Open DNS Resolvers Report

A scan report on your network or constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

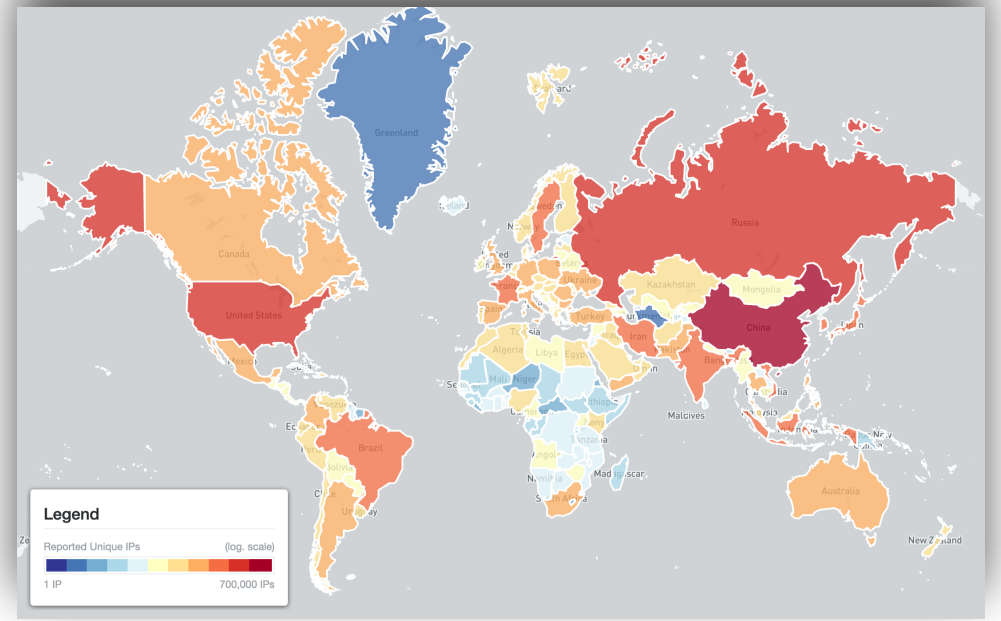
Presentation Aims & Objectives

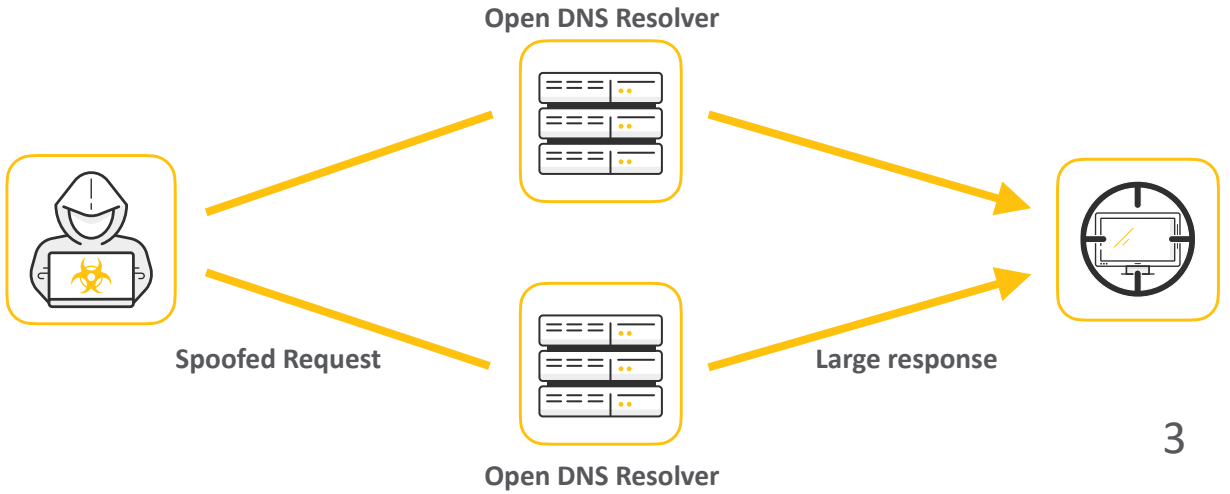
- Introduce Open DNS Resolvers
- Introduce Shadowserver scans and methodology
- Highlight a sample Open DNS report
- Describe key features of the report
- Demonstrate how a National CERT can action an Open DNS report
- Offer guidance on how to protect and secure Open DNS
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

Open DNS Resolvers - Summary

- Domain Name System (DNS) translates domain names to IP addresses so browsers can load Internet resources
- Each device connected to the Internet has a unique IP address which other machines use to find a device
- An "open DNS resolver" is a DNS server that resolves recursive DNS lookups for anyone on the internet
- A simple lack of authentication allows malicious actors to propagate DNS amplification attacks and flood victim sites with fake DNS lookup requests, making them inaccessible





SHADOWSERVER

Internet-wide Scanning

- Shadowserver scans the entire IPv4 Internet for 70 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols

- These are primarily "hello" type port/application scans

- Shadowserver does not exploit any vulnerability

- Scans allow for identifying misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or are simply just population enumeration

- Read more on why we scan at: https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/

SHADOWSERVER

Internet-wide Scanning - Open DNS

- A project to search for publicly available recursive DNS servers
- The goal of this project is to identify DNS servers that will send a reply to any IP address for domains that the DNS server is not authoritative for and report them back to the network owners for remediation
- These servers have the potential to be used in DNS amplification attacks and if at all possible, we would like to see these services made un-available to attackers that would abuse these resources
- We are querying all computers with routable IPv4 addresses that are not firewalled from the internet on port 53/udp with a request for the "A" record of "dnsscan.shadowserver.org", capturing the response from the DNS server and parsing the result
- For an overview of UDP DNS amplification attacks please read: https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

SHADOWSERVER

Open DNS Resolvers Report

- Report is available as a file in CSV format
- The report filename contains `scan_dns`
- Reports can be sent as e-mail attachments, or downloaded via HTTP or obtained via a RESTful API
- All timestamps are in UTC
- For more documentation on API access, please visit the below URLs and send a request for access to contact@shadowserver.org
  https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
  https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

Open DNS Resolvers Report Example

DNS Open Resolvers Report

This report identifies DNS servers that have the potential to be used in DNS amplification attacks by criminals that wish to perform denial of service attacks.

