Open NTP Monitor & NTP Version (Mode 6) Reports

Scan-based reports on your network or constituency

@shadowserver

✉ contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce Shadowserver scanning
- Introduce our NTP Monitor report
- Highlight a sample NTP Monitor report
- Introduce our NTP Version (Mode 6) report
- Highlight a sample NTP Version (Mode 6) report
- Demonstrate how a National CERT or network owner can action NTP reports
- Describe key features of each report
- Offer guidance on how to protect NTP on your network
- Provide a key list of Shadowserver online resources to enable report subscription and use

Internet-wide Scanning

- Shadowserver scans the entire IPv4 Internet for 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

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

SHADOWSERVER

Open NTP Monitor Report

NTP Monitor

- Network Time Protocol (NTP) is a UDP based protocol used to synchronize computer clock time sources in a network

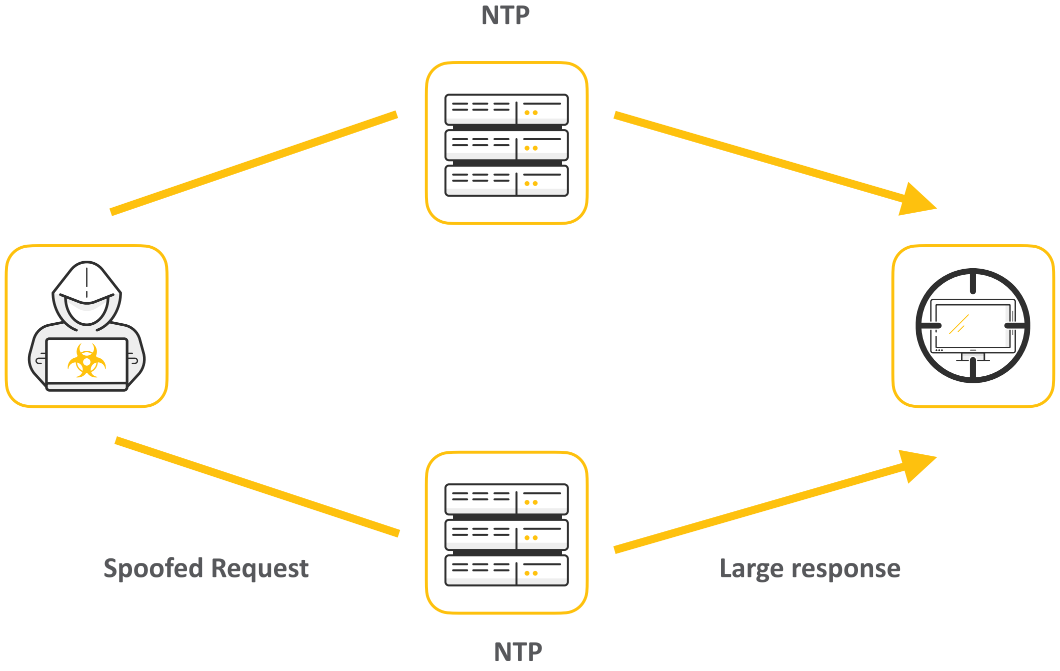
- It is widely used by servers, mobile devices, endpoints, and network devices

- NTP contains a command called Monlist (or sometimes MON_GET_LIST) which can be sent to an NTP server for monitoring purposes

- Monlist queries return larger responses, sending back the addresses of up to the last 600 machines that the NTP server has interacted with

- This can leverage a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker exploits publicly accessible NTP servers

- IP address spoofing generates large responses to significantly smaller NTP network queries, tricking servers to respond and flood the victim with data



SHADOWSERVER

Internet-wide Scanning - NTP Monitor

- A project to search for publicly accessible devices that have NTP running Mode 7 queries for MON_GET_LIST: https://scan.shadowserver.org/ntpmonitor/

- The goal of this project is to identify openly accessible NTP services and report them back to the network owners for remediation

- As NTP is a UDP based protocol, these devices have the potential to be used in NTP amplification attacks and if at all possible, we would like to see these services made un-available to attackers that would misuse these resources

- We are querying all computers with routable IPv4 addresses that are not firewalled from the internet on port 123/udp with an NTPv2 request for the MON_GETLIST_1 control message. We are capturing the response from the NTP service and parsing the result

- For an overview of UDP amplification attacks please read: https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

NTP Monitor Report

- NTP Monitor : https://www.shadowserver.org/what-we-do/network-reporting/ntp-monitor-report/

