



CyberGreen

A global community to measure and improve cyberhealth

Risk Mitigation for Open SSDP

Agenda

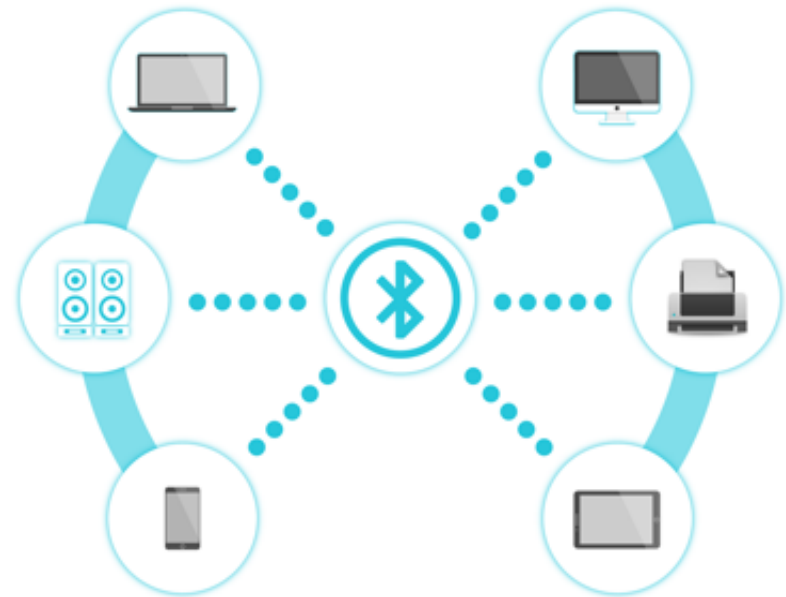
1. Introduction
2. About SSDP
3. Mitigation recommendations for open SSDP
4. Making the case for implementing mitigations



Introduction

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

Simple Service Discovery Protocol (SSDP) is the standard search protocol for Universal Plug and Play (UPnP)



Introduction

UPnP is pervasive - it is enabled by default on home gateways, network printers, webcams, network storage servers, and “smart home” devices such as thermostats, automated assistants and wireless home security systems that are part of the Internet of Things (IoT)



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

These materials are distributed under the following license:

Permission to use, copy, modify, and/or distribute these materials for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE MATERIAL IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS MATERIAL INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS MATERIAL.

About SSDP

Simple Service Discovery Protocol (SSDP)

Simple Service Discovery Protocol (SSDP) is the standard search protocol for Universal Plug and Play (UPnP)

It allows computers and various other network connected devices to communicate with each other

It simplifies the discovery and control of network devices on a local network



Universal Plug and Play (UPnP)

UPnP **enabled by default** on many devices: smart TVs, IP cameras, printers, media servers and routers, and most operating systems

