Large-scale Analysis of Infrastructure-leaking DNS Servers

Dennis Tatang, Carl Schneider, Thorsten Holz

Ruhr-University Bochum, Germany

Motivation

- DNS: www.rub.de ➡ 134.147.64.10

- Daily use on the Internet by every user
- Various studies: DDoS, Censorship, Measurements
- Overlooked aspect: Leaking DNS servers to external queries with internal network information

Reconnaissance

- Information leakage part of active infrastructure reconnaissance

- Goal: Get as much information as possible about a target network

Contributions

- Measurement approach to find information leaking DNS servers
- Systematic study on DNS servers that might expose internal network information to external requests
- Self-check for identifying information-leaking DNS servers

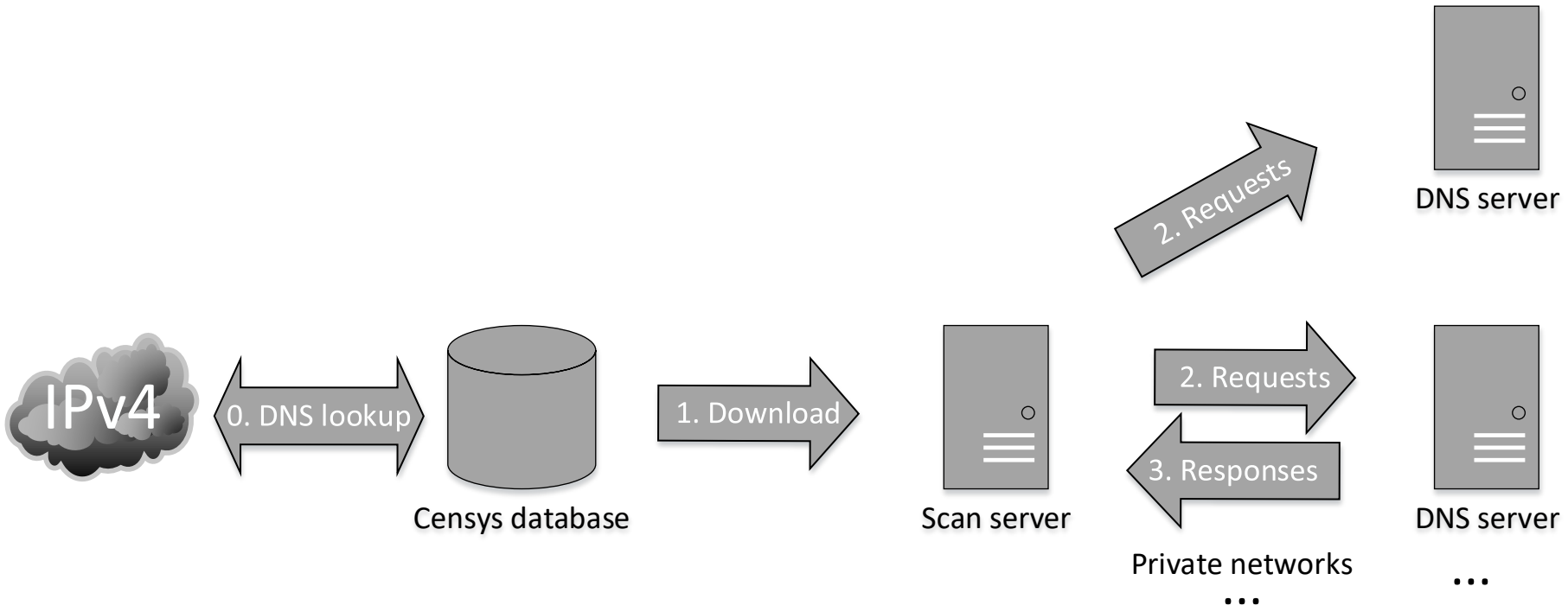
Domain Name System (DNS)

- Distributed, hierarchy-based service
- Primarily responsible for translation of domain names into IP addresses (A, AAAA)
- Reverse lookup (PTR)
- Private IP ranges (*10/8*, *172.16/12*, *192.168/16*)