- Report is available as a file in CSV format

- All timestamps are in UTC

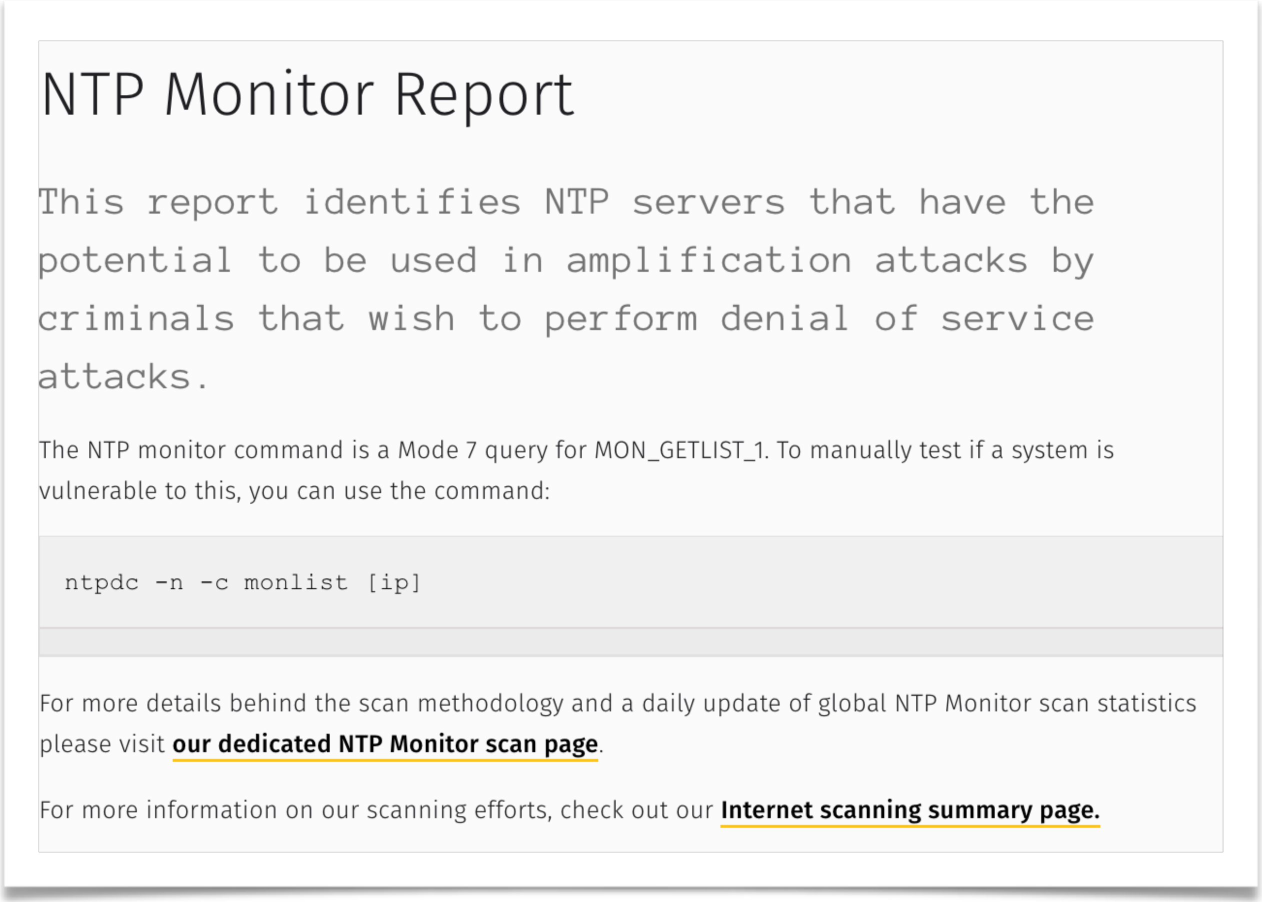
- Reports can be sent as e-mail attachments, downloaded via HTTP or obtained via a RESTful API

- 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/

NTP Monitor Report



NTP Monitor Report

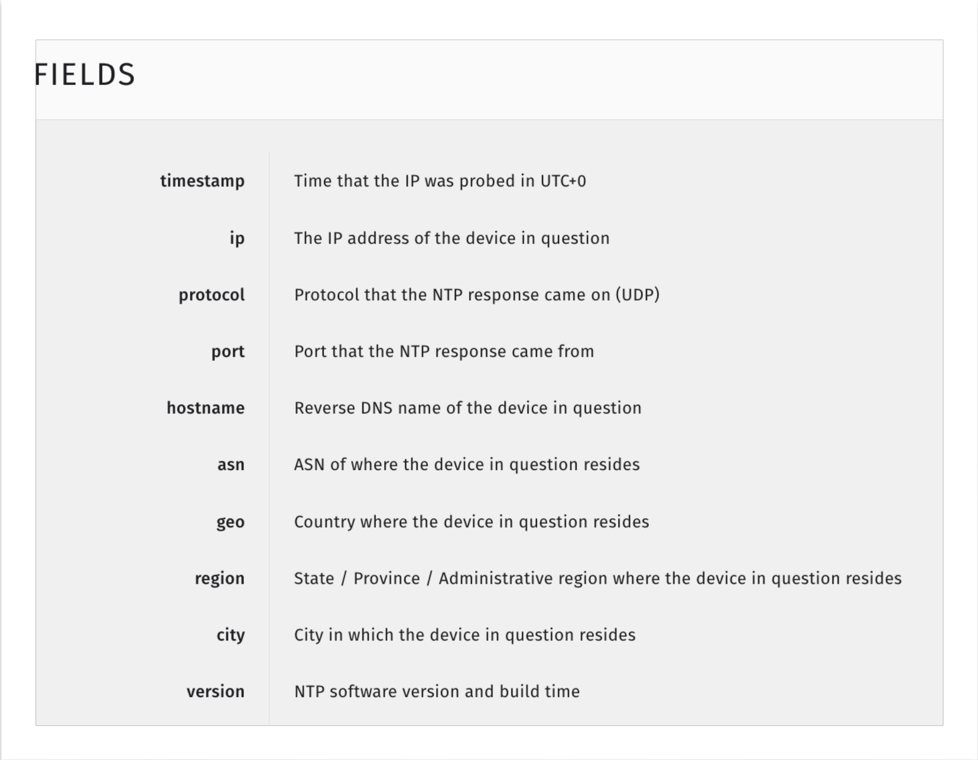
This report identifies NTP servers that have the potential to be used in amplification attacks by criminals that wish to perform denial of service attacks.

The NTP monitor command is a Mode 7 query for MON_GETLIST_1. To manually test if a system is vulnerable to this, you can use the command:

```
ntpdc -n -c monlist [ip]
```

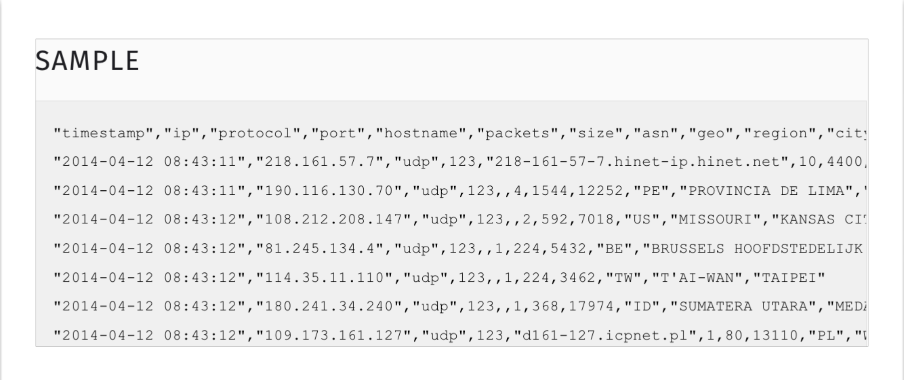
For more details behind the scan methodology and a daily update of global NTP Monitor scan statistics please visit **our dedicated NTP Monitor scan page**.

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



FIELDS

timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the NTP response came on (UDP)
port	Port that the NTP response came from
hostname	Reverse DNS name 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
version	NTP software version and build time



SAMPLE

```
"timestamp","ip","protocol","port","hostname","packets","size","asn","geo","region","city
"2014-04-12 08:43:11","218.161.57.7","udp",123,"218-161-57-7.hinet-ip.hinet.net",10,4400,
"2014-04-12 08:43:11","190.116.130.70","udp",123,,4,1544,12252,"PE","PROVINCIA DE LIMA","
"2014-04-12 08:43:12","108.212.208.147","udp",123,,2,592,7018,"US","MISSOURI","KANSAS CI
"2014-04-12 08:43:12","81.245.134.4","udp",123,,1,224,5432,"BE","BRUSSELS HOOFDSTEDELIJK
"2014-04-12 08:43:12","114.35.11.110","udp",123,,1,224,3462,"TW","T'AI-WAN","TAIPEI"
"2014-04-12 08:43:12","180.241.34.240","udp",123,,1,368,17974,"ID","SUMATERA UTARA","MED
"2014-04-12 08:43:12","109.173.161.127","udp",123,"d161-127.icpnet.pl",1,80,13110,"PL","
```

