiCERT	59	8	20	101
SWITCH-CERT	17	27	104	215
SingCERT	36	13	25	135

Showing 1 to 10 of 81 entries <>

National CERTs across continents

	Vulnerable domains	Vulnerable servers	Remediated Domains	Remediated Servers
Eastern Asia	2449	860	32000	1194
Northern America	2159	827	3416	1257
Western Asia	1205	247	1506	368
South America	691	210	959	362
South-Eastern Asia	581	182	790	272
Eastern Europe	281	180	655	307
Northern Europe	538	177	829	279
Western Europe	521	158	1090	286
Southern Asia	313	141	707	242
Southern Europe	345	117	623	196
Others	410	206	951	337



Notification campaigns summary

- **752,511** A RR -> **11,912** A RR (remediation: **98,4%**)
- **418,573** domains -> **9,535** (remediation: **97,7%**)
- **7,333** name servers -> **3,345** (remediation: **45,6%**)

Notifications in the context of GDPR

- Available options:
  - Generic email addresses: `hostmaster@domain`, `webmaster@domain`, `abuse@domain` and `security@domain`
    - Very low deliverability
  - Start of Authority (SOA) RNAME field
    - Very low deliverability
  - Through intermediaries (registrars, hosting providers, CERTs)
    - Scalable, better deliverability but requires a lot of effort
  - Web form which messages could be forwarded to the registrant email address
    - Not scalable
  - Anonymized email address forwarded to the registrant email address
    - If implemented correctly

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
- Notifications are hard
- Help us to remediate the problem

Acknowledgments

Many thanks to Paul Vixie and Farsight Security for sharing DNSDB, CERTs for the remediation efforts, Jeroen van der Ham (NCSC), Jelte Jansen, Moritz Muller and Marco Davids (SIDN) for their constructive and valuable comments.

Grenoble INP ENSIMAG

Questions?

maciej.korczynski@univ-grenoble-alpes.fr