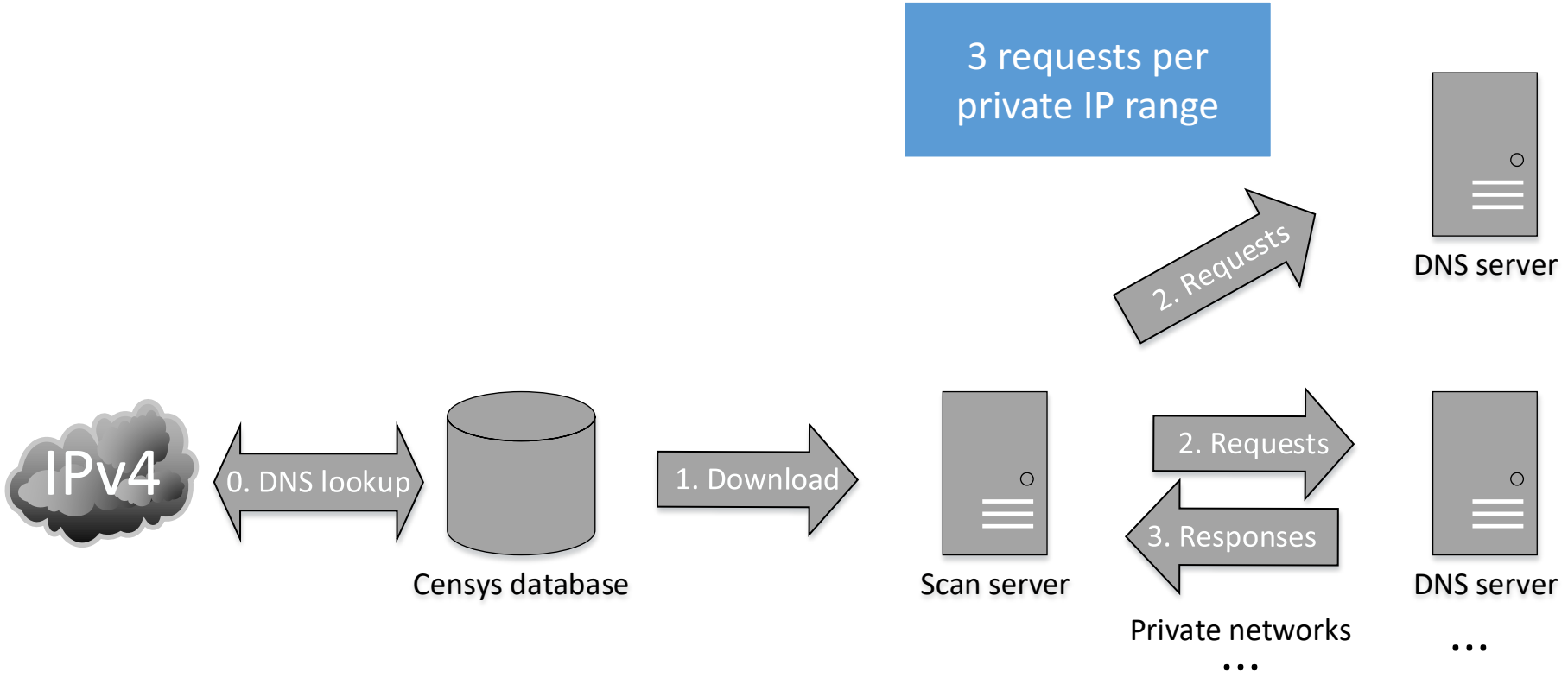
Idea

- Using reverse DNS requests for internal resources on Internet reachable DNS servers