FIELDS

timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides
port	Port that the DNS response came from
protocol	Protocol that the DNS response came on (usually UDP)
hostname	Reverse DNS name of the device in question

SAMPLE

```
"timestamp","ip","asn","geo","region","city","port","protocol","hostname","min_amplifica
"2013-10-10 00:05:10","208.70.149.107","36252","US","Illinois","Chicago","53","udp","107
"2013-10-10 00:05:10","204.245.210.223","2914","US","Oregon","Warren","53","udp","","1.3
"2013-10-10 00:05:10","40.135.0.109","7029","US","Nebraska","Pawnee City","53","udp","h1
"2013-10-10 00:05:10","76.74.186.178","13768","CA","British Columbia","Richmond","53","u
"2013-10-10 00:05:10","31.42.105.195","51003","RU","-","-","53","udp","","1.3810","dnsma
```

https://www.shadowserver.org/what-we-do/network-reporting/dns-open-resolvers-report/

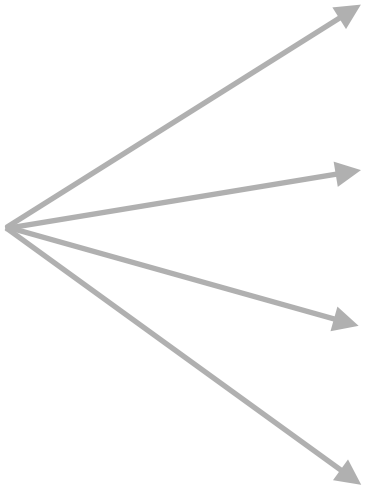
https://scan.shadowserver.org/dns/

SHADOWSERVER

Action an Open DNS report

timestamp	IP	asn	geo	region	city	port	protocol	Hostname
05/03/2022 00:02	220.118.230.XX	4766	KR	SEOUL TEUGBYEOLSI	SEOUL	53	UDP	XXX

Key event fields



timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides
port	Port that the DNS response came from
protocol	Protocol that the DNS response came on (usually UDP)
hostname	Reverse DNS name of the device in question

SHADOWSERVER

Action an Open DNS report

timestamp	IP	asn	geo	region	city	port	protocol	Hostname
05/03/2022 00:02	220.118.230.XX	4766	KR	SEOUL TEUGBYEOLSI	SEOUL	53	UDP	XXX

IP WHOIS
220.118.230.XX

```
inetnum:        220.116.0.0 - 220.127.255.255
netname:        KORNET
descr:          Korea Telecom
admin-c:        IM667-AP
tech-c:         IM667-AP
country:        KR
status:         ALLOCATED PORTABLE
mnt-by:         MNT-KRNIC-AP
mnt-irt:        IRT-KRNIC-KR
last-modified:  2017-02-06T02:32:51Z
source:         APNIC

irt:            IRT-KRNIC-KR
address:        Jeollanam-do Naju-si Jinheung-gil
e-mail:         irt@nic.or.kr
abuse-mailbox:  irt@nic.or.kr
admin-c:        IM574-AP
tech-c:         IM574-AP
auth:           # Filtered
remarks:        irt@nic.or.kr was validated on 2020-04-09
mnt-by:         MNT-KRNIC-AP
last-modified:  2021-06-15T06:21:49Z
source:         APNIC
```

SHADOWSERVER

Verifying our results

- The scan results may contain false positives if an actor attempts to spoof UDP replies to our scans

- In some cases when hosts have multiple interfaces we may register a scan response from another interface with another IP, but report it out as the IP we scanned for

- If you would like verify our results and to see if your server supports open recursion, try using the command: "dig +short @[IP] dnsscan.shadowserver.org" from computer that does **not** use the IP listed in the command as it's authoritative DNS server. If the device does support open recursion, you should see the IP address of dnsscan.shadowserver.org returned as the result.
    - Make sure your queries are not being filtered

- Remember the scan results we share are for the previous day (up to 24 hour delay)

SHADOWSERVER

Open DNS - PROTECT

- Implement BCP38 also known as “Network Ingress Filtering”
- DNS queries from a trusted source to tighten server security
- Implementing Source IP verification on a device
- Response Rate limiting (RRL) settings settings on DNS Servers
- Disabling Recursion on Authoritative Name Servers
- Limiting Recursion to Authorised Clients

SHADOWSERVER

Summary & Key Report Pages

Reports overview

- https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
- https://www.shadowserver.org/what-we-do/network-reporting/
- https://www.shadowserver.org/what-we-do/network-reporting/dns-open-resolvers-report/

Report Updates

- https://www.shadowserver.org/news-insights/
- Twitter @shadowserver
- Mailing list access send request to contact@shadowserver.org and request access to public@shadowserver.org
- Or subscribe directly at https://mail.shadowserver.org/mailman/listinfo/public

Reports API

- Request access to contact@shadowserver.org
- https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
- https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG