# Your Bitcoins, or Your Site!

*An Overview of the DD4BC*
*2014-2015 DDoS Extortion Campaign*

Roland Dobbins <rdobbins@arbor.net>
*Principal Engineer, ASERT*

# Introduction & Context

# DDoS Background

What is a **D**istributed **D**enial **o**f **S**ervice (DDoS) attack?

- An attempt to **consume** finite **resources**, **exploit weaknesses** in software design or implementation, or **exploit lack** of infrastructure **capacity**

- Targets the **availability** and **utility** of computing and network resources

- Attacks are almost always **distributed** for even more significant effect (i.e., DDoS)

- The **collateral damage** caused by an attack can be as bad, if not worse, than the attack itself

- **DDoS attacks affect availability**!  No availability, no applications/services/data/Internet!  No revenue!

- DDoS attacks are attacks **against capacity and/or state**!

# Three Security Attributes

**Availability**

**Confidentiality**

**Integrity**
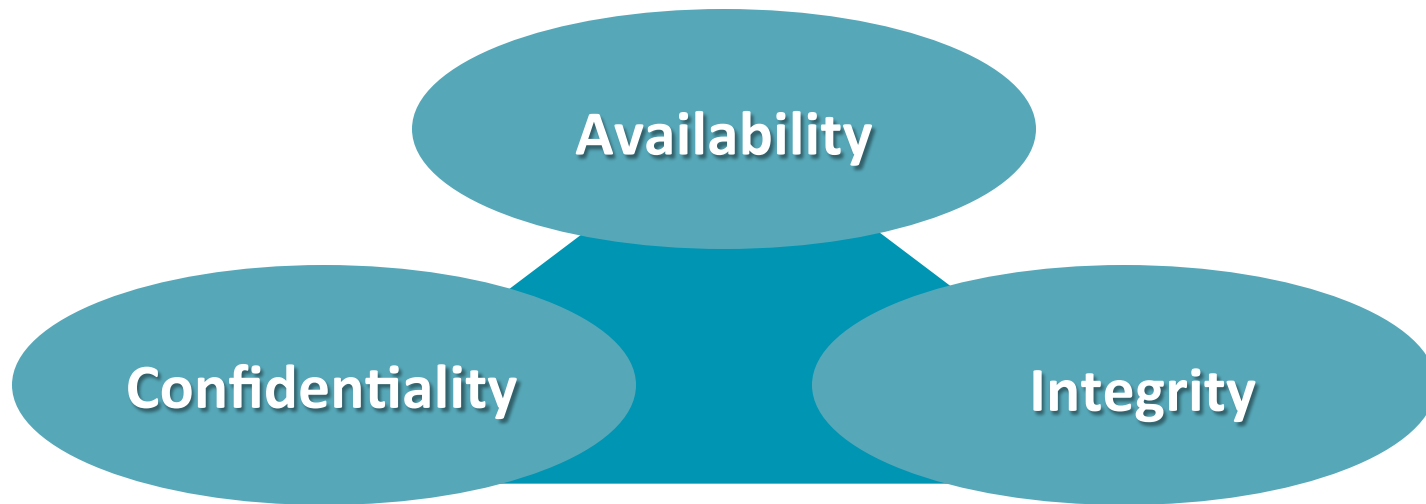
- The goal of security is to maintain these three attributes.

# Three Security Attributes



- The primary goal of DDoS defense is maintaining availability in the face of attack

# A Brief History of DDoS Extortion

# Blackmail vs. Extortion.

- Blackmail = someone threatens to release potentially damaging information about the victim unless he receives payment (this is how the Ashley Madison imbroglio started off).

- Extortion = someone threatens to take some harmful action against the victim unless he receives payment.

- Blackmail these days often uses Skype, webcams, etc.

- Extortion these days often uses DDoS attacks.

## Way Back in the Earlies

- First DDoS attacks on nascent Internet related to IRC channel disputes, 'warez' scene in the late 1980s/early 1990s.

- First DDoS extortion related to both IRC and 'warez' – i.e., 'give me ops in your channel', 'give me your 0-day warez first'.

- Mostly confined to IRC protocols like CTCP, DCC.

- Graduated to ICMP – this is when DDoS started to become a more general problem on the Internet.

- SYN-flooding started in 1995. Other methods followed.

## DDoS Extortion Goes Commercial

- First monetary DDoS extortion emerged in the late 1990s.

- Targeted 'fringe' online businesses – online gambling operations, 'adult' entertainment.

- Early DDoS extortion activity emerged in Caribbean, Latin America – lots of early 'fringe' online businesses established there in order to evade U.S. and European laws, regulations, scrutiny.

- ISPs who tried to help targeted customers threatened with being DDoSed out of existence (this has happened multiple times over the years).

- Some ISPs decided this was a good model – stood aside and encouraged attackers in exchange for a portion of the 'take'.

- A few ISPs even helped attackers identify targets!

9

# DDoS Extortion Becomes the New Normal

- DDoS extortion has been around as long as the Internet.

- Totally subjective estimate that extortion is the motive behind ~15% of DDoS attacks.

- Many ideologically-motivated DDoS attacks are actually a form of extortion – trying to force the targeted organization to stop doing something the attackers find objectionable, or start doing something the attackers find desirable.

- Early commercial DDoS extortion rackets used wire transfers to collect payments – route through multiple banks, hard to trace (at the time).

- Payoff channels migrated to Western Union, PayPal, eGold (remember them)?, other early online pseudo-fiat currencies.

- Some payoffs in material goods purchased by extortee via credit cards, delivered to drop addresses.

- A lot of intra-miscreant DDoS is extortion – demanding CC dumps, etc.

# What is Bitcoin?

# What is Bitcoin?

## What is Bitcoin?

- Decentralized, anonymous, digitally-generated (by Bitcoin 'mining') crypto-currency.

- Transactions are verifiable, recorded in a public distributed ledger.

- Not the first crypto-currency, but the most popular and well-known.

- All transactions are public.

- Fees lower than credit cards, paid by purchaser.

- Lots of criminal activity around Bitcoin – theft of Bitcoins from electronic 'wallets', botnets set up to covertly mine Bitcoins, payment for illicit goods/services, etc.

- DDoS used for Bitcoin valuation manipulation by DDoSing Bitcoin miners, thereby affecting expansion of Bitcoin currency volume.

- Most ordinary people have either never heard of it or have no idea what it actually is or how it works.

# Why Use Bitcoin for DDoS Extortion Payouts?

- Accepted/convertible internationally.

- Potentially anonymous, like cash.

- Difficult to trace through multiple transactions.

- Until recently, Bitcoin was a high-valuation currency.

- No need to involve government agencies, regulated entities in Bitcoin transactions.

- No tax (practically speaking).

- Victims can potentially mine more Bitcoin for themselves – not directly tied to physical-world labor/compensation exchanges.

## Disadvantages of Using Bitcoin for Extortion Payouts

- Myth that it's 'untraceable' – untrue, it can be traced, somewhat analogous to serial numbers on physical cash.

- Potentially easier to trace than cash.

- Potentially more susceptible to theft than cash.

- Highly volatile, conversion rates swing up and down.

- Many of the victims *have never heard of it*, and/or *have no idea* how to get their hands on Bitcoins.

## What is DD4BC?

- A threat actor who launches DDoS extortion attacks against organizations, demanding payment to cease the attacks in Bitcoin.

- DD4BC = 'DDoS for Bitcoins'

- Self-labeled acronym.  Often mangled in conversation, news articles, etc.

- Currently the most notorious DDoS attacker in both the public and the operational security spheres.

# Genesis of DD4BC

# DD4BC Makes Its Debut

- First emerged in July 2014, debuted with DDoS extortion attempt against Bitcoin lotto sites (yes, that is a thing).

- Attacked online Bitcoin-based online sports betting house about a week later.

- This second verified DD4BC attack was the first known instance of a DD4BC victim paying – the victim initially paid off DD4BC in order to buy time to put defenses in place, mitigated subsequent attacks.

- Contrary to claims of one-time-only payment, DD4BC kept hitting up the betting house week after week, until they could defend against the attacks.

- Throughout the rest of 2014, DD4BC attacked various Bitcoin mining pools, Bitcoin exchanges, Bitcoin wallet providers, etc., mostly in Europe and North America.

- Most/all targets were Bitcoin-savvy.

- Extortion demands have ranged from 1 – 100 Bitcoins: approximately $227USD - $22,700USD.

## 'Fringe' Businesses – the Pattern Repeats

- Online betting shops, even when they're legal, are generally viewed as being on the edges of legitimate commerce. They generally aren't eager to engage with the authorities.

- Likewise for Bitcoin miners, Bitcoin exchanges, etc. They tend to try and keep as far away from 'official' notice as possible.

- In many cases, authorities regard these types of businesses with mutual suspicion, aren't overly eager to help.

- And of course, law enforcement action against DDoS attackers in general nets very few arrests/convictions – almost all of those who end up behind bars/fined essentially ratted themselves out by bragging about their crimes.

# Broadening the Campaign

## Going After the Financials


"That's Where the Money is…"
— Willie Sutton

# Going After the Financials

- In 2015 Q2, DD4BC shifted its target base to financial institutions - largely to the exclusion of Bitcoin-specific organizations - as well as to e-commerce sites.

- So far, DD4BC has attacked financial institutions in Central and Western Europe, Switzerland, Guernsey, Iceland, North America (relatively few), Australia, New Zealand, and Japan.

- Ancillary financial services organizations such as ACH processors and other types of non-customer-facing specialties have also been attacked.

- No financial organization has publicly admitted to paying DD4BC, but at least one has done so.

- Most of the financial institutions attacked so far have been mid-tier and smaller, with only a few considered to be first-tier.

- Previously, DD4BC issued far more threats than attacks, and abandoned unsuccessful attacks quickly. This has changed – more attacks carried out, greater persistence.

# Not Just Banks!

- DD4BC has also attempted to extort ISPs and e-commerce sites.

- In Europe, DD4BC spammed thousands of users of a shared hosting provider with DDoS extortion demands emailed to 'abuse@', 'security@', and 'root@' email addresses.

- This is atypical of DD4BC; most DD4BC extortion emails are deliberately targeted at specific organizations.

- E-commerce sites have also been threatened and attacked.

- Online gambling sites and sports betting shops are still being targeted, as well.

- DD4BC has attacked specific customers of several IaaS and VPS providers, in some cases causing significant collateral damage to multiple customers of those services.

# Evolution of DD4BC Modus Operandi

# Typical DD4BC Extortion Process

- Unannounced DDoS attack against targeted organization, 10-15gb/sec, anywhere from 15 minutes to an hour in length.

- DD4BC then send email extortion demand providing detailed knowledge of DDoS attack, demanding payment within 24 hours.

- If the victim doesn't pay, follow-up email increases the amount of Bitcoin payout, and threatens another DDoS attack – up to 60gb/sec observed.  DD4BC claim 400gb/sec of DDoS attack generation capability, but this hasn't been borne out, so far.

- DD4BC DDoSes some (not all) targets who don't pay, sends repeated emails demanding increased extortion payout amounts.

- DD4BC will increase the demanded extortion payouts if the target takes inadequate defensive measures.

# Typical DD4BC Extortion Process (cont.)

- DDoS attacks persist anywhere from a few hours to 12 hours to a series of attacks over multiple days.

- If the DDoS attack is successfully thwarted, DD4BC will eventually give up and go away.

- Sometimes, DD4BC will target the same organization again, a few days or weeks later.

- On a couple of occasions, DD4BC has re-targeted the same organization dozens of times.

# Typical DD4BC Initial Extortion Demand

From: DD4BC Team [mailto:dd4bct@gmail.com] Sent: 10 April 2015 02:07 PM
Subject: Re: DDOS ATTACK!

Hitting example.com at the moment.

Good luck if you think you can stop what they can't. But you still have time.

On Thu, Apr 9, 2015 at 3:46 PM, DD4BC Team <dd4bct@gmail.com> wrote: Hello,

To introduce ourselves first:

https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html http://bitcoinbountyhunter.com/bitalo.html

http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses- ccedk-of-withholding-info

Or just google "DD4BC" and you will find more info.

Recently, we were DDoS-ing example.net. You probably know it already.

So, it's your turn!

<site> is going under attack unless you pay 20 Bitcoin. Pay to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother.

Right now we are running small demonstrative attack on your server.
Don't worry, it will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 20 BTC at the moment, so we are giving you 48 hours to get it and pay us.

We do not know your exact location, so it's hard to recommend any Bitcoin exchanger, so use Google. Current price of 1 BTC is about 250 USD.

IMPORTANT: You don't even have to reply. Just pay 20 BTC to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z – we will know it's you and you will never hear from us again.
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service.

But if you ignore us, and don't pay within 48 hours, long term attack will start, price to stop will go to 50 BTC and will keep increasing for every hour of attack.

ONE MORE TIME: It's a one-time payment. Pay and you will not hear from us ever again!

# Typical DD4BC Initial Extortion Demand

- Date: Sun, 15 Feb 2015 17:42:31 +0000
  From: "DD4BC Team" <dd4bc@Safe-mail.net>

- btw. Attack temporarily stopped.
  If payment not received within 6 hours, attack restarts and price will double up.


- -------- Original Message --------


- From: "DD4BC Team" <dd4bc@Safe-mail.net>
  Subject: DDOS ATTACK!
  Date: Sun, 15 Feb 2015 12:34:28 +0000

- Hello,
  Your site is extremely vulnerable to DDoS attacks.
  I want to offer you info how to properly setup your protection, so that you can't be ddosed. If you want info on fixing it, pay me 1.5 BTC to 1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6

# Typical DD4BC Initial Extortion Demand

From: "DD4BC Team" <dd4bc@Safe-mail.net>

Date: Mon, 16 Feb 2015 14:13:40 +0000

Subject: Re: DDOS ATTACK!

Return site back online without paying me first, it's going down again (protection will not help) and price to stop it increases to 3 BTC. And will keep doubling for every day of attack.

-------- Original Message --------

From: "DD4BC Team" <dd4bc@Safe-mail.net>
Subject: DDOS ATTACK!
Date: Sun, 15 Feb 2015 12:34:28 +0000

Hello,
Your site is extremely vulnerable to DDoS attacks.
I want to offer you info how to properly setup your protection, so that you can't be ddosed. If you want info on fixing it, pay me 1.5 BTC to
1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6

# Initial DD4BC Attack Profile

- DD4BC first attacked targets with a mixture of ntp, SSDP, and DNS reflection/amplification attacks, with SYN-flooding mixed in, from time to time.

- As time progressed, ntp and SSDP reflection/amplification became the primary vectors, with occasional SYN-floods.

- If a targeted organization successfully defends against one attack vector, DD4BC will shift to another one.

- ntp and SSDP reflection/amplification vectors are sometimes used simultaneously.

- DD4BC concentrates attacks on the Web sites of targeted organizations.

- DD4BC typically attacks only one target at a time.

# DD4BC Relies on Booters/Stressers

- It appears that DD4BC has settled on utilizing commercial 'booter'/'stresser' services to launch DDoS attacks.

- While these masquerade as testing tools, they're actually cloud-based DDoS attack services; attackers typically pay hourly rates to use them (mainly in Bitcoins, of course).

- As various booter/stresser services have expanded their attack offerings, DD4BC has broadened its DDoS attack methodologies to include chargen reflection/amplification and WordPress XMLRPC 'pingback' DDoS attacks.

- DD4BC has largely adopted a 'cookie-cutter', standardized approach to attacking extortion targets.

- DD4BC will react to successful DDoS defense, varying attack methodologies (SSDP to ntp to SYN-flooding to WordPress XMLRPC 'pingback) and increasing attack bandwidth.

# DD4BC Relies on Booters/Stressers

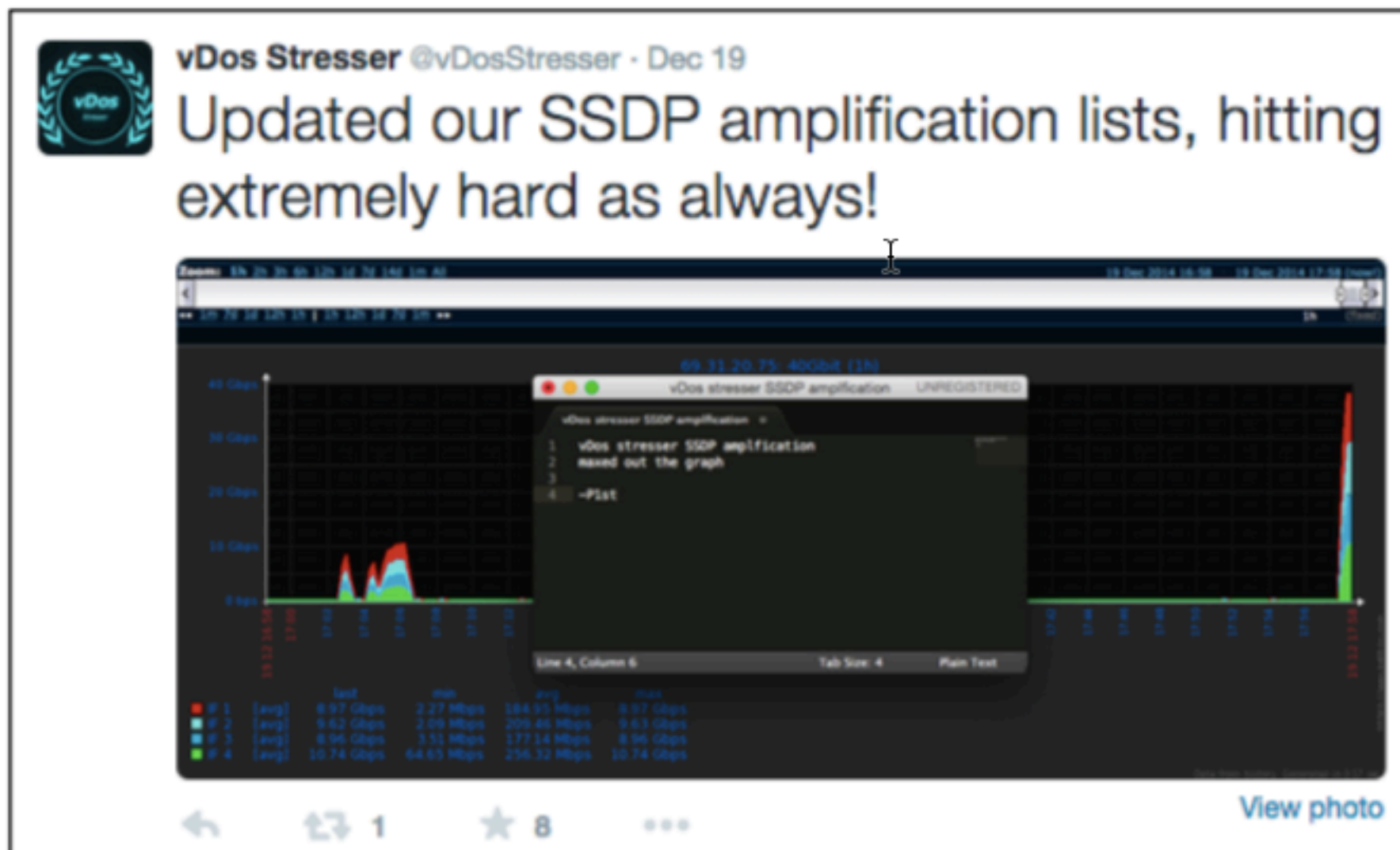## DD4BC Relies on Booters/Stressers

# SSDP/UPnP Innovation – Leveraging Services Behind CPE

- We have observed DD4BC utilizing a relatively new variation on SSDP/UPnP reflection/amplification attacks.

- If typical SSDP reflection/amplification attacks are thwarted, DD4BC will shift attack modes from sending M-Search enumeration queries (thus stimulating M-Search enumeration responses to DDoS the target) to issuing spoofed UPnP presentation page requests to specific UPnP-gatewayed services running on the private LANs of abusable UPnP CPE devices.

- This stimulates the services running behind the CPE devices to respond with HTTP/U packets of ~300 – 500 bytes, sourced from UPnP-mapped ephemeral ports on the abusable CPE, targeting the destination port of the attacker's choice.
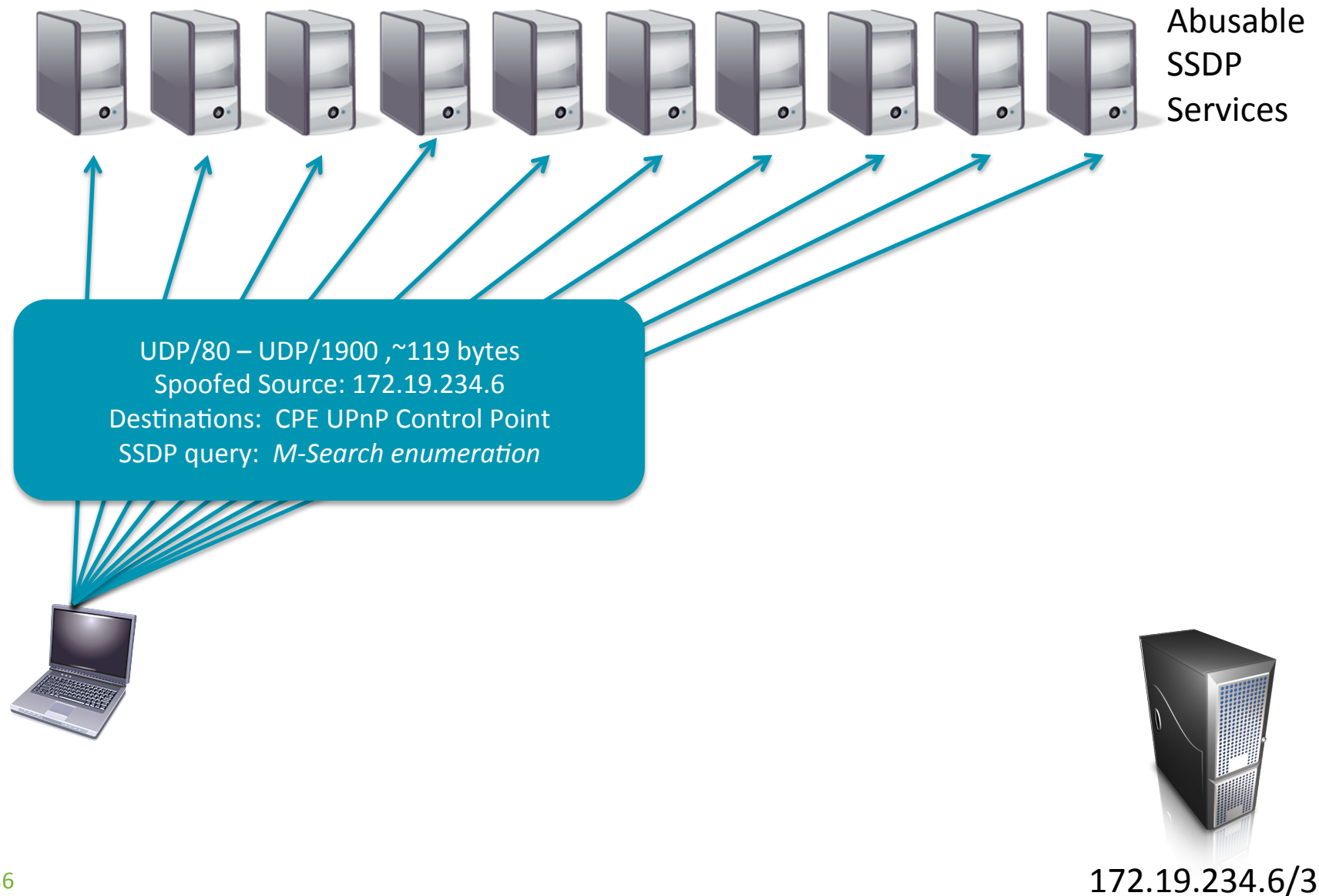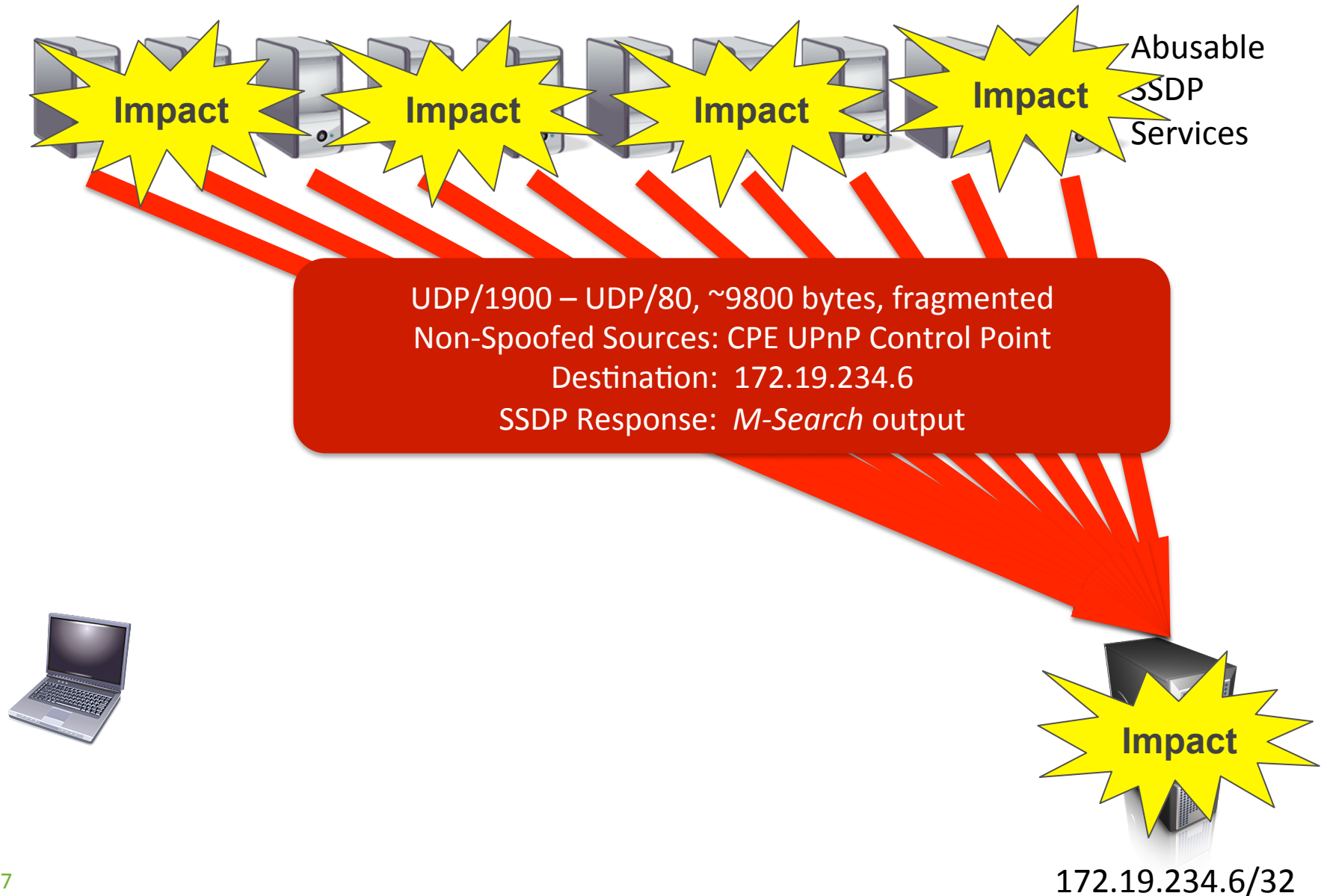
# Typical SSDP Reflection/Amplification Attack

Abusable SSDP Services

Internet-Accessible CPE devices, old Windows XP boxes, etc.

172.19.234.6/32

# Typical SSDP Reflection/Amplification Attack

Abusable
SSDP
Services

UDP/80 – UDP/1900 ,~119 bytes
Spoofed Source: 172.19.234.6
Destinations:  CPE UPnP Control Point
SSDP query:  *M-Search enumeration*

172.19.234.6/32

# Typical SSDP Reflection/Amplification Attack



Abusable SSDP Services

**Impact**  **Impact**  **Impact**  **Impact**

UDP/1900 – UDP/80, ~9800 bytes, fragmented
Non-Spoofed Sources: CPE UPnP Control Point
Destination:  172.19.234.6
SSDP Response:  *M-Search* output

**Impact**

172.19.234.6/32

# UPnP HTTP/U Services Reflection/Amplification Attack

Abusable
SSDP
Services

Services running *behind* Internet-Accessible CPE devices, old Windows XP boxes, etc.

172.19.234.6/32

# UPnP HTTP/U Services Reflection/Amplification Attack

Abusable
SSDP
Services

UDP/80 – UDP/32768, variable size
Spoofed Source: 172.19.234.6
Destinations:  CPE UPnP Control Point
UPnP presentation query:  *HTTP/U GET*

172.19.234.6/32

# UPnP HTTP/U Services Reflection/Amplification Attack

Abusable
SSDP
Services

**Impact**   **Impact**   **Impact**   **Impact**

UDP/32768 – UDP/80, ~300 – 500 bytes
Non-Spoofed Sources: CPE UPnP Control Point
Destination:  172.19.234.6
UPnP presentation response:  *HTTP/U  response*

**Impact**

40

172.19.234.6/32

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/qatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e::urn:schemas-upnp-
org:device:InternetGatewayDevice:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e::urn:schemas-upnp-
org:device:InternetGatewayDevice:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP devices/1.6.6

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e::urn:schemas-upnp-org:device:InternetGatewayDevice:1

# Layer-7 Decodes of UPnP HTTP/U Responses

HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP devices/1.6.6

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1

USN: uuid:75802409-bccb-40e7-8e6c-fa095ecce13e::urn:schemas-upnp-org:device:InternetGatewayDevice:1

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 23:09:56 GMT

EXT:

LOCATION: http://192.168.1.1:49154/gatedesc.xml

SERVER: Linux/2.6.34.10_sd5115h_v100f, UPnP/1.0, Portable SDK for UPnP
devices/1.6.6

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1

USN: uuid:75802409-bccb-40c7-8c6c-fa005ccce13e::urn:schemas-upnp-
org:device:InternetGatewayDevice:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=100

DATE: Fri, 12 Jun 2015 15:09:04 GMT

EXT:

LOCATION: http://222.208.210.248:49156/TxMediaRenderer_desc.xml

OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01

01-NLS: 78f69340-1110-11e5-8cd7-cad0e7b6b491

SERVER: 6.1.7601 2/Service Pack 1, UPnP/1.0, Portable SDK for UPnP devices/
1.6.17

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:service:AVTransport:1

USN: uuid:a348ae6e889af22ceade28c7a4551931_MR::urn:schemas-upnp-
org:service:AVTransport:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=100

DATE: Fri, 12 Jun 2015 15:09:04 GMT

EXT:

LOCATION: http://222.208.210.248:49156/TxMediaRenderer_desc.xml

OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01

01-NLS: 78f69340-1110-11e5-8cd7-cad0e7b6b491

SERVER: 6.1.7601 2/Service Pack 1, UPnP/1.0, Portable SDK for UPnP devices/
1.6.17

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:service:AVTransport:1

USN: uuid:a348ae6e889af22ceade28c7a4551931_MR::urn:schemas-upnp-
org:service:AVTransport:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=100

DATE: Fri, 12 Jun 2015 15:09:04 GMT

EXT:

LOCATION: http://222.208.210.248:49156/TxMediaRenderer_desc.xml

OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01

01-NLS: 78f69340-1110-11e5-8cd7-cad0e7b6b491

SERVER: 6.1.7601 2/Service Pack 1, UPnP/1.0, Portable SDK for UPnP devices/
1.6.17

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:service:AVTransport:1

USN: uuid:a348ae6e889af22ceade28c7a4551931_MR::urn:schemas-upnp-
org:service:AVTransport:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=100

DATE: Fri, 12 Jun 2015 15:09:04 GMT

EXT:

LOCATION: http://222.208.210.248:49156/TxMediaRenderer_desc.xml

OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01

01-NLS: 78f69340-1110-11e5-8cd7-cad0e7b6b491

SERVER: 6.1.7601 2/Service Pack 1, UPnP/1.0, Portable SDK for UPnP devices/
1.6.17

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:service:AVTransport:1

USN: uuid:a348ae6e889af22ceade28c7a4551931_MR::urn:schemas-upnp-
org:service:AVTransport:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=100

DATE: Fri, 12 Jun 2015 15:09:04 GMT

EXT:

LOCATION: http://222.208.210.248:49156/TxMediaRenderer_desc.xml

OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01

01-NLS: 78f69340-1110-11e5-8cd7-cad0e7b6b491

SERVER: 6.1.7601 2/Service Pack 1, UPnP/1.0, Portable SDK for UPnP devices/
1.6.17

X-User-Agent: redsonic

ST: urn:schemas-upnp-org:service:AVTransport:1

USN: uuid:a348ae6e889af22ceade28c7a4551931_MR::urn:schemas-upnp-
org:service:AVTransport:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 15:09:57 GMT

EXT:

LOCATION: http://169.254.39.32:49152/wps_device.xml

SERVER: Unspecified, UPnP/1.0, Unspecified

ST: urn:schemas-wifialliance-org:service:WFAWLANConfig:1

USN: uuid:56eb2067-c465-582f-b238-6cb0ce1987f1::urn:schemas-wifialliance-
org:service:WFAWLANConfig:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

```
HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 15:09:57 GMT

EXT:

LOCATION: http://169.254.39.32:49152/wps_device.xml

SERVER: Unspecified, UPnP/1.0, Unspecified

ST: urn:schemas-wifialliance-org:service:WFAWLANConfig:1

USN: uuid:56eb2067-c465-582f-b238-6cb0ce1987f1::urn:schemas-wifialliance-
org:service:WFAWLANConfig:1
```

# Layer-7 Decodes of UPnP HTTP/U Responses

HTTP/1.1 200 OK

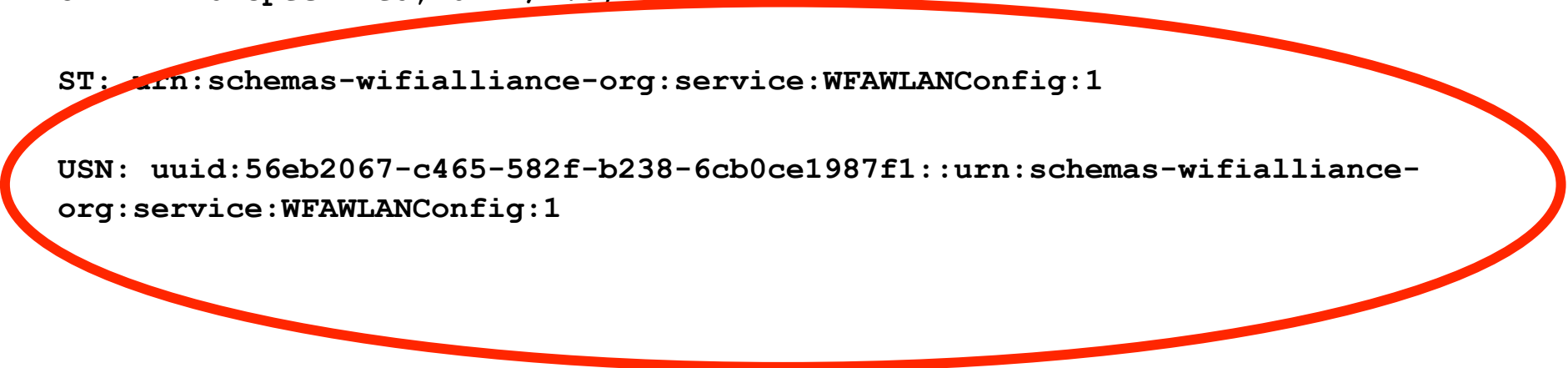CACHE-CONTROL: max-age=1800

DATE: Fri, 12 Jun 2015 15:09:57 GMT

EXT:

LOCATION: http://169.254.39.32:49152/wps_device.xml

SERVER: Unspecified, UPnP/1.0, Unspecified

ST: urn:schemas-wifialliance-org:service:WFAWLANConfig:1

USN: uuid:56eb2067-c465-582f-b238-6cb0ce1987f1::urn:schemas-wifialliance-org:service:WFAWLANConfig:1

# Who or What is DD4BC?

# What Do We Think We Know About DD4BC?

- Based on the language used in DD4BC extortion threat email messages, we believe DD4BC is fluent in English, but English isn't DD4BC's primary language.

- DD4BC has demonstrated ignorance of the US Fourth of July holiday, sending repeated extortion demands to US-based financial institutions during this long weekend. As this is the most well-known US holiday apart from Christmas/New Year's Day, it is unlikely DD4BC is familiar with American culture.

- The fact that DD4BC only appears to attack one target at a time indicates that DD4BC may well be a single individual. DD4BC remaining at large also tends to support this theory.

- DD4BC is reasonably tech-savvy (Bitcoin, DDoS attacks), but does not appear to be a high-level technical expert – hence, the reliance on booter/stresser services.

- DD4BC does not seem to fully realize that attacking financial institutions attracts the attention of LEAs far more than attacking Bitcoin-related sites and online gambling/casino organizations
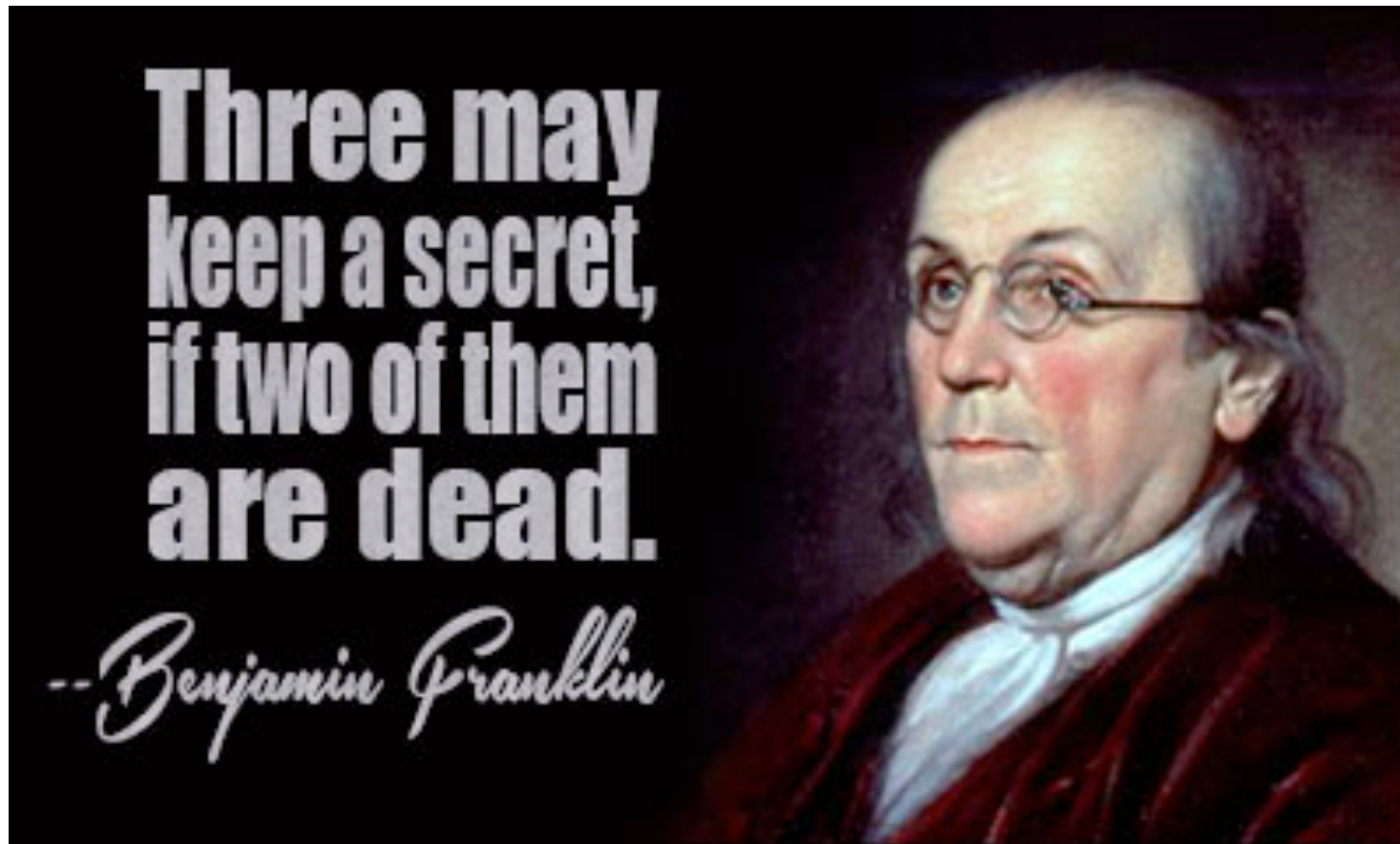
# Why Hasn't DD4BC Been Caught?

- Reasonably good operational security – no bragging (this is how the few DDoSers who are caught give themselves away, in most cases)

- Started out attacking 'fringe' organizations – online casinos, lottos, sports betting shops.  LEA in many jurisdictions don't always put a high priority on attacks against these types of organizations.

- Attacks are distributed across many geographies and countries.

- DD4BC is willing to cut losses and abandon attacks against well-defended targets, is not generally very persistent.

- Despite claims of 400gb/sec of DDoS attack traffic capacity, largest known DD4BC attack volume is 60gb/sec – this is non-trivial, but does not always choke peering links, disrupt bystander traffic, etc.

- DD4BC attacks tend to be sporadic, both jurisdictionally and chronologically.  One target at a time.

- If DD4BC is an individual, this would also contribute to avoiding capture, assuming no bragging/loose lips.

Three may keep a secret, if two of them are dead.
--Benjamin Franklin

# DD4BC Today & Tomorrow

# Imitation is the Most Sincere Form of Flattery

- DD4BC has gained enough notoriety (in part because of its longevity and broadening its target base to the financial sector) that there are several DD4BC copycats operating.

- Analysis of the copycat extortion threat emails makes it clear that these email messages were not composed by the original DD4BC, and that whoever composed them is not as fluent in English as is DD4BC.

- The DD4BC copycats have also resorted to posting DDoS extortion threat targets and attack timetables (shades of Operation Ababil) on Pastebin and regional Pastebin-equivalent sites.

- The UPnP variant DDoS attack utilized by DD4BC is not known to have been utilized by DD4BC copycats, to date.

# Projected Evolution of DD4BC

- As booter/stresser DDoS attack methodologies expand, DD4BC will likely take advantage of them, as with the WordPress XMLRPC pingback attacks and the SSDP HTTP/U services attack variant.

- DD4BC will likely target more organizations in Asia, though the language barrier will likely limit the efficacy of doing so.

- The same holds true of Latin/South America and Africa – language will be an impediment.

- DD4BC will likely expand to other verticals.

- DD4BC may begin employing indirect attack vectors.

- DD4BC has gained the attention of LEAs, intelligence agencies, and security researchers worldwide.

- If DD4BC persists in attacking financial institutions, the likelihood of identification and capture is far higher than DD4BC seems to realize.

# Defending Against DD4BC

# All the Usual Recommendations, and Then Some

- Network infrastructure, server/service/application BCPs.

- Situationally-appropriate network access policies – e.g., ACLs – will keep out-of-profile attack traffic off servers, can be forward-emplaced on customer aggregation routers, mitigation center diversion gateways, etc.

- Organizations must have the ability to detect/classify/traceback DDoS attack traffic – flow telemetry.

- S/RTBH, flowspec, IDMS as reaction tools.

- If an extortion email is received, contact LEAs, ISPs, MSSPs immediately; share with appropriate vertical orgs and opsec groups.

- Simulate language difficulties, unfamiliarity with Bitcoin, etc. to buy time while contacting LEAs, ISPs, MSSPs, etc.

- Do not pay!

# Conclusion

## Conclusions

- DD4BC is prolific, long-running.

- DD4BC is reasonably skilled.

- DD4BC has reasonably good operational security.

- Monitors attacks and reacts to defensive measures.

- Knows when to cut losses.

- Is probably not American.

- May be an individual.

## Conclusions (cont.)

- Standard BCPs and detection/classification/ traceback/mitigation techniques work well against DD4BC DDoS attacks.

- Attack capacity maxes at ~60gb/sec, so far.

- Gradually adopts new DDoS vectors as booters/stressers add support.

- Has aroused the focus of LEA, intelligence, security researchers worldwide.

- Will go away if reasonable DDoS defensive measures are taken.

- Can be defeated!

# Discussion

# This Presentation – http://bit.ly/1F0Nfrc

**ARBOR**
NETWORKS

*Special thanks to Curt Wilson for his
contributions to this presentation.*

# Thank You!

Roland Dobbins <rdobbins@arbor.net>
*Principal Engineer, ASERT*