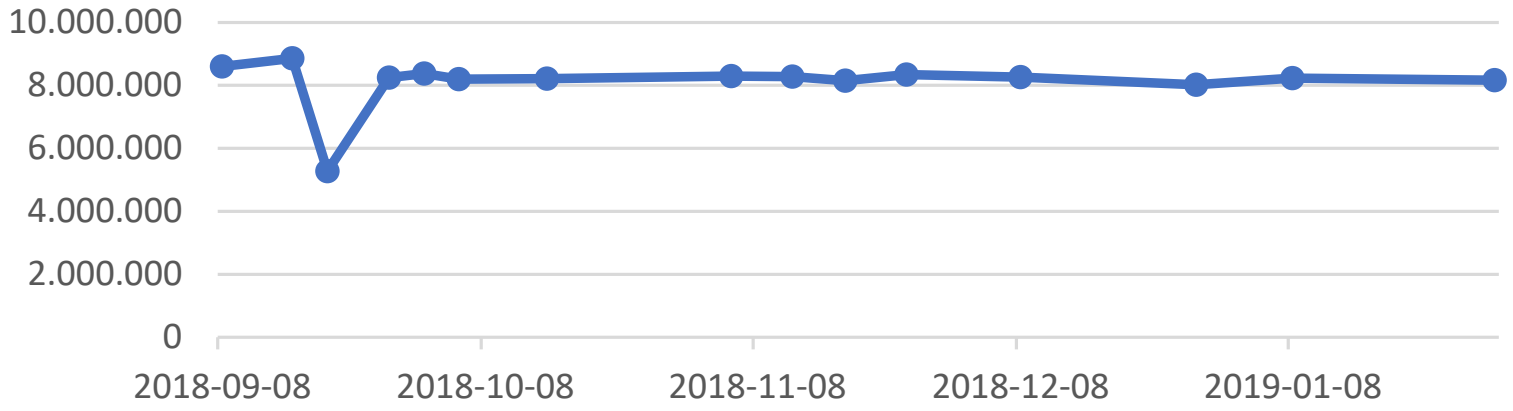
Discovering Leaking DNS Servers

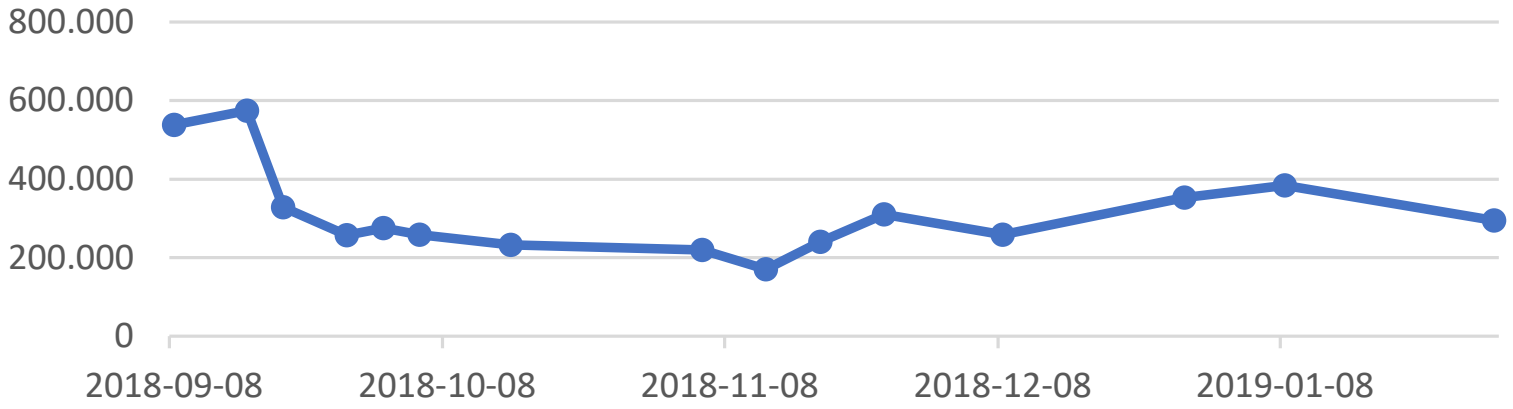


Discovering Leaking DNS Servers



General Measurement Results





Response Groups (1)

Localhost: “localhost.”	*Single*: one host
IP: IP addresses	*Emptyresponse*: “.”
Arpa: Reverse DNS	*Bogon*: “bogon.”
Constant: unique hostname for all hosts	