https://www.shadowserver.org/what-we-do/network-reporting/ntp-monitor-report/

SHADOWSERVER

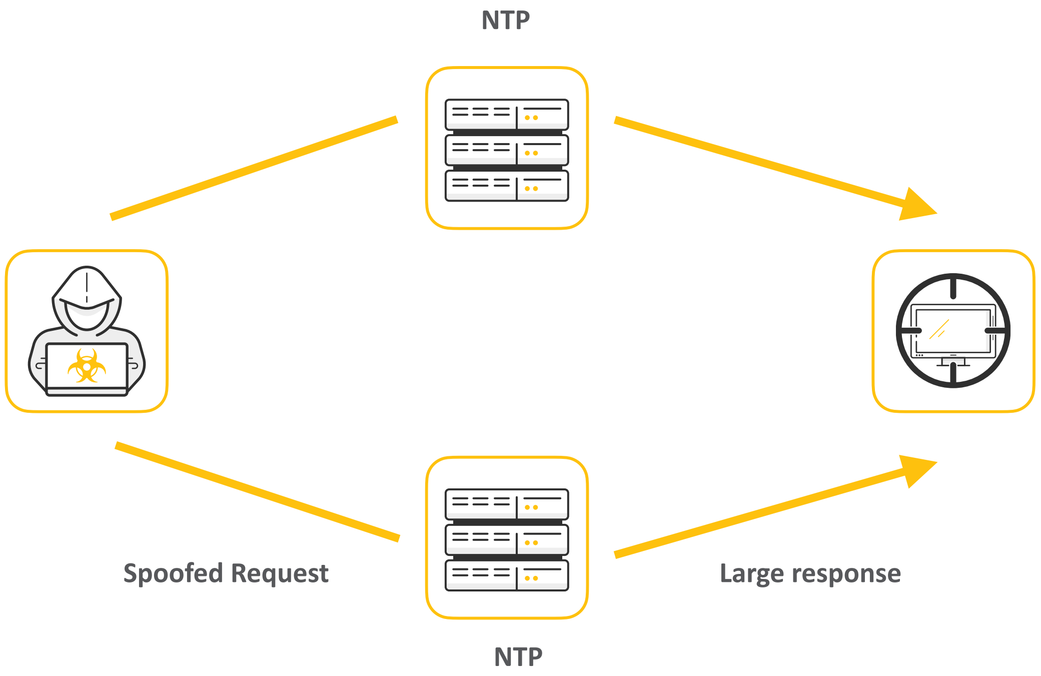
Open NTP Version (Mode 6) Report

NTP Version (Mode 6)

- NTP ‘Mode 6’ commands allow NTP services to be administered while running requests e.g. report generation queries, status information and NTP configuration

- Mode 6 queries return much larger responses than associated queries that can lead to amplification attacks, in which an attacker exploits publicly accessible NTP servers

- IP address spoofing generates large responses to significantly smaller Mode 6 NTP network queries, tricking servers to respond and flood the victim with data



Internet-wide Scanning - NTP Version (Mode 6)

- A project to search for publicly accessible devices that have NTP running and answering Mode 6 queries: https://scan.shadowserver.org/ntpversion/
- The goal of this project is to identify openly accessible NTP services and report them back to the network owners for remediation
- As NTP is a UDP based protocol, these devices have the potential to be used in NTP amplification attacks and if at all possible, we would like to see these services made un-available to miscreants that would misuse these resources.
- We are querying all computers with routable IPv4 addresses that are not firewalled from the internet on port 123/udp with an NTPv2 request for READVAR control message. We are capturing the response from the NTP service and parsing the result
- For an overview of UDP amplification attacks please read: https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

NTP Version (Mode 6) Report

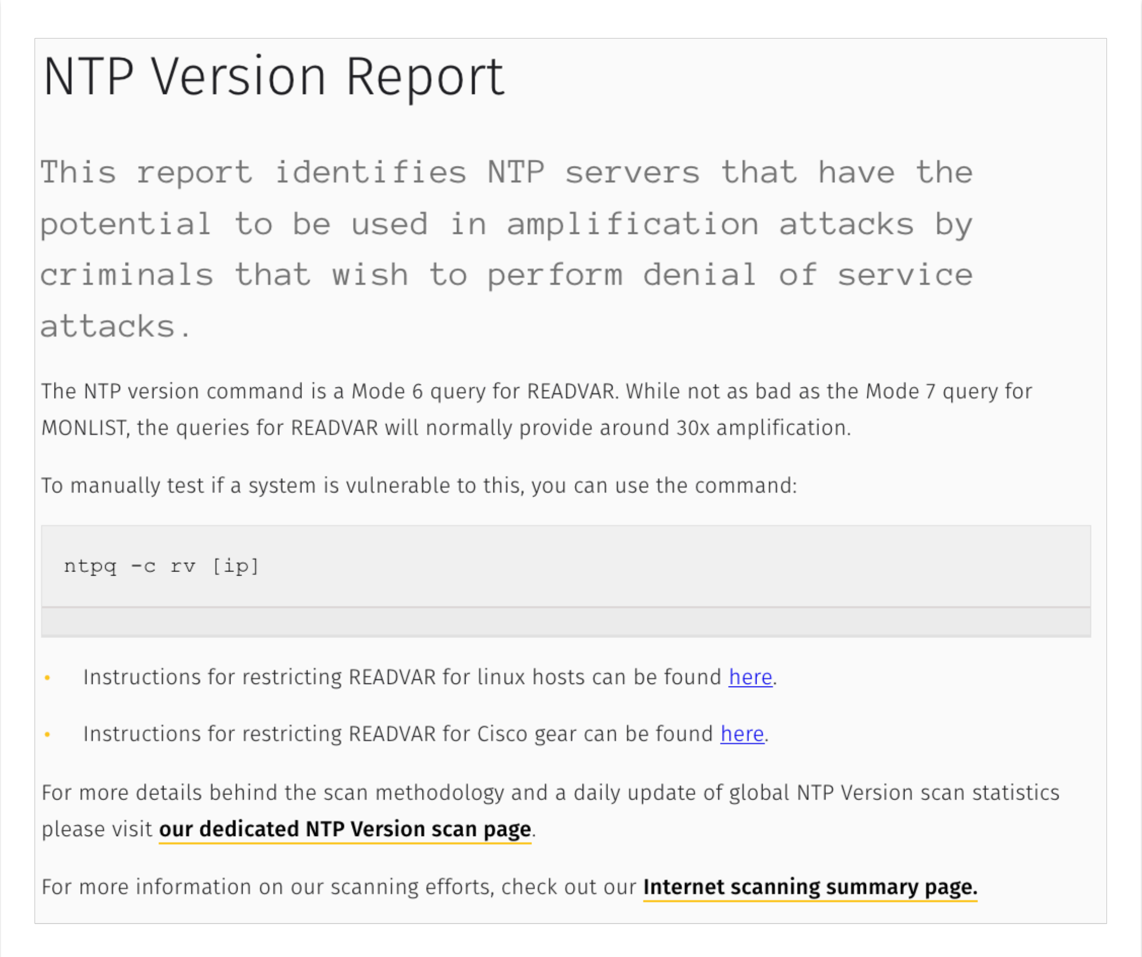
- NTP Version (Mode 6) : https://www.shadowserver.org/what-we-do/network-reporting/ntp-version-report/
- This report identifies NTP servers that have the potential to be used in amplification attacks by threat actors that wish to perform denial of service attack
- Report is available as a file in CSV format
- All timestamps are in UTC
- Reports can be sent as e-mail attachments, 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/

SHADOWSERVER

NTP Version (Mode 6) Report



NTP Version Report

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

The NTP version command is a Mode 6 query for READVAR. While not as bad as the Mode 7 query for MONLIST, the queries for READVAR will normally provide around 30x amplification.

To manually test if a system is vulnerable to this, you can use the command:

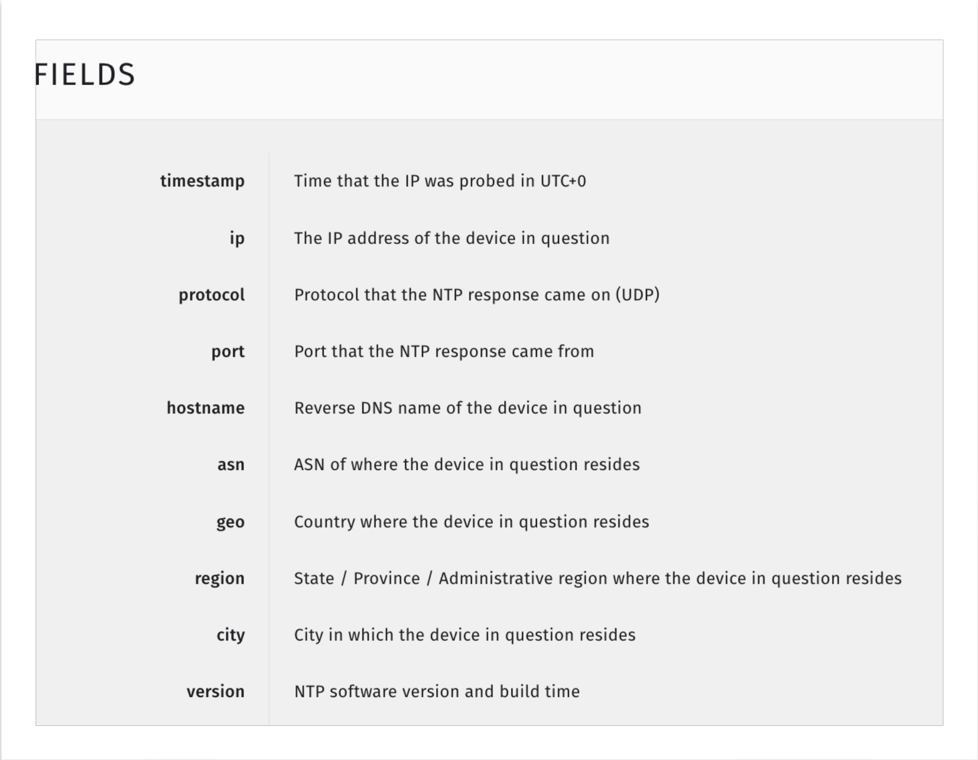
```
ntpq -c rv [ip]
```

- Instructions for restricting READVAR for linux hosts can be found here.
- Instructions for restricting READVAR for Cisco gear can be found here.

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

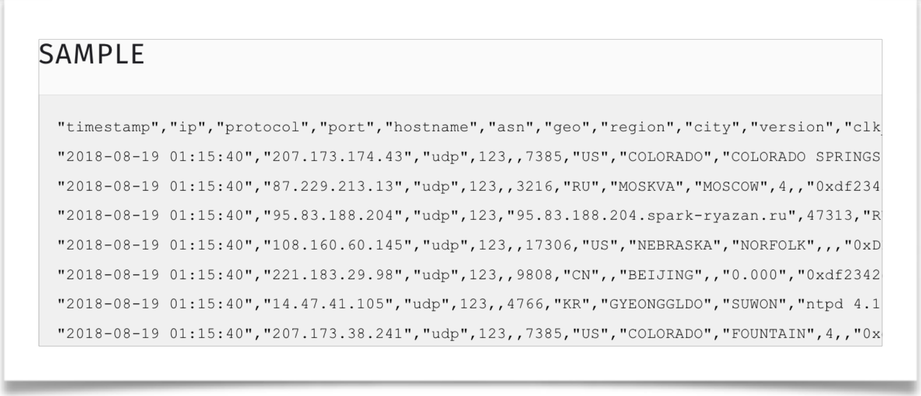
For more information on our scanning efforts, check out our **Internet scanning summary page.**

https://www.shadowserver.org/what-we-do/network-reporting/ntp-version-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 NTP response came on (UDP)
port	Port that the NTP response came from
hostname	Reverse DNS name 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
version	NTP software version and build time



SAMPLE

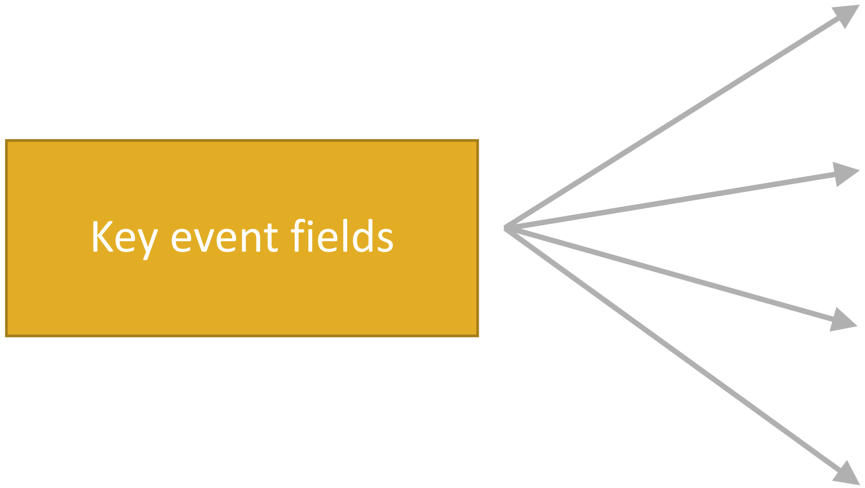
```
"timestamp","ip","protocol","port","hostname","asn","geo","region","city","version","clk
"2018-08-19 01:15:40","207.173.174.43","udp",123,,7385,"US","COLORADO","COLORADO SPRINGS
"2018-08-19 01:15:40","87.229.213.13","udp",123,,3216,"RU","MOSKVA","MOSCOW",4,,"0xdf234
"2018-08-19 01:15:40","95.83.188.204","udp",123,"95.83.188.204.spark-ryazan.ru",47313,"R
"2018-08-19 01:15:40","108.160.60.145","udp",123,,17306,"US","NEBRASKA","NORFOLK",,,"0xD
"2018-08-19 01:15:40","221.183.29.98","udp",123,,9808,"CN",,"BEIJING",,"0.000","0xdf2342
"2018-08-19 01:15:40","14.47.41.105","udp",123,,4766,"KR","GYEONGGLDO","SUWON","ntpd 4.1
"2018-08-19 01:15:40","207.173.38.241","udp",123,,7385,"US","COLORADO","FOUNTAIN",4,,"0x
```

SHADOWSERVER

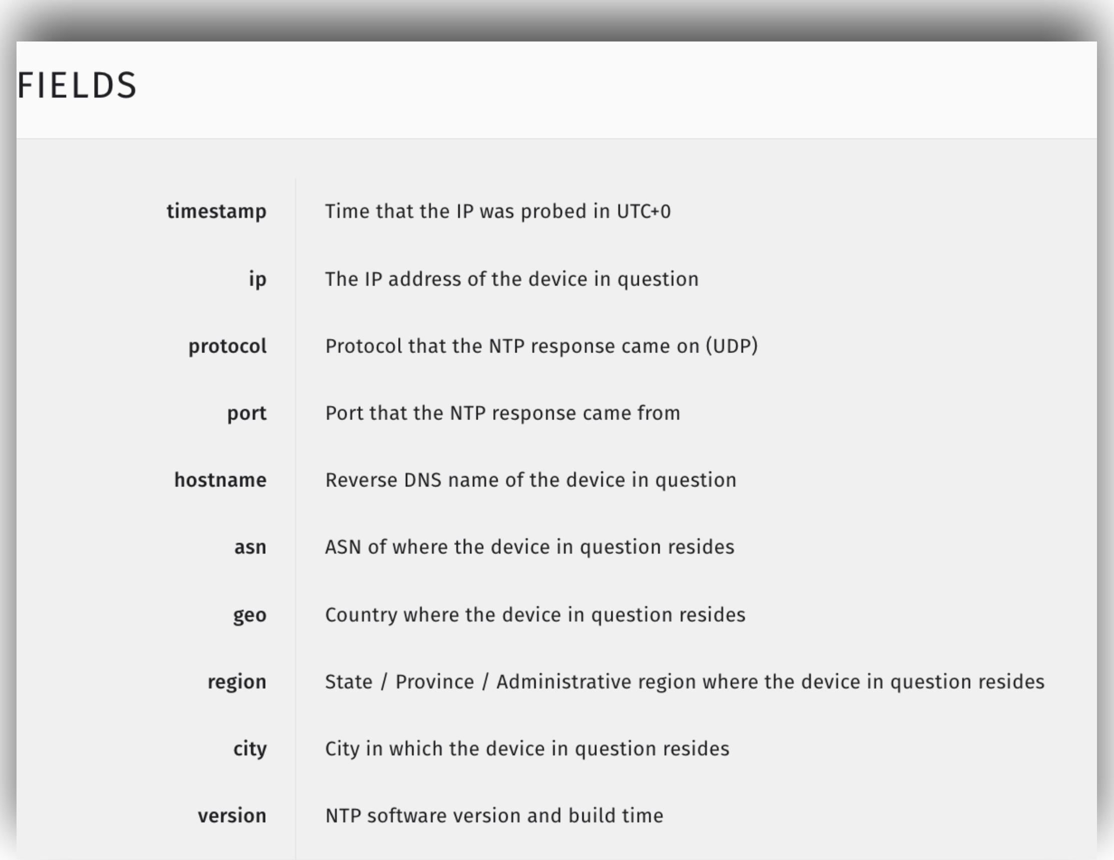
Actioning the NTP Reports

Action an NTP Report

timestamp	ip	protocol	port	hostname	asn	geo	region	city	version
18/04/2022 00:00	207.173.X.X	udp	123	XXX	7385	us	colorado	colorado springs	4



Key event fields



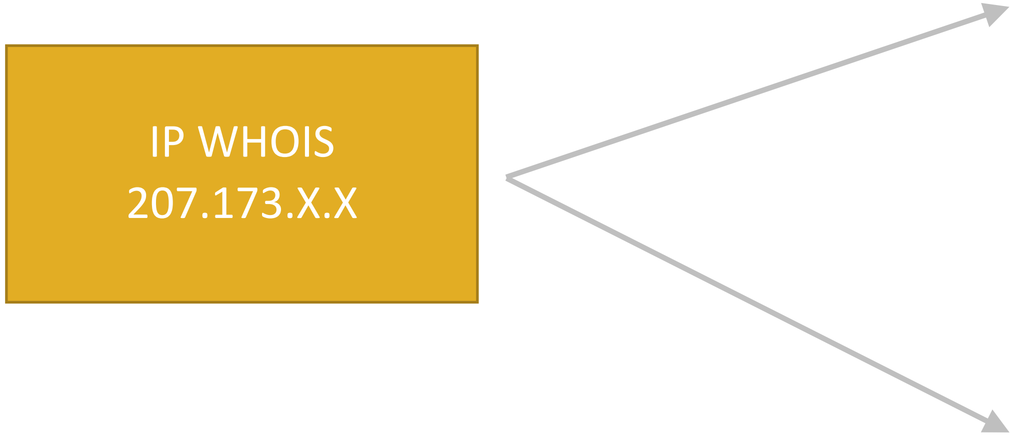
FIELDS

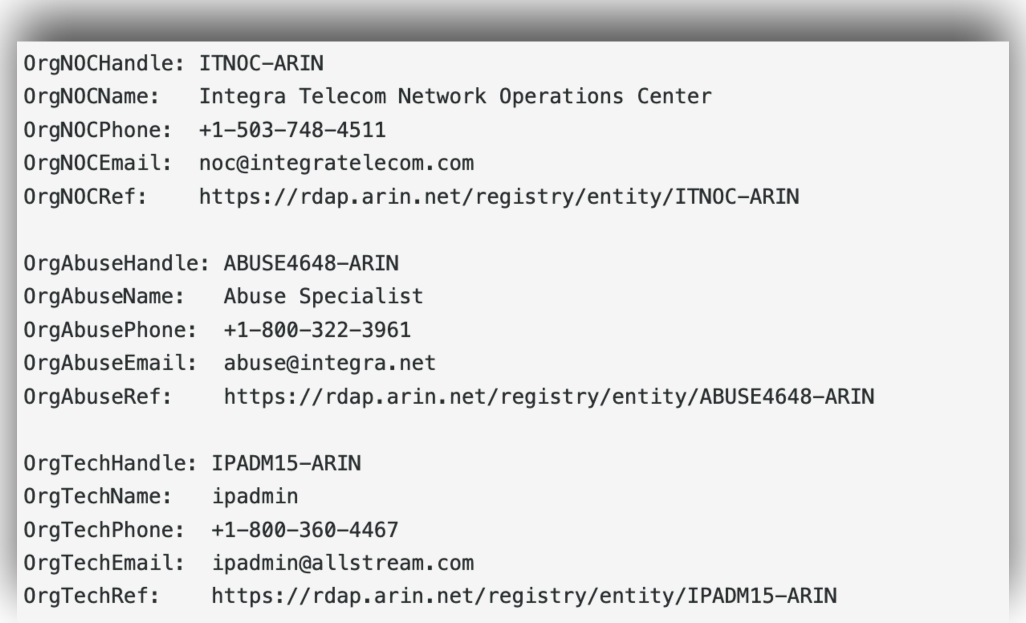
timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the NTP response came on (UDP)
port	Port that the NTP response came from
hostname	Reverse DNS name of the device in question
asn	ASN of where the device in question resides
geo	Country where 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
version	NTP software version and build time

SHADOWSERVER

Action an NTP Report

timestamp	ip	protocol	port	hostname	asn	geo	region	city	version
18/04/2022 00:00	207.173.X.X	udp	123	XXX	7385	us	colorado	colorado springs	4


IP WHOIS
207.173.X.X


```
OrgNOCHandle: ITNOC-ARIN
OrgNOCName:   Integra Telecom Network Operations Center
OrgNOCPhone:  +1-503-748-4511
OrgNOCEmail:  noc@integratelecom.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/ITNOC-ARIN

OrgAbuseHandle: ABUSE4648-ARIN
OrgAbuseName:   Abuse Specialist
OrgAbusePhone:  +1-800-322-3961
OrgAbuseEmail:  abuse@integra.net
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE4648-ARIN

OrgTechHandle: IPADM15-ARIN
OrgTechName:   ipadmin
OrgTechPhone:  +1-800-360-4467
OrgTechEmail:  ipadmin@allstream.com
OrgTechRef:    https://rdap.arin.net/registry/entity/IPADM15-ARIN
```

NTP Monitor - Verifying 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 an NTP server is open, try using the command:

  -
    ```
    ntpdc -n -c monlist [ip]
    ```
  - you will obtain a list of recent clients that queried the NTP server (or an empty list if none)
  - if you are getting a timeout, make sure your queries are not being filtered

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

NTP Version (Mode 6) - Verifying 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 an NTP server is open, try using the command:
  - `ntpq -c rv [IP]`. If the command is successful, you will see a string of information from the IP that you queried that usually starts off with something like this: '`associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync, version="ntpd 4.2.6p2@1.2194-o Sun Oct 17 13:35:13 UTC 2010 (1)", processor="x86_64", system="Linux/3.2.0-0.bpo.4-amd64", leap=00`'.
  - if you are getting a timeout, 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

NTP - PROTECT

- Unless servers are part of a public NTP server pool, they should not be enabled on public interfaces
- Scan your NTP server and upgrade the NTP daemon to the latest version. Do this regularly!
- If an upgrade is not possible, disable the *MONLIST* command or enforce that requests come from valid sources (access controls/filtering)
- Read more on secure configuration at: https://support.ntp.org/bin/view/Support/AccessRestrictions
- If you do not run an NTP server but are worried that you may become a victim of an NTP reflection attack :
    - Monitor NTP traffic for UDP packet volume spikes on port 123
    - Prevent IP spoofing to make sure that the IP of your internet-facing assets cannot be spoofed by implementing security measures such as BCP38
    - Close UDP port 123 on your internet-facing assets if time synchronization is not required

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/ntp-version-report/
- https://www.shadowserver.org/what-we-do/network-reporting/ntp-monitor-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