Open SSDP Report

A scan report on your network or constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

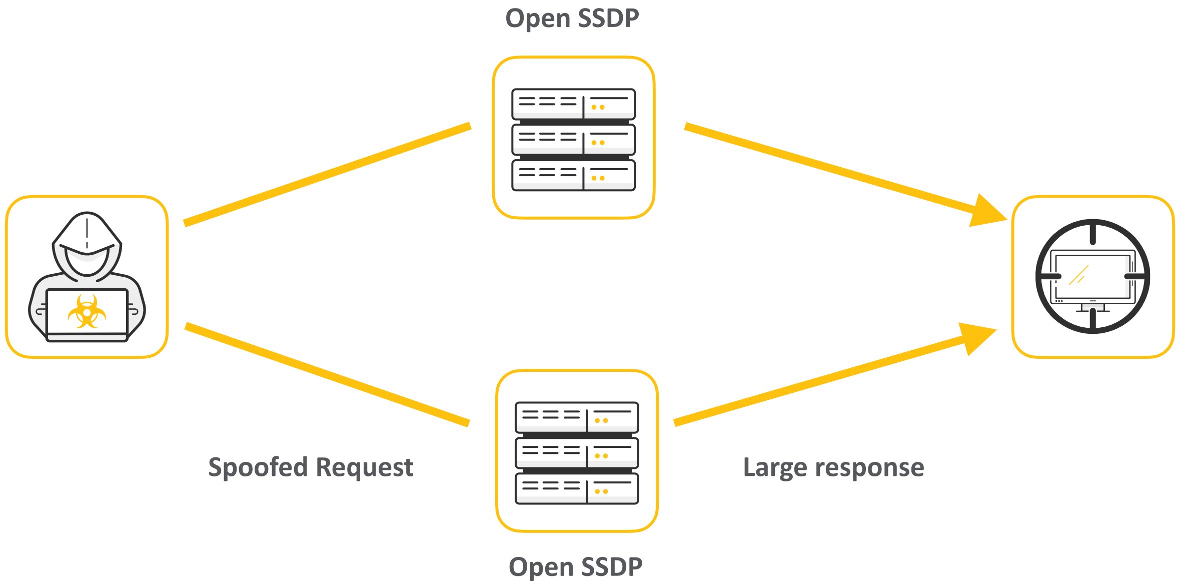
- Introduce what is meant by an Open SSDP service
- Introduce Shadowserver scans and methodology
- Highlight a sample Open SSDP report
- Describe key features of the report
- Demonstrate how a National CERT or network owner can action an Open SSDP report
- Offer guidance on how to protect and secure SSDP
- Provide a key list of Shadowserver online resources to enable report subscription and use

Internet-wide Scanning

- Shadowserver scans the entire IPv4 Internet for over 90 different network protocols every day (as of 2022-04-27), and also performs IPv6 scans based on IPv6 hitlists for selected protocols
- These are primarily "hello" type 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 scans
- Read more on why we scan at: https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/

Open SSDP

- SSDP (Simple Service Discovery Protocol) is deployed in networks for plug-and-play discovery (UPnP)
- Devices receive broadcast messages from other UPnP devices to interconnect, for example IP cameras, routers and Smart TVs
- Publicly exposed SSDP services can be abused for reflection-based distributed denial-of-service attack (DDoS)
- IP address spoofing generates large responses to significantly smaller SSDP network queries, tricking servers to respond and flood the victim with data



Open SSDP

Spoofed Request

Large response

Open SSDP

Internet-wide Scanning - Open SSDP

- A project to search for publicly available Open SSDP servers: https://scan.shadowserver.org/ssdp/
- These servers have the potential to be used in 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 1900/udp SEARCH request and capturing the response
- For an overview of UDP amplification attacks please read:

  https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

Open SSDP Report

- Open SSDP Report: https://www.shadowserver.org/what-we-do/network-reporting/open-ssdp-report/

- Report is available as a file in CSV format

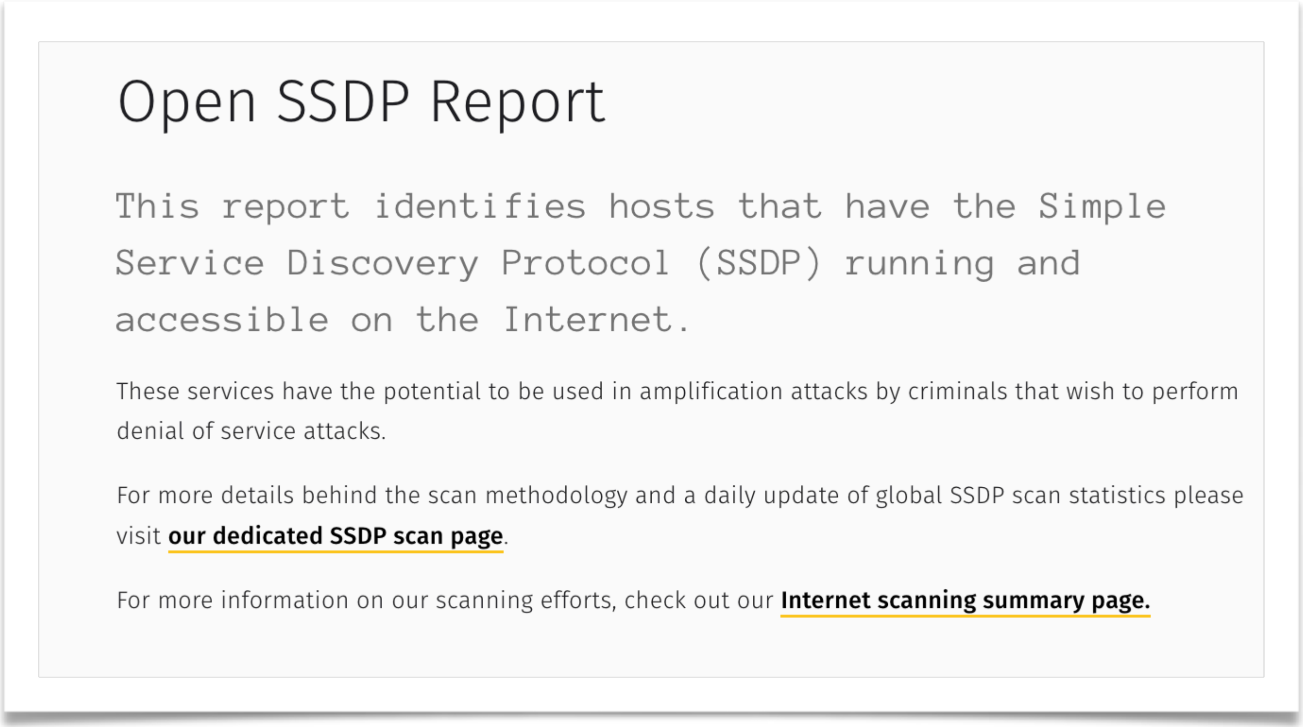
- The report filename contains `scan_ssdp`

- All timestamps are in UTC

- Reports can be sent as e-mail attachments, or downloaded via HTTP or obtained via a RESTful API

- 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/

Open SSDP Report Example



Open SSDP Report

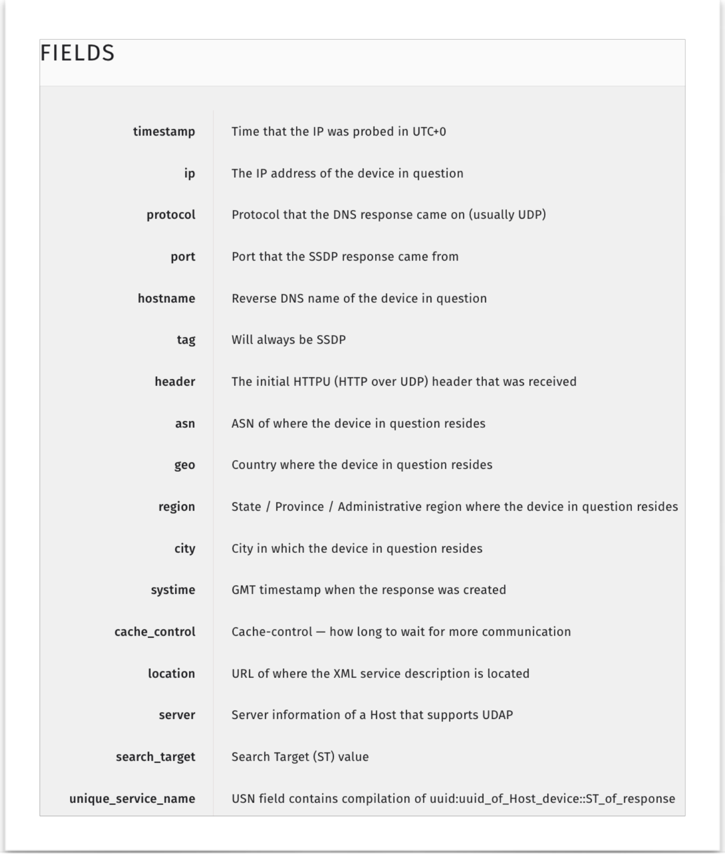
This report identifies hosts that have the Simple Service Discovery Protocol (SSDP) running and accessible on the Internet.

These services have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

For more details behind the scan methodology and a daily update of global SSDP scan statistics please visit **our dedicated SSDP scan page**.

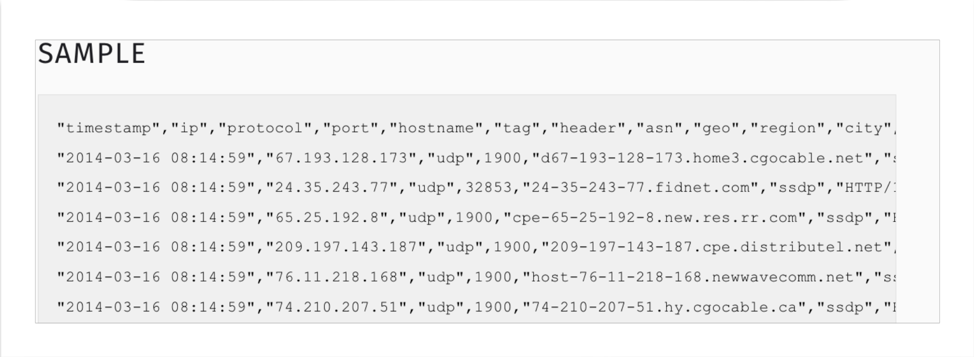
For more information on our scanning efforts, check out our **Internet scanning summary page.**

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



FIELDS

timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the DNS response came on (usually UDP)
port	Port that the SSDP response came from
hostname	Reverse DNS name of the device in question
tag	Will always be SSDP
header	The initial HTTPU (HTTP over UDP) header that was received
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
systime	GMT timestamp when the response was created
cache_control	Cache-control — how long to wait for more communication
location	URL of where the XML service description is located
server	Server information of a Host that supports UDAP
search_target	Search Target (ST) value
unique_service_name	USN field contains compilation of uuid:uuid_of_Host_device::ST_of_response



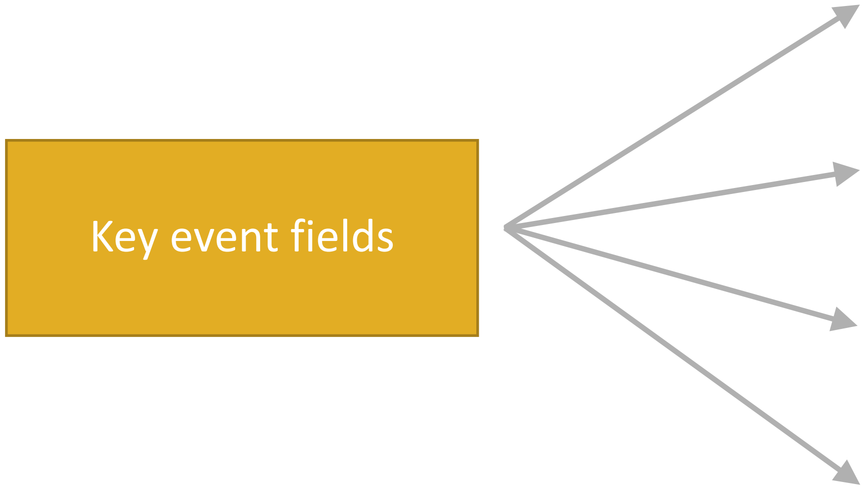
SAMPLE

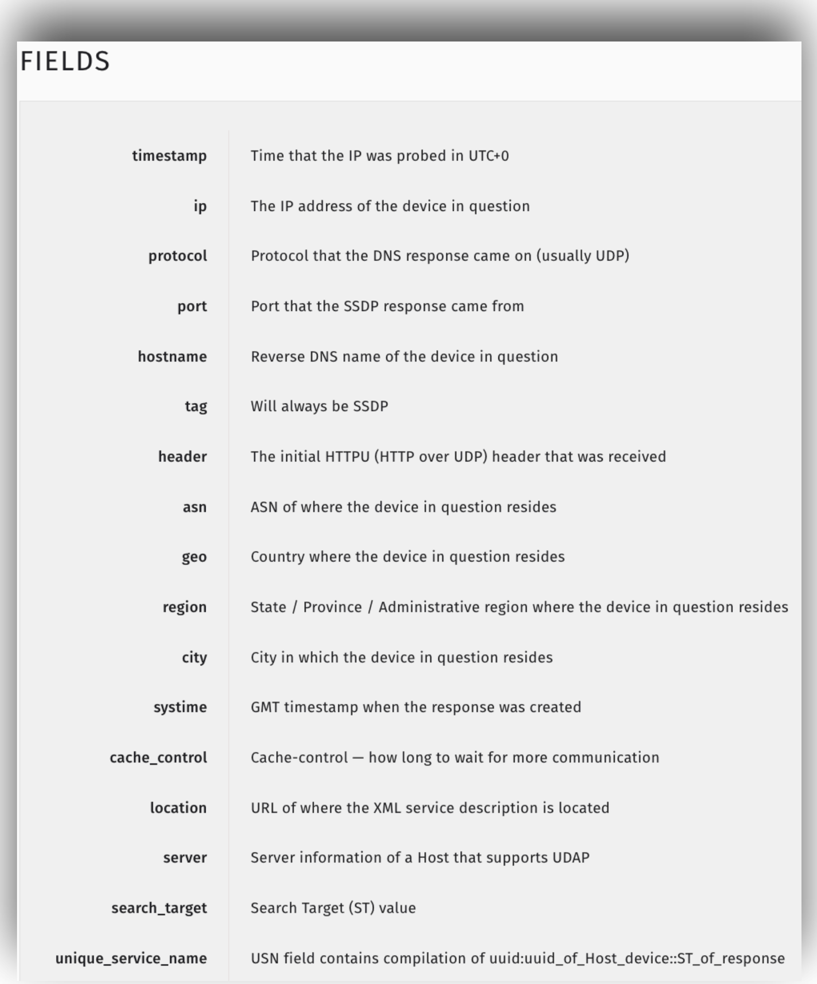
```
"timestamp","ip","protocol","port","hostname","tag","header","asn","geo","region","city",
"2014-03-16 08:14:59","67.193.128.173","udp",1900,"d67-193-128-173.home3.cgocable.net","
"2014-03-16 08:14:59","24.35.243.77","udp",32853,"24-35-243-77.fidnet.com","ssdp","HTTP/
"2014-03-16 08:14:59","65.25.192.8","udp",1900,"cpe-65-25-192-8.new.res.rr.com","ssdp","
"2014-03-16 08:14:59","209.197.143.187","udp",1900,"209-197-143-187.cpe.distributel.net",
"2014-03-16 08:14:59","76.11.218.168","udp",1900,"host-76-11-218-168.newwavecomm.net","s
"2014-03-16 08:14:59","74.210.207.51","udp",1900,"74-210-207-51.hy.cgocable.ca","ssdp","
```

SHADOWSERVER

Action an Open SSDP report

timestamp	ip	protocol	port	hostname	tag	header	asn	geo
05/03/2022 00:02	65.25.X.X	udp	1900	cpe-65-25-192-8.new.xx.xx	ssdp	53HTTP/1.1 200 OK	10796	US

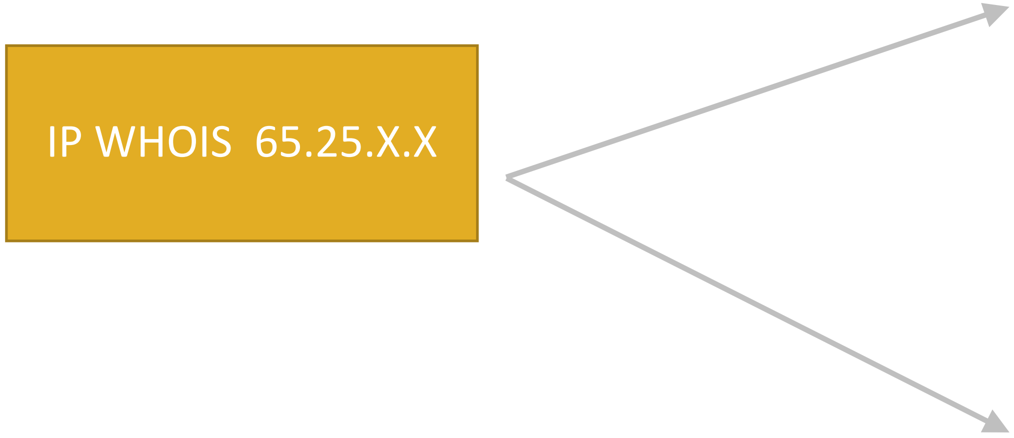

Key event fields

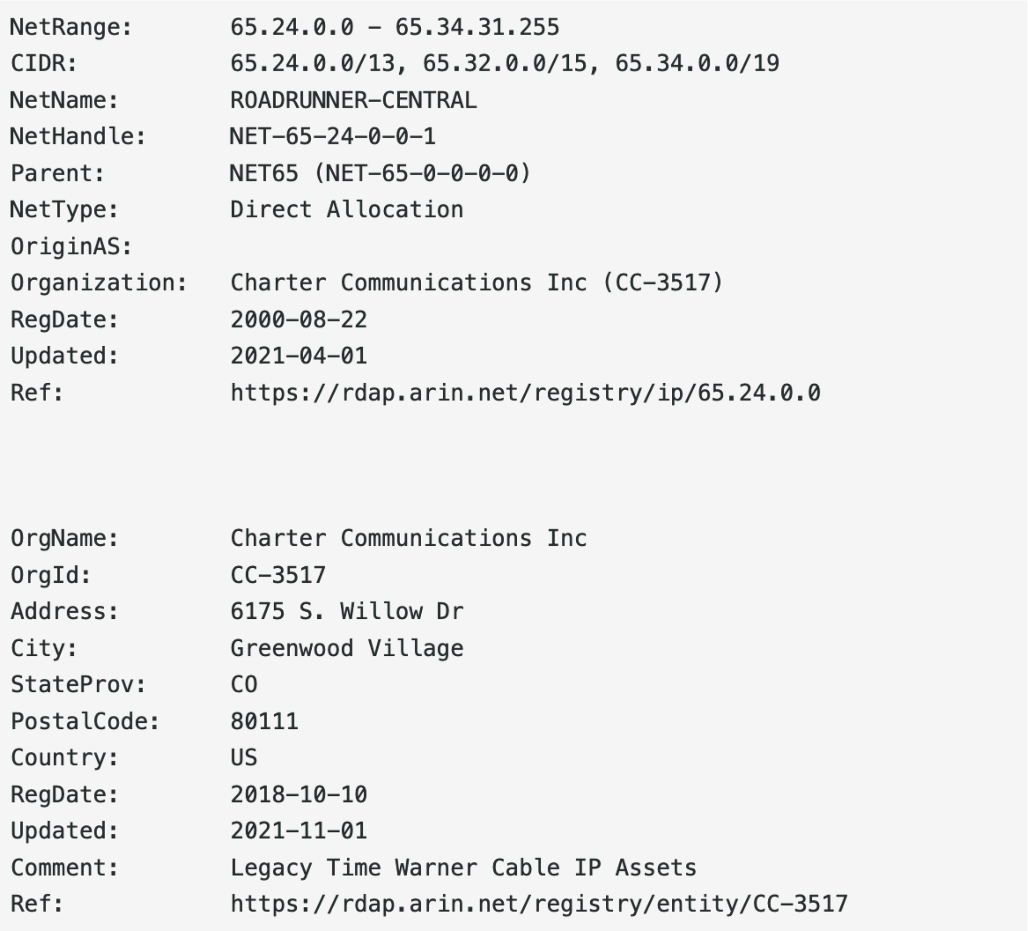

FIELDS

timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the DNS response came on (usually UDP)
port	Port that the SSDP response came from
hostname	Reverse DNS name of the device in question
tag	Will always be SSDP
header	The initial HTTPU (HTTP over UDP) header that was received
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
systime	GMT timestamp when the response was created
cache_control	Cache-control — how long to wait for more communication
location	URL of where the XML service description is located
server	Server information of a Host that supports UDAP
search_target	Search Target (ST) value
unique_service_name	USN field contains compilation of uuid:uuid_of_Host_device::ST_of_response

Action an Open SSDP report

timestamp	ip	protocol	port	hostname	tag	header	asn	geo
05/03/2022 00:02	65.25.X.X	udp	1900	cpe-65-25-192-8.new.xx.xx	ssdp	53HTTP/1.1 200 OK	10796	US


IP WHOIS 65.25.X.X


```
NetRange:       65.24.0.0 - 65.34.31.255
CIDR:           65.24.0.0/13, 65.32.0.0/15, 65.34.0.0/19
NetName:        ROADRUNNER-CENTRAL
NetHandle:      NET-65-24-0-0-1
Parent:         NET65 (NET-65-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Charter Communications Inc (CC-3517)
RegDate:        2000-08-22
Updated:        2021-04-01