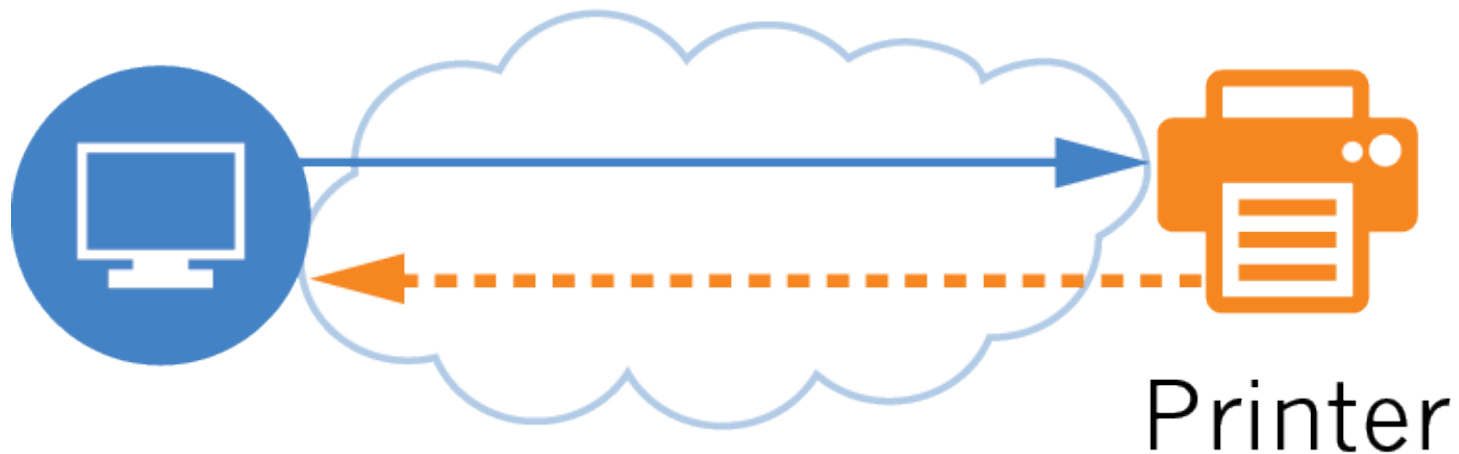
UPnP provides

- Incoming port mapping on home routers
- Identification of network printers
- Management of media services

Also used in many “smart home” control technologies: programmable thermostats, wireless security systems, home hubs and Internet assistants

How UPnP uses SSDP to discover services

Query on UDP port 1900:
Are there any printing services
available in local network?



Reply on TCP Port 5000:
URL of printer description file.

What is open SSDP?

“Open SSDP” refers to a device that is running SSDP and responds to UPnP discovery requests **from the Internet**



Risks posed by open SSDP

Devices running open SSDP 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 SSDP servers

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

Open SSDP in reflection attacks

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

Reflection attacks often exploit User Datagram Protocol (UDP) traffic

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



SSDP reflection amplification attack

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

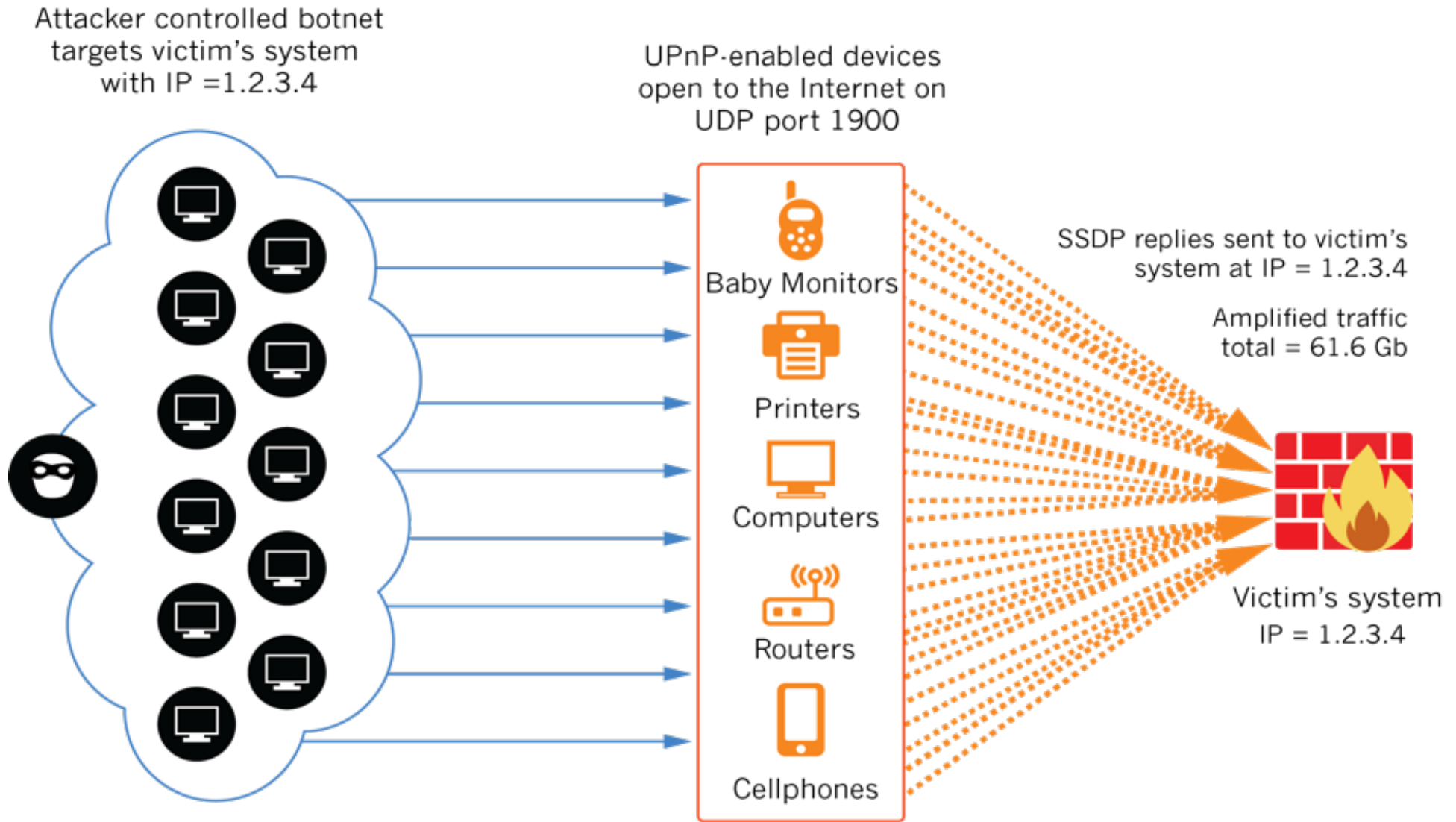
- Can result in the initial traffic from the attacker being amplified by a factor of 30 ^[1]