Response Groups (2)

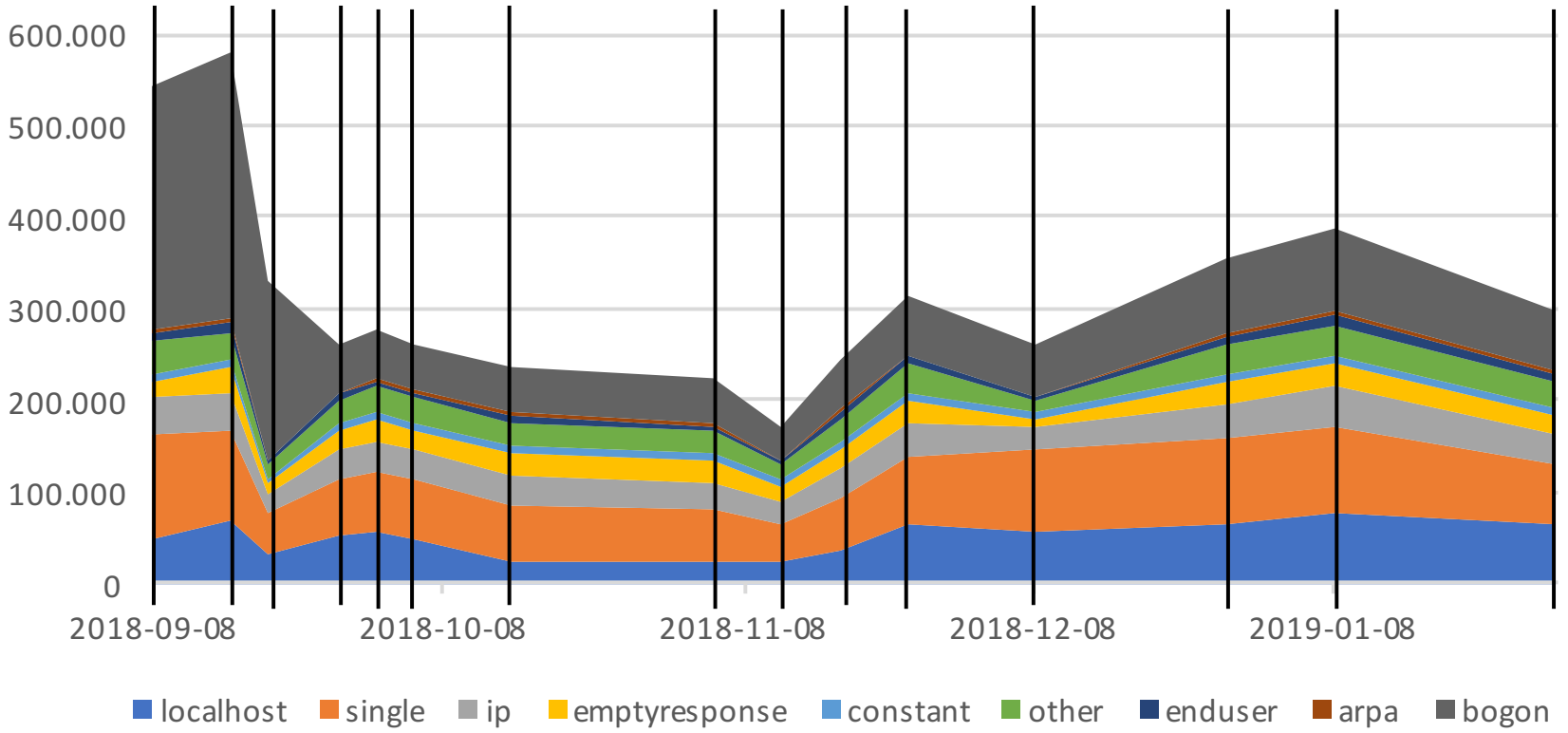
Enduser: Keyword-based	*Other*

- apple, iphone, ipad, samsung, galaxy, home

Response Groups (3)

