Travel Hacking: Hotel Edition

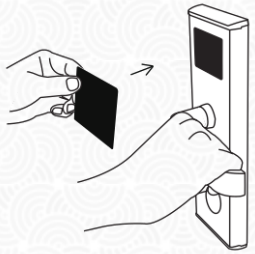
THIS SIDE UP
INSERT AND REMOVE

https://conference.hitb.org/hitbsecconf2018pek/
Beijing, China

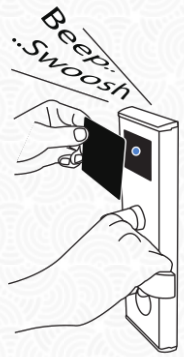
Made from 100% recycled plastic.

Hendrik Scholz
hs@123.org

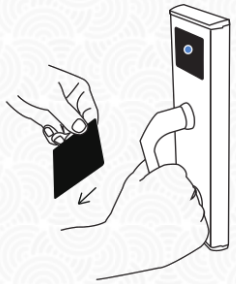
Agenda



Rationale



Data gathering



Analytics and application

Rationale

Why am I doing this?

Isn’t a hotel room just a room?

- Room vs. suite vs. villa
- Flexible vs. non-refundable rates
- Breakfast/dinner/club lounge inclusions
- (bonus) Loyalty points
- Airport transfers, included event/theme tickets

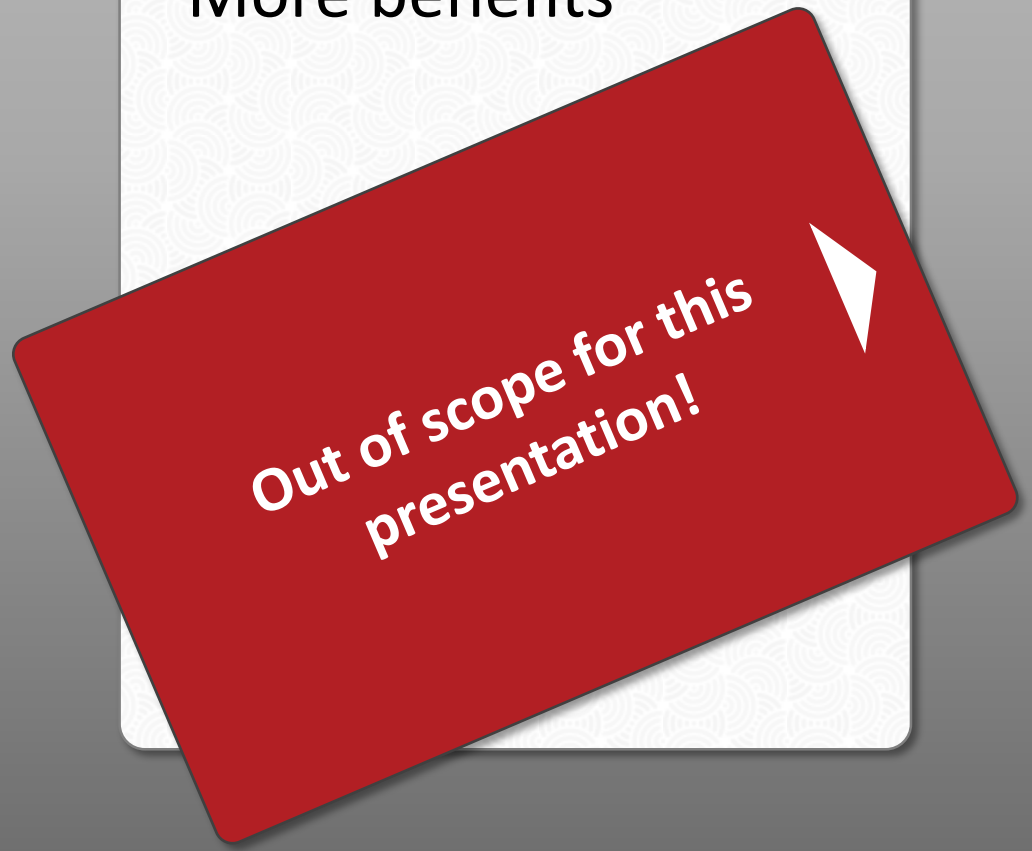
Hotel Hacking Goals

Two distinct types of travel

Mandatory travel

Fixed travel date and destination

- Save money
- Better room
- More benefits



Memorable travel

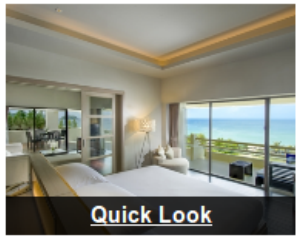
Flexible date and destination

- Great destinations
- Awesome suites and villas
- New experiences
- Affordable

$40 Suite at Hilton Phuket, Thailand

SUPERIOR DELUXE SUITE

138 sq. m. suite, panoramic ocean views, balcony, Executive ...



Rate plan	Price per night (THB) **Plus 10.00**% service charge per stay	
AARP AARP MEMBER SAVINGS PLUS 2PM LATE CHCKOUT BASED UPON AVAILABILITY...	฿1,235	Select
AAA STAY AND SAVE AAA STAY AND SAVE EXCLUSIVE AAA/CAA MEMBER SAVINGS. VALID AAA/ ...	฿1,235	Select
Best Available Rate Change or cancel up to 7 days before arrival.	฿1,300	Select
HONORS DISCOUNT Change or cancel up to 7 days before arrival. Pay when you stay. ... Pay with Points & Money	~~฿1,300~~ ฿1,235	Select
PREMIUM ROOM REWARDS **Hilton Honors Special** Premium Room Rewards allow Hilton Honors members to use points to... Pay with Points & Money	10,000 Hilton Honors Points	Select
BREAKFAST INCLUDED Change or cancel up to 7 days before arrival. Includes breakfast ...	฿1,600	Select