Ref:            https://rdap.arin.net/registry/ip/65.24.0.0



OrgName:        Charter Communications Inc
OrgId:          CC-3517
Address:        6175 S. Willow Dr
City:           Greenwood Village
StateProv:      CO
PostalCode:     80111
Country:        US
RegDate:        2018-10-10
Updated:        2021-11-01
Comment:        Legacy Time Warner Cable IP Assets
Ref:            https://rdap.arin.net/registry/entity/CC-3517
```

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 to test your own device to see if it has SSDP (UPnP) enabled, you can do the following
- In one window, start tcpdump with the command: "`tcpdump -n host [IP]`" and then in a second window, enter:

  -
    ```
    perl -e 'print "M-SEARCH * HTTP/
    1.1\r\nHost:239.255.255.250:1900\r\nST:upnp:rootdevice\r\nMan:
    \"ssdp:discover\"\r\nMX:3\r\n\r\n"' > /dev/udp/[IP]/1900
    ```

- If your device has SSDP enabled, you should see a fair amount of traffic on the tcpdump window
- Make sure your queries are not being filtered
- Remember the scan results we share are for the previous day (up to 24 hour delay)

Open SSDP - PROTECT

- No reason to have an SSDP service exposed on the public Internet
- Aside from abuse for DDoS attacks, it can also expose an additional attack surface
- Block inbound and outbound UDP port 1900 traffic on your firewall
- Follow best security practice to reduce your network attack surface

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/open-ssdp-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

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG