CyberGreen

A global community to measure and improve cyberhealth

# Risk Mitigation for Open NTP

Sept 2016

# Agenda

1. Introduction
2. About NTP
3. Mitigation recommendations for open NTP
4. Making the case for implementing mitigations

# Introduction

When cyber infrastructure is insecure there is a risk to the global Internet community

Network Time Protocol (NTP) is the standard protocol for time synchronization for networked devices NTP can be found in nearly every network environment

Synchronized time is critical to logging, authentication, cryptography and general system administration

NTP infrastructure needs to be secure and trustworthy

# About CyberGreen

- Global non-profit and collaborative organization focused on helping improve the health of global Cyber Ecosystem
- Working to provide reliable metrics and mitigation best practice information to Cyber Security Incident Response Teams (CSIRTs), network operators, and policy makers
- Mission: help CSIRTs and others focus remediation efforts on the most important risks
  - Help understand where improvements can be made
  - How we can achieve a more sustainable, secure, and resilient cyber ecosystem

# Copyright (c) 2016, CyberGreen

# About NTP

# Network Time Protocol (NTP)

Network Time Protocol (NTP) is standard protocol for time synchronization for devices on a network, used by servers, mobile devices, endpoints and networking devices from all vendors

The latest definition of NTP is version 4, as described in RFC 5905[1]

[1] http://www.ietf.org/rfc/rfc5905.txt

# Network Time Protocol (NTP)

NTP clients synchronize their time with a local time server (like the Domain Controller in Windows environments), which will in turn synchronize its clock with reliable NTP servers available on the Internet

Just to get the time, very few types of messages are needed

- Additional messages and modes only needed for NTP servers that need to talk to each other

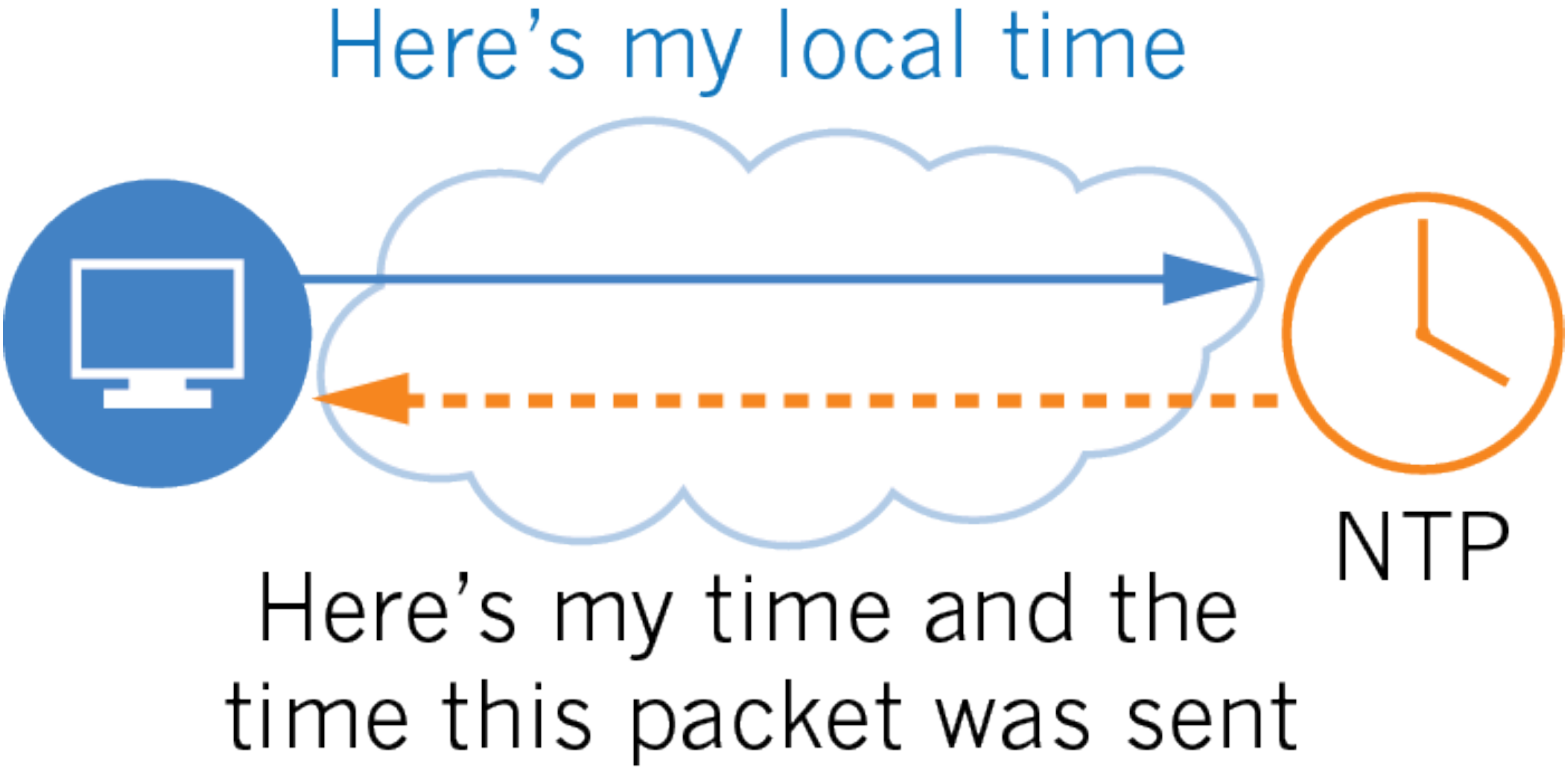
# What is open NTP?

“Open NTP” is a server where

- NPT is running on a device available to the public Internet, and
- NTP answers Mode 6 or Mode 7 queries
  - These queries have vulnerabilities that can be exploited by attackers[2]

[2] https://community.rapid7.com/community/metasploit/blog/2014/08/25/r7-2014-12-more-amplification-vulnerabilities-in-ntp-allow-even-more-drdos-attacks

# How NTP works



Here’s my local time

NTP

Here’s my time and the time this packet was sent

# Risks posed by open NTP

Devices running open NTP can be used in reflection attacks, a type of traffic amplification attack

- **Denial of service (DoS)** – attacker tries make a victim's machine or network unavailable to its intended users
- **Amplification** – when the attacker sends a small packet to a server that will generate a large reply

In amplification distributed denial of service (DDoS) attacks, attackers simultaneous abuse multiple amplifiers such as NTP servers

- Creates highly-distributed DoS attack conducted from a single command and control host

# Open NTP in reflection attacks

Attacker tries to exhaust the victim's bandwidth by abusing the fact that servers using protocols such as NTP allow spoofing of sender IP addresses

Reflection attacks often exploit User Datagram Protocol (UDP) traffic

- UDP responds to requests without any validation of sender identity, i.e. IP address
- UDP traffic can be spoofed (i.e. have a misleading apparent source IP address) and attacker is able to hide true identity

# NTP reflection amplification attack

A DDoS that relies on publically accessible open NTP servers to overwhelm a victim system with NTP response traffic

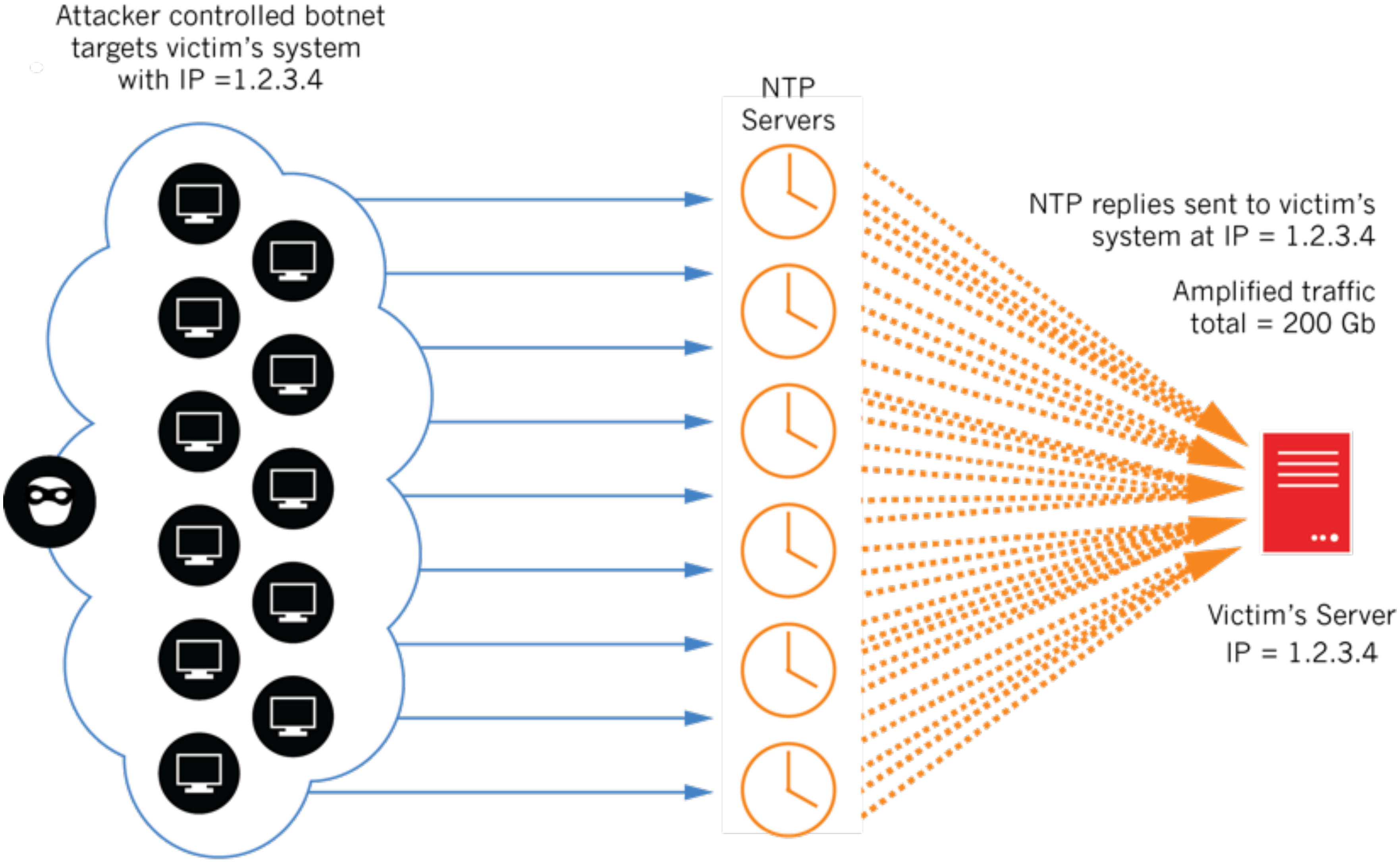
- An attacker with a single 1 Gigabit/second (Gb/s) connection can theoretically generate more than 200 Gb/s of DDoS traffic[3]

Only ***scalable and effective mitigation*** is to reduce number of servers that can be used by attackers

- As of 07/27/16, Shadowserver reported 4,062,384 unique IPs with open NTP; see https://ntpscan.shadowserver.org/stats/

[3] https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks

# NTP Amplification Attack



Attacker controlled botnet
targets victim's system
with IP =1.2.3.4

NTP
Servers

NTP replies sent to victim's
system at IP = 1.2.3.4

Amplified traffic
total = 200 Gb

Victim's Server
IP = 1.2.3.4

Botnet systems send Mode 6 and Mode 7 queries (UDP port 123) using spoofed source IP of victim (IP = 1.2.3.4)

Total size of all requests = 1 Gb

# NTP amplification attack

Attackers generate a large number of UDP packets using spoofed source IP address

UDP packets are sent to NTP servers on port 123

Attackers particularly like NTP servers that support the `MONLIST` command[4]

- `MONLIST` command returns a list with last 600 IP addresses that connected to the NTP server
- Acts as reconnaissance tool for hackers: helps build profile of local network

[4] A discussion of `MONLIST` can be found at https://blog.qualys.com/securitylabs/2014/01/21/how-qualysguard-detects-vulnerability-to-ntp-amplification-attacks

# Real life attack using open NTP

Early 2014 report of attack using open NTP[5]

- Generated around 400Gbp/s of traffic using 4,529 NTP servers
- Each server reportedly sent 87Mbp/s of traffic to the victim

NTP amplification attacks can result in a bandwidth amplification factor of 556.9[6]

[5] https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

[6] http://www.christian-rossow.de/articles/Amplification_DDoS.php

# Potential impacts from NTP attacks

**Productivity**

- Service interruption or failure of business operations relying on network connectivity, particularly for seasonal operations - *e.g. online retailers where a majority of sales happen between Thanksgiving and New Years*
- Time sensitive operations, *e.g. colleges with limited online registration periods or online wagering on upcoming sporting events, etc.*

# Other potential NTP attack impacts

**Brand**

- Loss of reputation with customers and partners
- Becoming known as a “DoS magnet” in global community

**Technical**

- Network service interrupted
- Isolation of victim network by network providers from the rest of Internet to mitigate collateral damage to other customers

**Financial**

- Loss of business resulting from service interruption
- Cost of specialized DDoS mitigation services

# Indirect impacts from Open NTP attacks

You may be impacted if a victim organization ***shares your upstream connectivity***

Open NTP devices on ***your network*** may be used to contribute to an attack on another organization

Potential indirect impacts include:

**Technical**

- Network service degraded
- Inbound or outbound bandwidth may be reduced
- Network providers may isolate your network (or at least your insecure recursive resolver) from the rest of Internet

# Other indirect impacts

**Brand**

- Loss of reputation with customers and partners due to slow or unreliable network and systems

**Financial**

- Unexpected network usage costs
- Loss of business resulting from service degradation

# Mitigate risks from open NTP

# Mitigation options vary by environment

Not all mitigation best practices are appropriate for all environments

CyberGreen provides information relevant to four basic environmental profiles

Look for these icons to find mitigations for your environment

1. Consumers
2. Companies
3. ISPs
4. Policy Makers

# Mitigate risks from open NTP

The best way to mitigate risks from open NTP moving forward is to purchase and deploy devices with minimal NTP configured, particularly on outside interfaces

Work with your internal acquisition and procurement teams, or vendors about other options

# Identify your open NTP risk

Even if you don't think your devices currently run NTP across the Internet, you should check your network

- Many devices may be running NTP without your knowledge
- NTP is often built into Customer Premise Equipment (CPE) gateways on network equipment such as cable modems, DSL routers, "broadband WiFi routers", etc.

# Find hosts running NTP

The simplest way is to use a web-based probe, such as the one at http://openntpproject.org

To manually identify NTP servers with amplified responses enabled, run one of the following commands:

```
    ntpdc -n -c monlist 192.0.2.1
    ntpdc -c sysinfo 192.0.2.1
    ntpq -c readvar 192.0.2.1
```

*The commands only verify if specified functions are enabled*

# Manually finding NTP hosts

If command was successful, you will see a string of information like this from the IP you queried :

```
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
```

# Mitigation: Upgrade NTP

The easiest way to mitigate the risk is to upgrade to NTP-4.2.7p230 (released in 2011) or later, which removes the `MONLIST` command entirely and disables Mode 7 responses by default

- Protects your network from inadvertently being used in a DDoS attack
- Protects your network from unwanted reconnaissance

# Mitigation: Upgrade NTP

If your environment is so fragile that upgrading is not an option, modify the NTP conf file to add the statement `disable monitor` and then restart your NTP processes

You should also implement an additional risk mitigation

# Mitigation: Disable status queries or restrict access

NTP queries may reveal information about the system running NTP that you do not want others to know, such as the operating system version and ntpd version

Disabling these query features may help to reduce the likelihood of this data leakage taking place

- Disabling these queries has a cost, as these query capabilities also provide useful Q/A and debugging information

# Mitigation: Restrict informational queries to authorized recipients

To disable `MONLIST` functionality on a public-facing NTP server that cannot be updated to 4.2.7, add the following lines to your ntp.conf file:

For IPv4:

```
restrict default kod nomodify notrap nopeer
noquery
```

For IPv6:

```
restrict -6 default kod nomodify notrap
nopeer noquery
```

*Note: requires a restart of the ntpd service to take effect*

# Mitigation: Restrict access per network segment

Modify your ntp.conf to restrict access: per network segment (modify line 3 to match your LAN settings) *and* per host (modify line 4):

```
restrict default noquery
restrict localhost
restrict 192.168.0.0 netmask 255.255.0.0 nomodify notrap nopeer
restrict 192.168.1.27
```

*Note: requires a restart of the ntpd service to take effect*

# Other NTP mitigations

Consider blocking large NTP packets at network edge

- Block packets 234 bytes – 482 bytes (the size of `MONLIST` replies)

Additional guidelines for securing the NTP service on different platforms and configurations are available from Team Cymru: [http://www.team-cymru.org/secure-ntp-template.html](http://www.team-cymru.org/secure-ntp-template.html)

# Mitigations for ASNs or ISPs

Use traffic shaping on UDP service requests

- Ensures repeated access to Internet resources is not abusive

Monitor NTP in your network for signs of amplification attacks (see https://www.us-cert.gov/ncas/alerts/TA14-017A) and generate abuse tickets for these customers

- Options: take a customer's modem offline, or notify via phone call

Notify your customers of issues, even if you can't tell them how to fix them

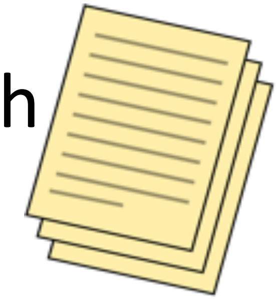
- They may not be intentionally running an NTP server - traffic may be result of malfunctioning home routers that Customer Care has no idea how to reconfigure

# Spoofed Traffic Mitigation: Implement ingress filtering on networks

Internet Engineering Task Force (IETF) Best Current Practice (BCP) documents

Configuration changes to substantially reduce potential for source IP spoofed attacks, the most popular DDoS attack type

- How to filter network traffic on network to verify the source address of a packet
- Reject packets with source addresses that are not reachable via the actual packet's path



# IETF BCPs recommended

All network operators should perform network ingress filtering as described in these BCPs:

**BCP-38 Network Ingress Filtering**

- Defeating Denial of Service Attacks which employ IP Source Address Spoofing: https://tools.ietf.org/html/bcp38

**BCP-84 Ingress Filtering for Multihomed Networks**

- https://tools.ietf.org/html/bcp84

# More info on IETF BCPs

Test whether your network currently follows BCP-38 using tools from the Spoofer Project: https://www.caida.org/projects/spoofer/

Additional details about how to implement BCP-38: http://www.bcp38.info/index.php/Main_Page

# Additional mitigations for ISPs

ISPs should ensure that they have a DDoS defense that is multi-layered, and designed to deal with:

- Attacks that can saturate their connectivity
- "Low and slow" sophisticated application layer attacks

# Verify your fix

Verify and monitor your infrastructure to ensure it remains secure by subscribing to free reports from Shadowserver, available at

https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

# Additional NTP resources

https://ntpscan.shadowserver.org/

http://openntpproject.org

http://www.us-cert.gov/ncas/alerts/TA14-017A

https://community.rapid7.com/community/metasploit/blog/2014/08/25/r7-2014-12-more-amplification-vulnerabilities-in-ntp-allow-even-more-drdos-attacks

http://www.acunetix.com/blog/articles/ntp-reflection-ddos-attacks

# Making the case for implementing mitigations such as BCP 38

# Making the case for mitigations

Help everyone understand the level of effort needed to improve cyber health in their community

Why should you implement the mitigations in your environment?

1. It is the right thing to do as a good Internet neighbor
2. Your organization may be next to be attacked

Let’s join together and stop bad guys from winning!

# Changing risk landscape

Increased need to demonstrate "due care"

- Obtaining cyber insurance
- Complying with risk frameworks to win business with local / national governments and large corporations

If we (***you!)*** don't do a better job of securing our own infrastructure and reducing cyber risk, government regulation may force additional mandates and/or penalties

# Anticipated organizational benefits

Increased productivity

- Fewer service interruptions and failures

Improved network performance

- Existing network more reliable and resilient, with greater capacity

Improved brand reputation

- Technical reliability and security a selling point to customers

# More anticipated benefits

- Decreased budget uncertainty
  - Fewer unanticipated usage costs for IT
  - Budget can be used as planned, e.g. - upgrading technical capability / capacity, additional personnel, etc.
- System admins may spend less time spent trying to deal with unexpected problems, which in turn may improve their productivity and reduce unexpected overtime

# What do you need to implement these mitigations?

Commands and configuration details for most important mitigations are publically available

- No additional software must be purchased
- Implementing mitigations does not require any special knowledge, skills, or abilities

Note: All mitigations should be carefully reviewed in light of your specific business requirements and infrastructure environment before proceeding

All organizational change management processes, including testing, should be followed

# How long will mitigations take?

System administrators in smaller organizations need a few hours per network to investigate, implement and verify upgrade of NTP

- Comparable effort needed for other mitigations, such as disabling status queries and `MONLIST` functionality, and blocking large NTP packets at the network edge

ISPs and large entities can take advantage of configuration management systems with task execution, such as Salt and Ansible, to automate administration of changes

# How long to implement BCP-38 network ingress filtering?

Small businesses: from a few minutes to less than an hour

Larger and more complex organizations: days to weeks

Bonus: with no real maintenance, the recurring cost is effectively zero!

# Acknowledgement

CyberGreen would like to thank the experts who made the creation of this document possible:

Written by:

- Laurin Buchanan, Applied Visions, Inc. – Secure Decisions Division

Contributed and Reviewed by:

- Matt Carothers, Cox Communications
- Baiba Kaskina, CERT.LV
- Moto Kawasaki, JPCERT/CC
- Art Manion, CERT/CC
- Yoshinobu Matsuzaki, IIJ
- Joe St Sauver, Farsight Security
- David Watson, ShadowServer Foundation

Disclaimer: CyberGreen believes this guidance and the advice from our experts should be of benefit to anyone mitigating a risk conditions, but it is not advice specific to any reader or network. Ultimately, each reader is responsible for implementing his or her own network remediation strategy and we assume no responsibility or liability therefore.

CyberGreen

For more information about
risk mitigation best practices
please contact:
contact@cybergreen.net