No information advantage	Active hosts, used subnet	Active hosts, used subnet, hostnames
Bogon		
Localhost		
Emptyresponse		
Constant		
Arpa		
IP	*Single*	*Enduser*
		Other

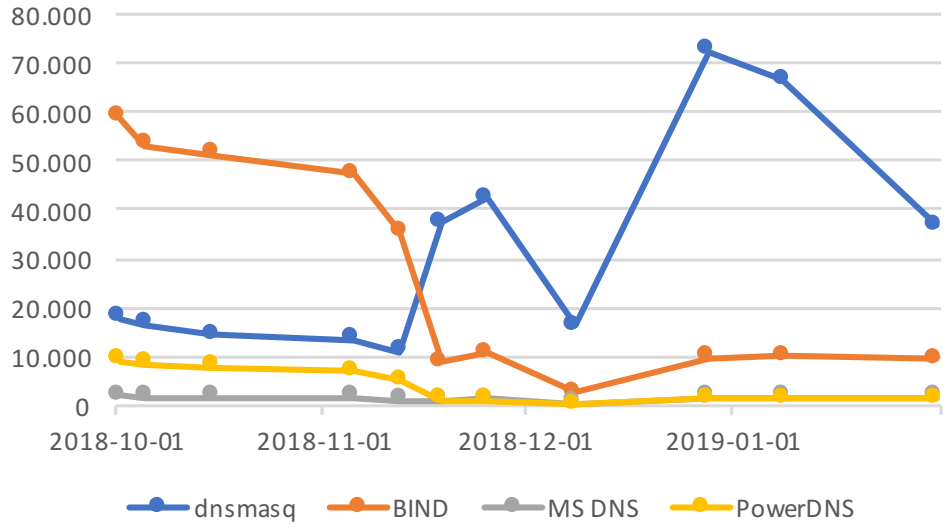
General Measurement Results

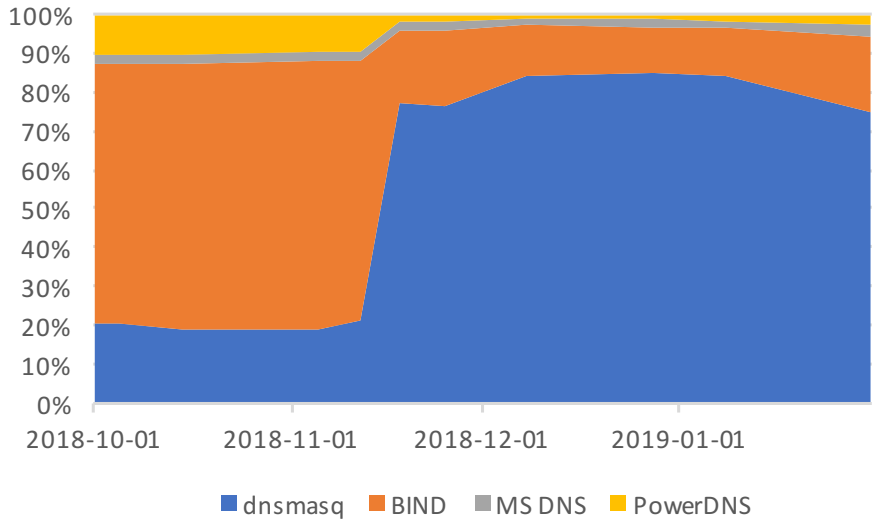


In-depth Analysis

- Daemon information
- AS numbers
- Countries
- Private IP ranges
- Hostname pattern analysis

Daemon Information





AS Numbers & Countries

Horst Görtz Institute for IT-Security

RUB

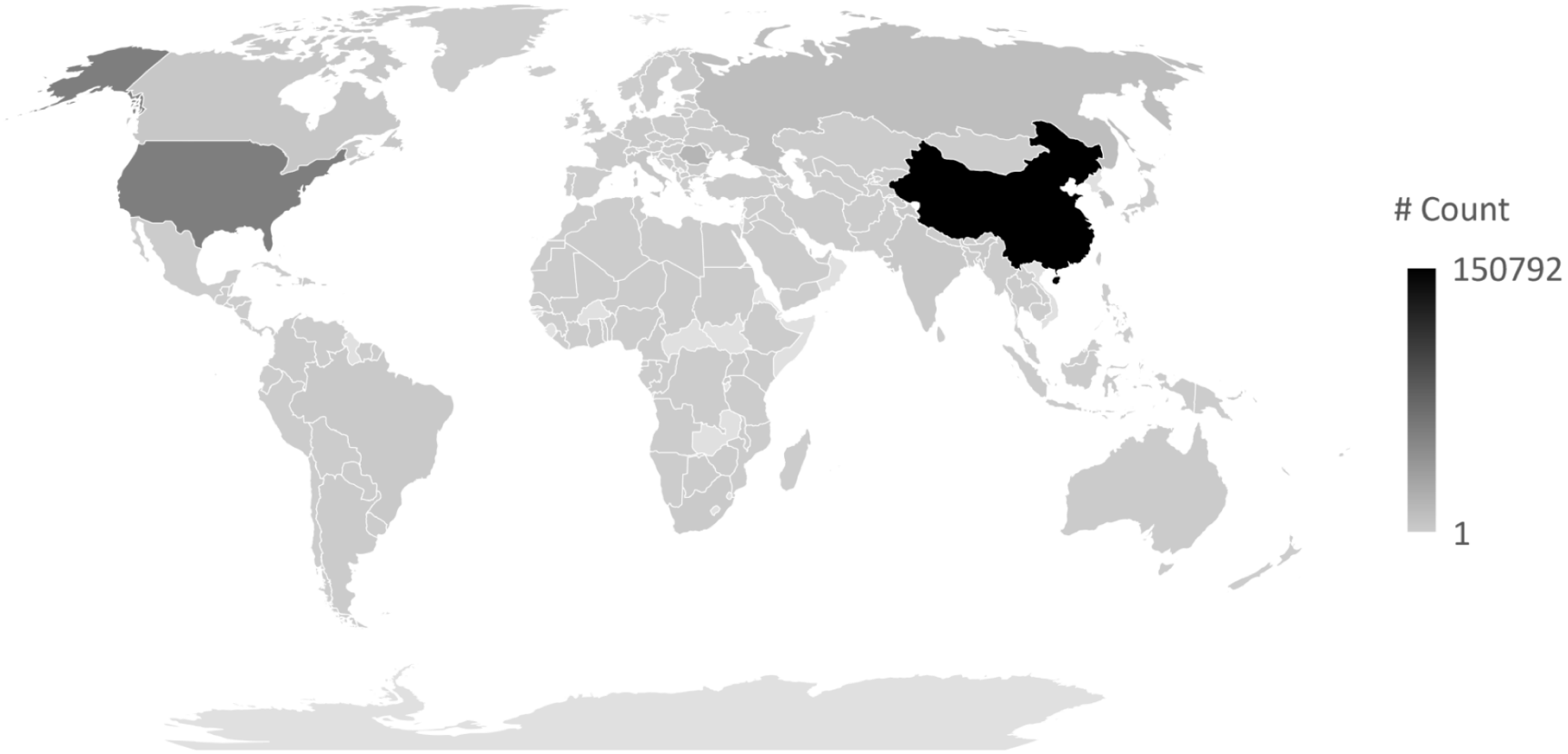
(a) per Country

Country	#Count
China	1,839,099
USA	970,727
Romania	186,677
Russia	178,678
Korea	117,091
Taiwan	111,418
Germany	90,319
Canada	83,352
France	74,729
Italy	70,729

(b) per AS number

ASN	AS Name	#Count
4837	CHINA UNICOM China169 Backbone	592,908
4134	No.31,Jin-rong Street	341,578
9808	Guangdong Mobile Communication Co.Ltd.	244,475
4847	China Networks Inter-Exchange	235,165
8708	RCS & RDS	161,954
209	Qwest Communications Company, LLC	150,003
5650	Frontier Communications of America	120,251
4808	China Unicom Beijing Province Network	110,620
3462	Data Communications Business Group	99,650
9394	China TieTong Telecommunications Corporation	88,032