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

- As of 08/30/16, Shadowserver reported 7,864,584 unique IPs with open SSDP; see <https://ssdpSCAN.shadowserver.org/stats/>

[1] <http://www.us-cert.gov/ncas/alerts/TA14-017A>

SSDP Amplification Attack



Botnet systems send SSDP requests (UDP port 1900) using spoofed source IP of victim (IP = 1.2.3.4)

Total size of all requests = 2 Gb

Real life attack using open SSDP

September 2014 report of attack using open SSDP [2]

- Documented traffic at a rate of 476 Megabits/second (Mb/s)
- Traffic originated from 111,000 different IP sources

The second half of 2014 saw a dramatic rise in the number of attacks using open SSDP [3]

Most significant impact is downstream impacts to others who are targeted victims of such attacks

[2] <https://blog.sucuri.net/2014/09/quick-analysis-of-a-ddos-attack-using-ssdp.html>

[3] <https://www.arbornetworks.com/arbor-networks-atlas-data-shows-reflection-ddos-attacks-continue-to-be-significant-in-q3-2014>

Potential impacts from SSDP 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 SSDP 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 SSDP attacks

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

Open SSDP 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 SSDP

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 SSDP

The best way to mitigate risks from open SSDP moving forward is to not purchase or deploy devices with UPnP enabled on outside interfaces

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



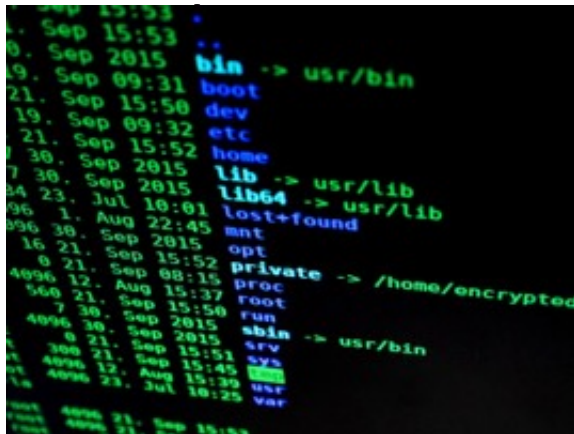
Identify your open SSDP risk

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

- Many devices may be running SSDP without your knowledge
- Additional vulnerabilities in UPnP discovered that could pose additional, direct risk to organizations

that allow SSDP from the Internet

- Mitigation strategies should include addressing known vulnerabilities



Find hosts running SSDP



In a shell window, start tcpdump:

```
tcpdump -n host [IP]
```

In a second shell 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 lot of traffic in the first shell window (running tcpdump)