AS Numbers & Countries



Countries (normalized)

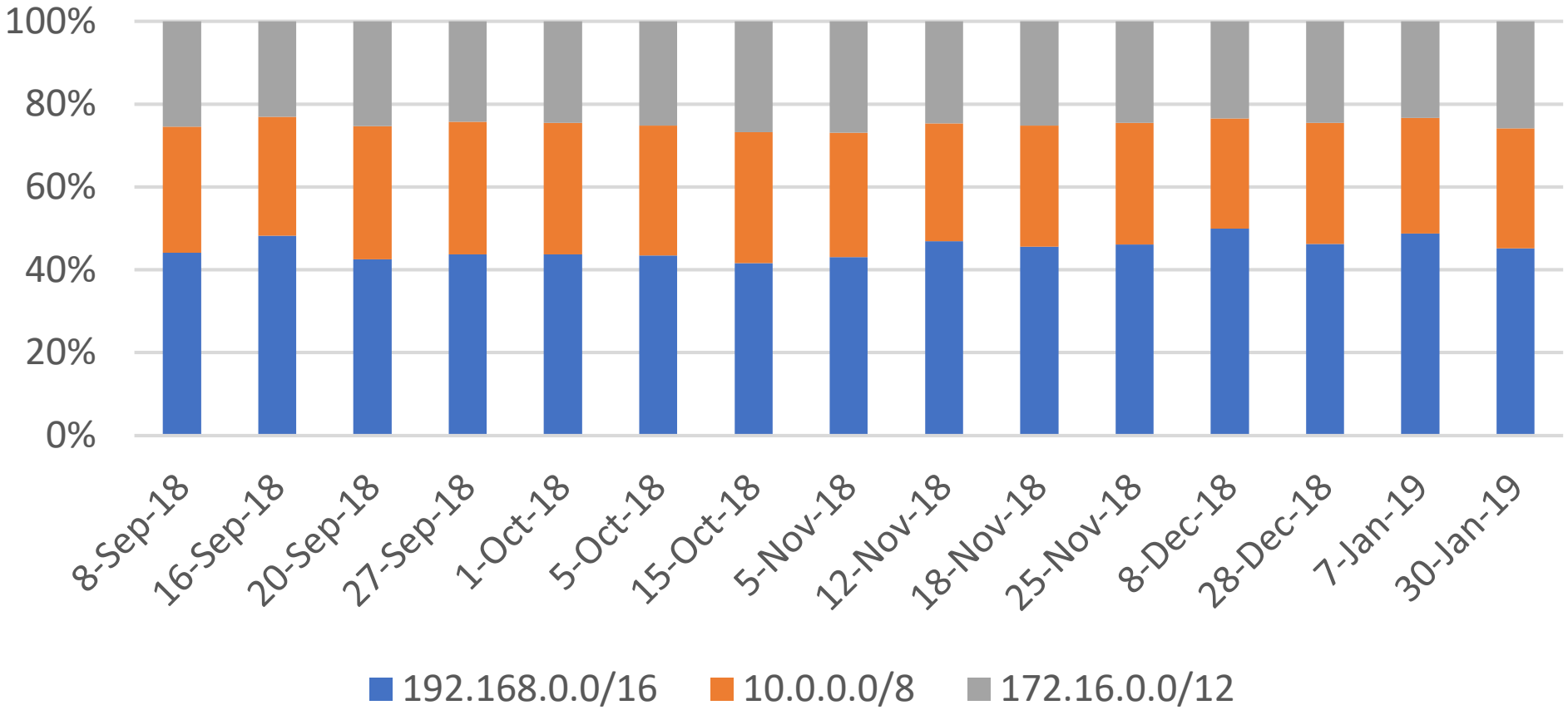
Country	Share	Count
British Virgin Islands	80%	2,533
Macao	41%	898
Comoros	29%	14

Countries (normalized)

Country	Share	Count
British Virgin Islands	80%	2,533
Macao	41%	898
Comoros	29%	14

Country	Share
China	9%
USA	3%
Romania	15%
Russia	3.4%

Private IP Ranges



Hostname Pattern Analysis

(a) Group: *enduser*

Hostname	#count
Broadcom.Home.	64,698
.	37,545
iPhone.	8,127
192.168.0.2	5,895
Cisco.Home.	5,183
Comtrend.Home.	4,437
192.168.0.3	4,316
qwestmodem.domain.	3,958
modem.domain.	2,842
192.168.0.4	2,455

(b) Group: *other*

Hostname	#count
bogon.	335,676
localhost.	115,470
ospd-gw.ospd.net.	50,354
tatina.ospd.net.	50,077
red.ospd.net.	48,997
T2.primorye.net.ru.	42,763
www.routerlogin.com.	37,786
AdtranTA924ATA	34,653
.	14,551
ntweb1.megawebservers.com.	13,927

Hostname Pattern Analysis

Example Hostname Patterns

- *<placeholder>.iPhone, <placeholder>.iPad*
- *android-<placeholder>*
- *amazon-<placeholder>*
- *<placeholder>desktop, <placeholder>-PC*

- Other:
  - *firewall<placeholder>, <placeholder>.dmz*

Mitigation & Self-Check

Horst Görtz Institute for IT-Security

RUB

DNS Information leakage

This page allows you to check your network for potential DNS information leakage.

To do so, it will issue rDNS requests for all local IP addresses that are within the /24 range of the given IP.

While this test should typically not disturb any running services, the author does not take any responsibilities for damage on your services.

The test might take some time, so please be patient when waiting for the results

---

Self-check

Your external IP: 127.0.0.1

Your local IP (This is used to determine the targeted subnet): 192.168.0.38

☐ I am allowed to perform tests on this network

Submit

Example output

Scanning for hosts in subnet 192.168.0.0/24 on DNS Server **redacted**

Daemon version: dnsmasq-2.55;

If the following list contains any valid hostname that is part of your local network, you are probably affected by a DNS information leakage

IP	Hostname
192.168.0.1	**redacted**.lan.
192.168.0.2	iPhone**redacted**.lan.
192.168.0.14	android-**redacted**.lan.
192.168.0.35	HUAWEI_Y6_Pro_2017.lan.
192.168.0.47	android-**redacted**.lan.
192.168.0.48	HUAWEI_P_smart-**redacted**.lan.
192.168.0.64	**redacted**-PC.lan.
192.168.0.76	**redacted**.lan.
192.168.0.82	220SFNw-**redacted**.lan.
192.168.0.99	Galaxy-J5.lan.

Discussion

- Share is about 3.9% - Absolute numbers up to 574,000 servers
  - Proper information leakage present with up to 158,000 servers
- No implementation problem but rather a configuration problem
- Number of potentially usable leaking DNS servers highest in the USA

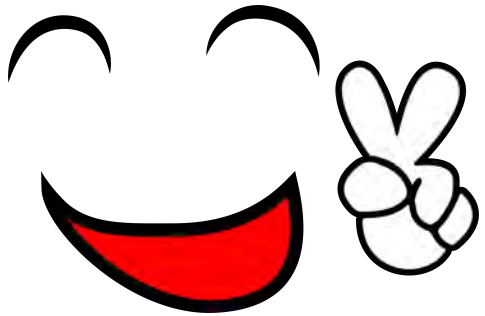
Conclusion

- Observed that misconfigured DNS servers might leak internal information to external intruders without the need for an exploit or vulnerability (configuration issue)
- Almost 4% of the DNS servers might leak such information
- Not a major Internet security problem, but the absolute numbers should be reduced
- Data at https://github.com/RUB-SysSec/InfraLeakingDNS

Questions?

Dennis Tatang

dennis.tatang@rub.de
@dennis4its on Twitter



Conclusion

- Observed that misconfigured DNS servers might leak internal information to external intruders without the need for an exploit or vulnerability (configuration issue)
- Almost 4% of the DNS servers might leak such information
- Not a major Internet security problem, but the absolute numbers should be reduced
- Data at https://github.com/RUB-SysSec/InfraLeakingDNS