Mitigation: Block SSDP at network edge



SSDP generally not needed across the Internet

Organizations should deploy firewall rules that block inbound port 1900/udp

- If you need SSDP or UPnP, restrict access to only allow trusted hosts on that port
- If you run applications across the Internet that depend on UPnP and you block the service, some applications may continue to work with lesser performance
 - E.g. Microsoft Live Messenger uses UPnP for file transfers; if UPnP is not available, it will use a proxy server from Microsoft that may be more congested

Mitigation: Block SSDP




Use Access Control Lists (ACLs) to restrict SSDP at border routers


Please refer to your specific vendor documentation for instructions on how to implement these changes

Blocking SSDP from Internet or disabling only on Internet will preserve local network functionality



Mitigation: Disable UPnP

 If blocking or upgrading UPnP is not an option, **disable UPnP**, particularly on Internet-accessible devices

 UnPlug n' Pray utility from Gibson Research Company helps consumers shut down and disable UPnP on their Windows devices - available for free at <https://www.grc.com/unpnp/unpnp.htm>

Mitigation: Update UPnP devices



Vulnerabilities in UPnP pose additional risk

- Two most commonly used UPnP software libraries contain vulnerabilities ^[4] that are remotely exploitable through a single UDP packet, which can be forged
- Some vulnerabilities would allow remote, unauthenticated attackers to scan internal hosts or proxy Internet traffic through the device

Contact your vendor to find out if a firmware update is available

- <http://www.kb.cert.org/vuls/id/357851>
- <https://web.nvd.nist.gov/view/vuln/search-results?query=ssdp>
- <https://web.nvd.nist.gov/view/vuln/search-results?query=udp>

[4] <https://community.rapid7.com/community/infosec/blog/2013/01/29/security-flaws-in-universal-plug-and-play-unplug-dont-play>

Spoofer Traffic Mitigation: Implement ingress filtering on networks



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

- Detail configuration changes to substantially reduce potential for source IP spoofed attacks of all kinds (the most popular types of DDoS attacks)
 - 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

Consider rate limited UDP fragments

- Note: Blocking UDP fragments negatively affects session initiation protocol (SIP), the protocol for Voice over IP (VoIP), and other text and multimedia sessions like instant messaging, video, online games and other services

Verify your fix



Re-run the command:

```
tcpdump -n host [IP]
```

Ensure open SSDP is not enabled again in the future and monitor your infrastructure by subscribing to free reports from Shadowserver:

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



Additional SSDP resources

<https://www.akamai.com/uk/en/multimedia/documents/state-of-the-Internet/ssdp-reflection-ddos-attacks-threat-advisory.pdf>

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

<http://www.kb.cert.org/vuls/id/922681>

<http://www.upnp-hacks.org/faq.html>

<http://community.rapid7.com/docs/DOC-2150>

<https://threatpost.com/50-million-potentially-vulnerable-upnp-flaws-012913/77465/>

<http://www.darkreading.com/attacks-breaches/report-iot-connected-devices-leading-to-rise-in-ssdp-based-reflection-attacks-/d/d-id/1320149>

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

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 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 these 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?

 Manually disabling SSDP takes a few minutes per device

 System administrators in smaller organizations need an 1-2 hours per perimeter device to investigate, implement and verify the basic mitigation of using firewall or ACLs to block access to SSDP

 ISPs and large entities can automate administration changes with configuration management (Salt, Ansible)



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, IJ
- 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.



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