Intercontinental Honduras: Same price for all rooms

1 of 1

DELUXE ROOM 3

Bed type and smoking preference cannot be guaranteed and will be allocated upon arrival

View Rate Details

25,000 points per night
20,000 points + $40.00 USD per night
15,000 points + $70.00 USD per night

BOOK THIS ROOM

1 of 1

1 KING BED SUITE 2

High speed internet wire or wireless with an additional cost soundproof window feather duvet and pillows rainshower 37 inch LCD TV safety box for small laptop work equipped desk cd player alarm clock luxury amenities

View Rate Details

25,000 points per night
20,000 points + $40.00 USD per night
15,000 points + $70.00 USD per night

BOOK THIS ROOM

1 of 1

KING BED PRESIDENTIAL SUITE NONSMOKING 2

Nonsmoking presidential suite

View Rate Details

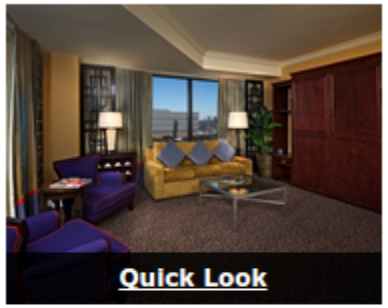
25,000 points per night
20,000 points + $40.00 USD per night
15,000 points + $70.00 USD per night

BOOK THIS ROOM

$39 room including $100 Food/beverage credit at Hilton Anatole Dallas

STANDARD PARLOR ROOM W/WALL BED

STANDARD PARLOR ROOM W/WALL BED 685 SQ. FT W/SITTING AREA HILTON ... Room Details



RATE PLAN	PRICE PER NIGHT (USD) plus 2.00% mandatory charge per stay, plus tax	
Best Available Rate Rate Details	$99	Select
BRKFST/PARKING/WIFI ★ Special offer INCLUDES BREAKFAST,PARKING, WIFI & VERANDAH CLUB ACCESS, SAVINGS ... Rate Details	$124	Select

View packages and promotions for this room

2X POINTS PACKAGE 2X POINTS PACKAGE GET REWARDED WITH DOUBLE HHONORS POINTS. NOT A ... Rate Details	$106	Select
DINE AND SAVE DINE AND SAVE $100 F/B CREDIT (INCLUDING SER) SELF PARKING Rate Details	$39	Select
STAY AND SEE DALLAS STAY AND SEE DALLAS SELF PARKING,BKST FOR UP TO 4 DAILY,IN-ROOM ... Rate Details	$124	Select

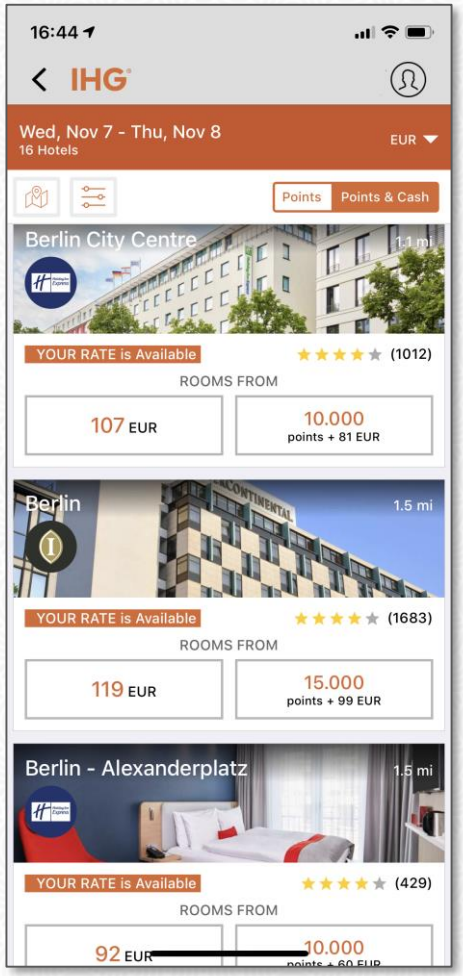
Data Gathering

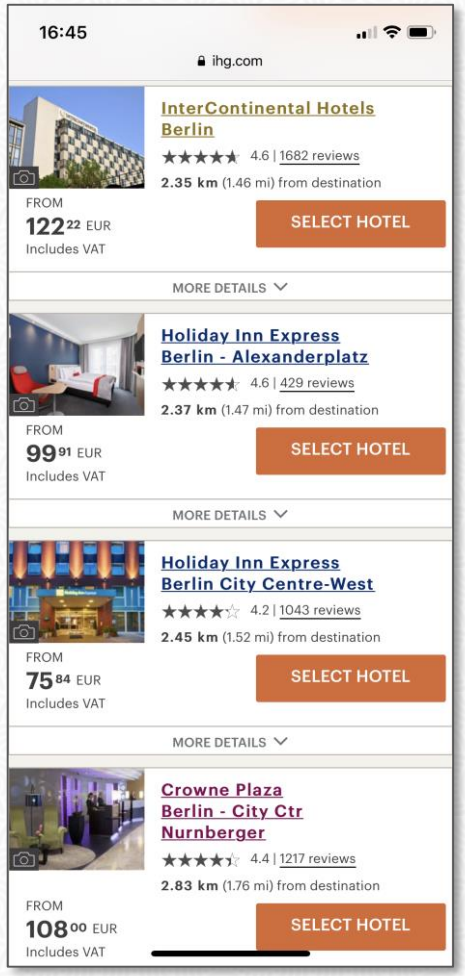
Web and app scraping

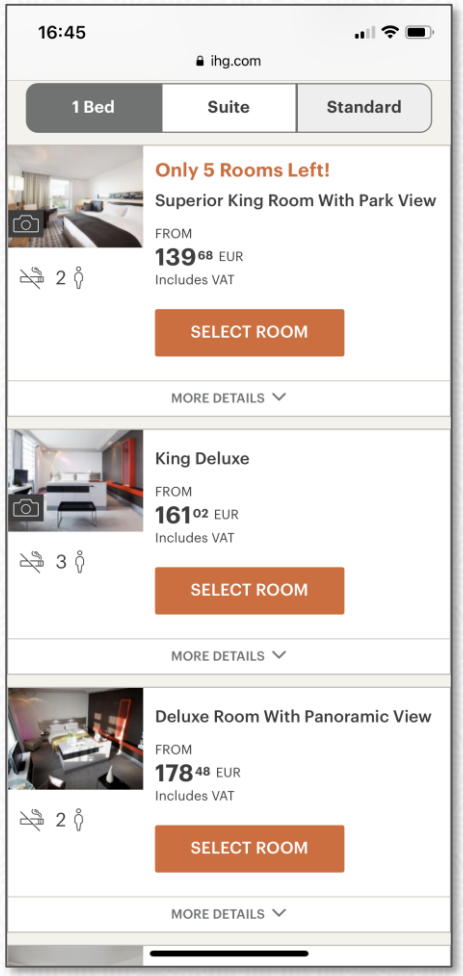
Reserve engineering APIs/Applications

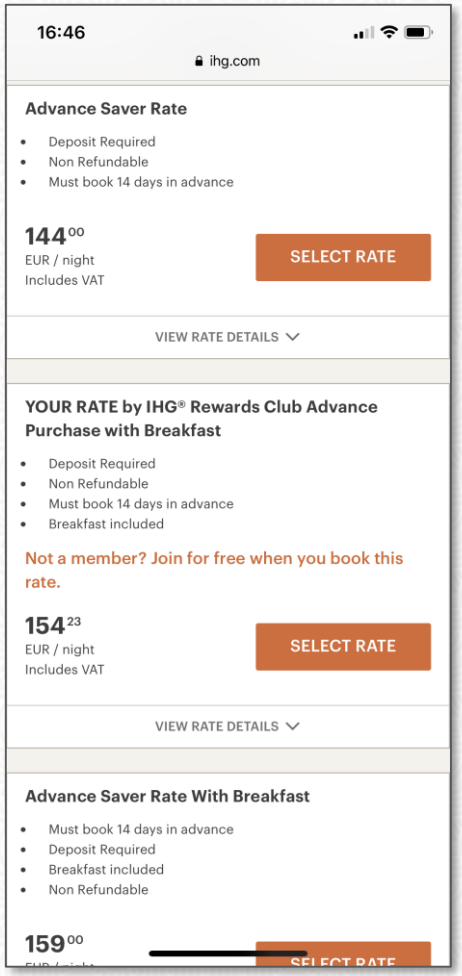
- Best entry point: mobile apps
  - ~30% of hotel chains have mobile-only API
  - Standard implementation: consumption of mobile website
- Less protection on mobile APIs
  - ‘My HTTP User-Agent string is my password’
- Android better target than IOS
  - Easy APK download and static code analysis
  - Fragmented Android version landscape
    - Longer supported APIs

IHG App and mobile website (m.ihg.com)

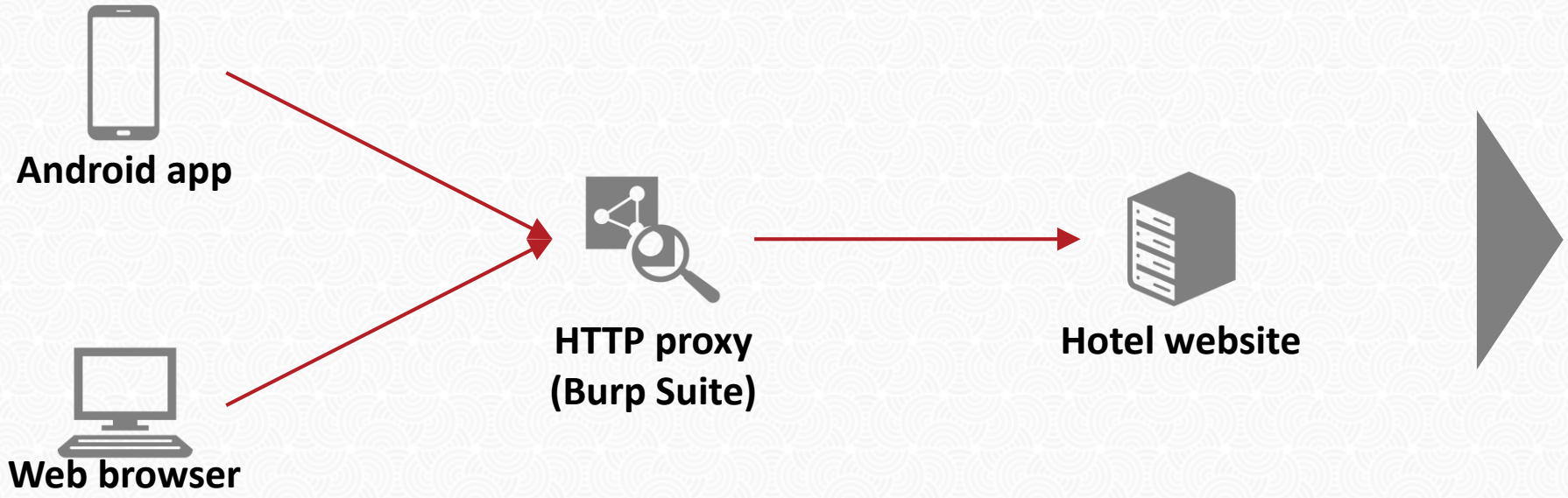








Reverse engineering APIs

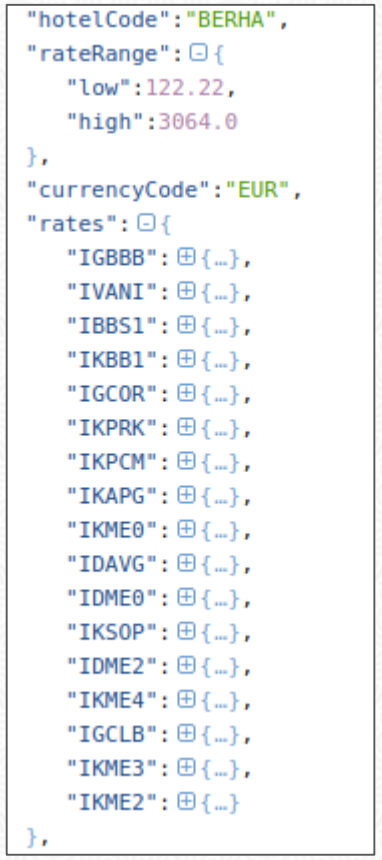


Reverse engineering details

- MITM tool
  - Burp Suite (https://portswigger.net/burp)
- Web browser
  - Set Burp as http/https proxy
  - Use User-agent plugin to pretend to be iPhone, Android, …
- Browse website (e.g http://m.ihg.com)
  - Mimic booking process
- JSON parser: http://json.parser.online.fr/

JSON API results

- API calls recorded by Burp show results
- JSON data
- Convert results in CSV



Requirements

- Goal
  - Command line tool
  - Make tool obtain data from hotel site(s)
  - Store data in CSV format or database
- Result set
  - Property, date, room, rate, USD price, room classification
- Parameters
  - Corporate rates, promo rates, points rates
  - # of adults, stay duration

Scraper implementation

- Always assume stuff fails
  - Overloaded sites
  - Overload/scraping prevention
  - Hotels fully booked, not open yet, …
- My implementation
  - One hotel chain per scanner (e.g. IHG, Hyatt, Hilton, ..)
  - Hotel directory scanner + per-property scanner
  - Perl WWW::Mechanize
  - Mimic Android app behavior where possible
- Parallelize everything
  - Use HTTP proxies. Assume that stuff fails!

Fail: Fixed API keys in Android apps

- Need to find origin of ‘strange’ strings in network traffic
- Bytecode from Android app (extracted using apktool)

```
const-string v1, "x-client-id"
const-string v2, "kTZ6WF"
.line 57
invoke-interface {p1, v1, v2}, Lretrofit/RequestInterceptor$RequestFacade;-
>addHeader(Ljava/lang/String;Ljava/lang/String;)V
const-string v1, "x-client-secret"
const-string v2, "j8G44bDhxIaLNruuf3wR"
.line 58
invoke-interface {p1, v1, v2}, Lretrofit/RequestInterceptor$RequestFacade;-
>addHeader(Ljava/lang/String;Ljava/lang/String;)V
```

More Fails

- No scraping protection at all
- Hidden information in apps
  - Promotions, secret sign-up bonuses
- Left-over code on site or Android app
  - How about passing ‘X-Environment: staging’ along with request?
- Security issues
  - No certificate pinning
  - Clear text authentication
  - Site returns PIN+credit card numbers

Fun with scraping (Turning it to 11)

- There's a radius parameter on the site
  - How about 2,000 miles?
- You can define how many hotels you want in the result set
  - How about 5,000?
  - JSON might be quite big

Implementation done right

- Congrats Marriott!
- Mobile app protected with ‘APIGuard’
  - SHA-224 HMAC for all requests
- Website uses Javascript to authenticate requests
  - Scrapable, but hard to scale
    - Requires JS engine and DOM
    - WWW::Mechanize::Chrome Perl module works
  - See commonMarriott.js requests in your browser

Using scraper data

Finding the needle in the haystack

Issues

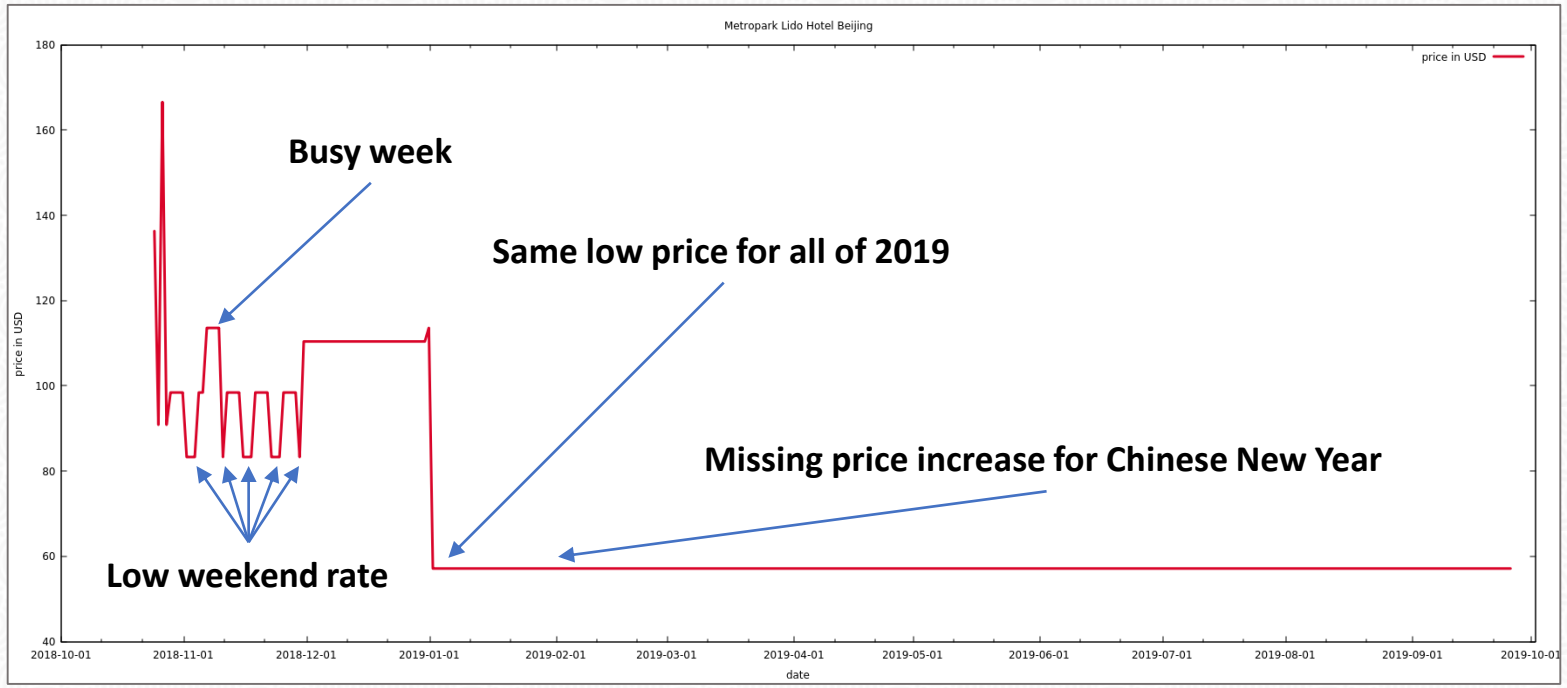
- Lots of data
- Redundant data
- What is a good deal?

Solution: automated discovery

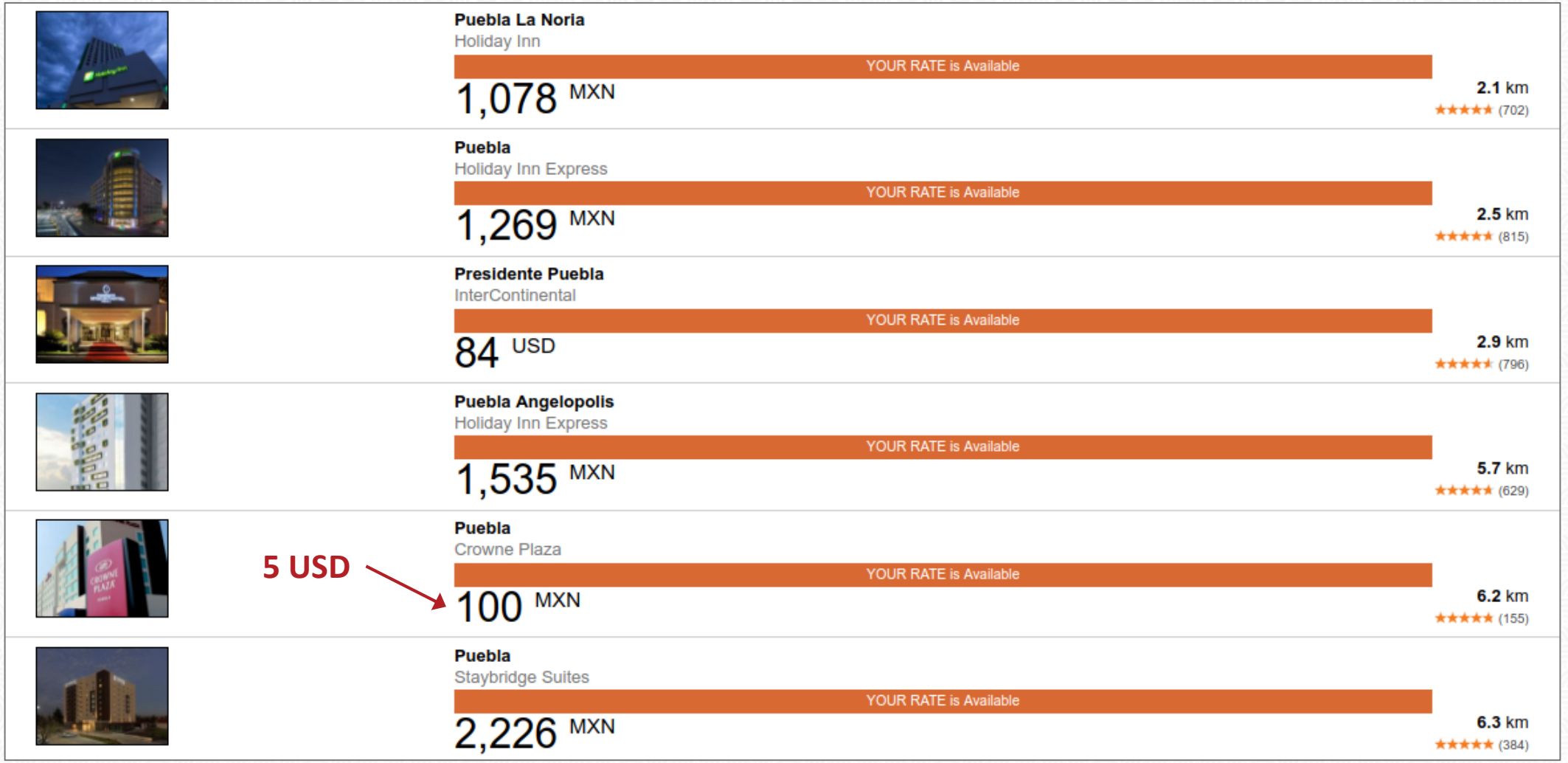
- Find rooms that are cheaper than usual
  - Compared to other nights
  - $ per loyalty point metrics
- Find bonuses
  - Points, free meals, SPA treatments, …
- Find suites that are bookable
  - On points
  - For same price as regular room

Tracking prices visually

- Track price for a certain room and rate combination
- Interesting to look at but yields few results



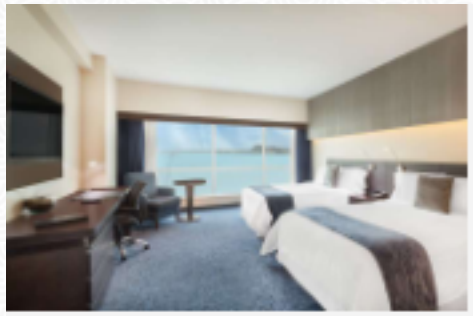
Currency mistakes: USD vs MXN



Price per point: Find great reward value

- Hotels sell rooms for loyalty points
  - Points value changes
  - Find sweet spots
- Compare cash rates against points rates
- Metric: CPP = US Dollar **c**ent **p**er **p**oint
  - Value of point in USD cent
  - Referred to as CPM (cent per mile) in air travel realm

Wyndham: Guayaquil (2019-06-29)



2 Double Beds Non-Smoking

2 Double Beds Deluxe Flat Screen Satellite TV 2 Deluxe Double Beds with pillow top, 43 inches flat screen satellite TV, air conditioning, work desk with comfort chair, coffee maker, auto-off iron and ironing board, iPhone/iPod clock radio, bathrobe, hair dryer, digital safe. Room Details

Wyndham Rewards Go Free Award Additional Rate Details • Total for Stay	15,000 PTS	BOOK
Best Available Rate Additional Rate Details • Total for Stay	$146 67 USD/NIGHT	BOOK

0.98 CPP for flexible rate, 0.73 CPP for advance purchase rate

Wyndham: Guayaquil (2019-06-29)

Only 1 rooms left!!

1 King Sleeper Sofa Suite

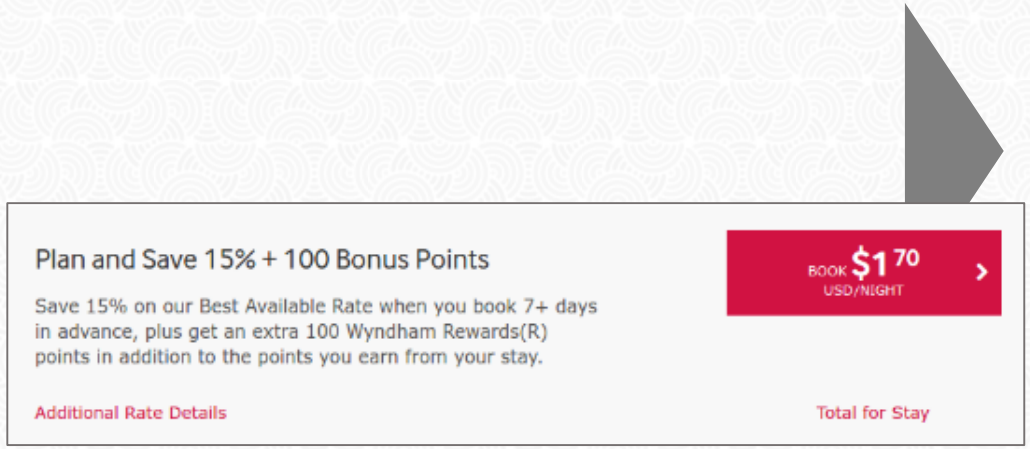
1 King Bed Presidential Suite nonsmoking Flat Screen Presidential Suite 3 ambiances featuring kitchen/dining room, living room and Deluxe 1 King Bed with pillow top, digital control hot tub, bathtub, shower, 43 inches flat screen satellite TV, Non-Smoking, air conditioning, work desk with comfort chair, coffee maker, auto-off iron and ironing board, iPhone/iPod clock radio, bathrobe, hair dryer, digital safe. Room Details

Wyndham Rewards Go Free Award Additional Rate Details • Total for Stay	15,000 PTS	BOOK
Best Available Rate Additional Rate Details • Total for Stay	$1,538.46 USD/NIGHT	BOOK

10.26 CPP for flexible rate, ~8CPP for advance purchase

Wyndham: ‘Stay twice, earn a free night’

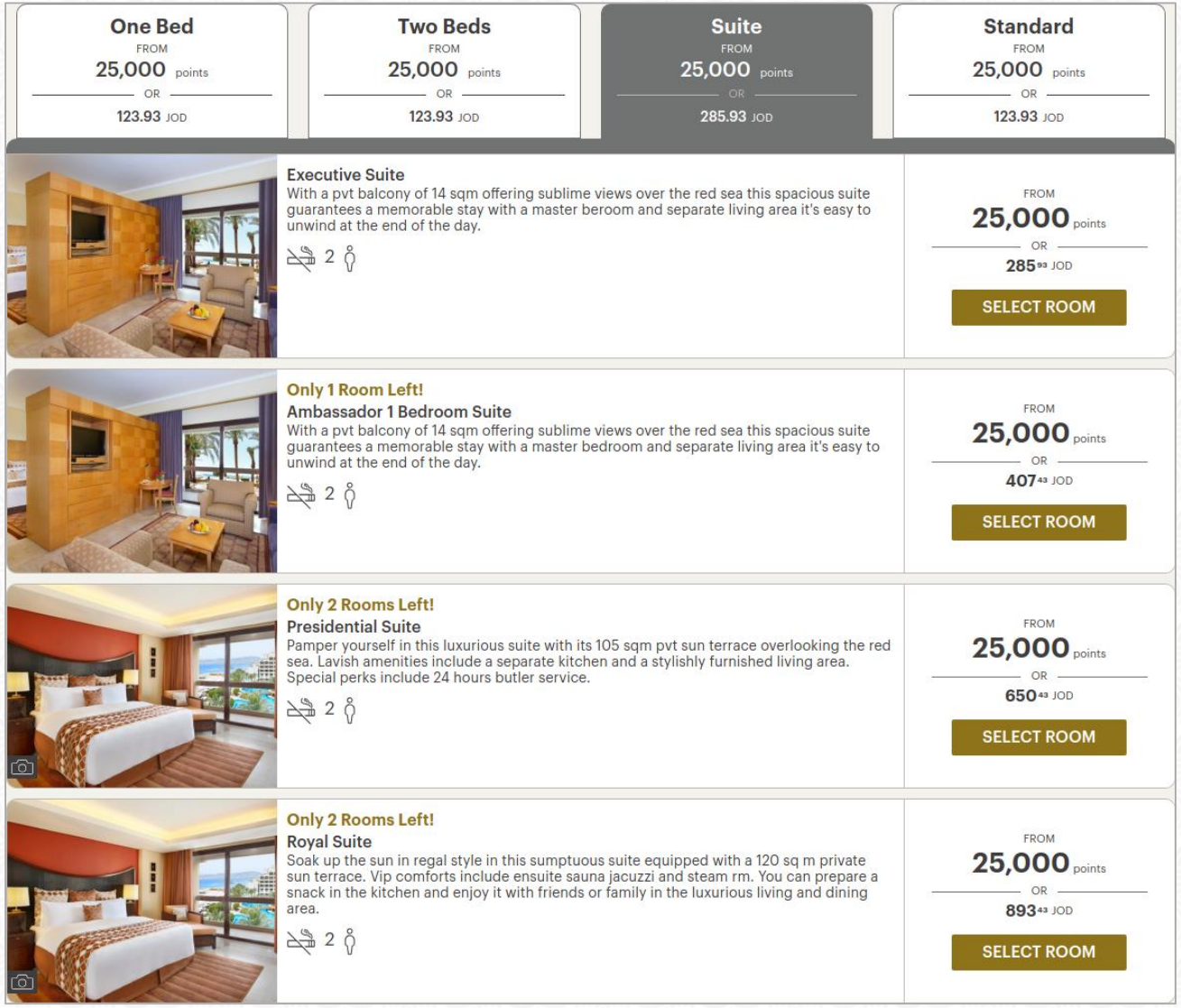
- Promotion: Stay 2 nights, get 1 free
  - Expired, likely to come back
- Value of free night
  - $200-$1500
- Cost of two paid nights:
  - E.g. $4, $30
  - Generally <$100



Great rewards

- Intercontinental Aqaba
- All rooms
- No longer bookable

- 25k points could be purchased for ~$200. Royal Suite sells for >$1200



Newly opened hotels

- New properties lack experience
  - Typically load basic rates for all dates
  - Need to add exceptions for conferences, holidays, …
- Look for errors
  - Suites redeemable for points
  - Suites for low cash rates
  - Cheap company/senior/AAA/… rates
- Requirement: detect new properties as quickly as possible

Delayed Opening compensation

- Book a hotel that is about to open
- Hope that it’s delayed
- Demand compensation (loyalty points) when delayed

```
363 362   4185|ITC Grand Bharat, a Luxury Collection Retreat, Gurgaon, New Delhi Capital Region|6
364 363   4187|W Brisbane - Opened June 1, 2018|5
365 364   4194|The St. Regis Langkawi|6
366     - 4220|The Dalmar, Fort Lauderdale, a Tribute Portfolio Hotel - Opening September 20, 2018|5
    365 + 4220|The Dalmar, Fort Lauderdale, a Tribute Portfolio Hotel - Opening October 30, 2018|5
367 366   4225|Las Alcobas, a Luxury Collection Hotel, Mexico City|6
368 367   4231|Sheraton Lake Como Hotel|5
369 368   4232|Great Northern Hotel, a Tribute Portfolio Hotel, London|5
        @@ -417,7 +416,7 @@
417 416   4857|The Whitley, a Luxury Collection Hotel, Atlanta Buckhead - Opened December 1, 2017|5
418 417   4858|Hotel de Berri, a Luxury Collection Hotel, Paris - Opened July 15, 2018|7
419 418   4903|The Westin Irving Convention Center at Las Colinas - Opening January 21, 2019|5
420     - 4947|Domes Miramare, a Luxury Collection Resort, Corfu - Opening August 15, 2018|5
    419 + 4947|Domes Miramare, a Luxury Collection Resort, Corfu - Opened August 15, 2018|5
421 420   5635|Sheraton Lakeside Terrace Villas at Mountain Vista, Avon, Vail Valley|5
422 421   5639|The Westin Kierland Villas, Scottsdale|5
423 422   5646|The Westin Lagunamar Ocean Resort Villas & Spa, Cancun|6
```

Starwood/SPG showed opening dates on website

Best Rate Guarantees

Best Rate Guarantees (BRG, BPG)

- ‘We guarantee the best price for this room and date’
  - … if booked on their site
- Offered by most hotel chains
  - Guarantees best price
  - Drives traffic to site (saving on commission payments)
- Compensation for valid claims
  - Price match + 20-25% rebate on rate
  - Free night
  - Gift card

Made from 100% recycled plastic.

IHG Best Rate Guarantee

IHG BRG: Introduction (Sept 2011)

- Started with very simple terms
- 'If you find a cheaper rate for the **same hotel + date + room + rate** combination we will give you the **first night free.**'
- Terms must be the same
  - # of adults and children
  - Cancelation conditions
  - Inclusions (breakfast, …)
- Use meta search engines to find better rates
  - Community had known working sites for specific properties
  - Shared Google docs, …

Intended BRG Process

- Book on IHG.com
- Stumble on better rate
- Fill out BRG form
- Get BRG approved
  - Low approval rate

Optimized BRG Process

- Check rate on IHG.com
  - Use flexible rate
- Check competing sites
- Find valid claim
- Book on IHG.com
- Fill out BRG form
- Get BRG approved
  - Cancel if not

How to stay multiple nights?

Issue: Only first night free

IHG BRG

- Use two guests
- Day 1) guest A
- Day 2) guest B
- Day 3) guest A

IHG BRG: Multiple nights

- ‘Two guest attack’ busted early on
- Asked for names of all guests in room
- Compared against other claims

IHG BRG: Multiple nights Redux

- Use multiple hotels
- Day 1) hotel A
- Day 2) hotel B
- Day 3) hotel A

- Busted via ‘50 miles apart’ rule (2012)

IHG BRG: Countermeasures

- “Cannot claim hotels in your home town”
- “Reimbursement after stay rather than free stay” (2013)
- “Have to book cheapest room”
- “Only one claim per week” (2013)

IHG BRG: “flexible only” loophole

- IHG terms state
  - “You need to compare against lowest rate”
    - Usually non-refundable
  - “If no non-refundable rate is available compare against cheapest third party rate”
    - This effectively allows comparing against all IHG.com rates
- Look for almost booked out hotels
  - Easy to automate when you have data
  - Book well in advance
  - Often works when town is busy (conference, event, …)

IHG BRG: 2018 status

- No more free nights
  - Will give up to 40,000 points credit instead
  - Points based on paid rate (5x normal points)
- Flexible rate trick still works
- Still gameable
  - 40,000 points are enough for a free night
  - Consider BRG points as bonus to regular stay
  - Use points at expensive hotel

Global Distribution Networks

… or how I accidentally found the holy grail

Global Distribution Networks (GDN)

- Comparable to GDS (Amadeus, Sabre, …) for airlines
  - Hotels (suppliers) supply inventory
  - GDN distributes data to channel partners
  - Enables room booking
- XML/SOAP interfaces

It began with a cheap room

- I was looking for a cheap room in New York
- Presidential suite had same price as regular room

- Room feature: ADA (Americans with Disabilities Act)
  - Wheelchair accessible, roll-in shower, audible/visible alarms, …
- These rooms have their own category
  - Limited inventory, other price, …

DELUXE ROOM KING BED

Modern design, king bed and sofa bed. Ideal for couples or ...

Room Details

RATE PLAN	PRICE PER NIGHT (USD)	
EASY CANCELLATION Changeable and refundable. Earn HHonors Points. Rate Details	$159	Select
EXEC LOUNGE ACCESS ★ Special offer CONTINENTAL BRKFST (630-11AM), HOT HORS D'OEUVRES (5-7PM) & ... Rate Details	$209	Select

View packages and promotions for this room

PRESIDENTIAL STE ONE BEDROOM HEARING ACCESS

Experience an unforgettable stay in this accessible ...

Room Details

RATE PLAN	PRICE PER NIGHT (USD)	
EASY CANCELLATION Changeable and refundable. Earn HHonors Points. Rate Details	$159	Select

View packages and promotions for this room

Missing room photo!

CLASSIC ROOM TWO BEDS

This room is ideal for families or groups. Sleeps 4....

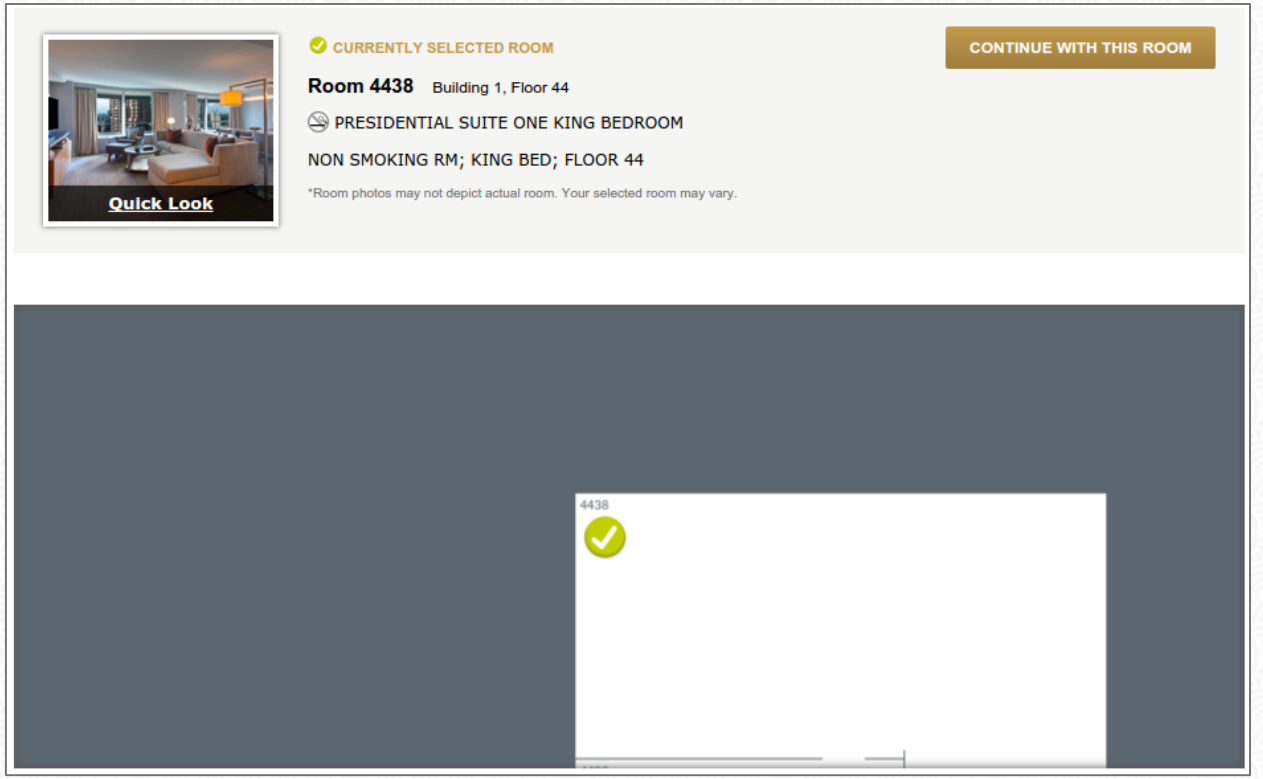
Room Details

RATE PLAN	PRICE PER NIGHT (USD)	
EASY CANCELLATION Changeable and refundable. Earn HHonors Points. Rate Details	$159	Select
EXEC LOUNGE ACCESS ★ Special offer CONTINENTAL BRKFST (630-11AM), HOT HORS D'OEUVRES (5-7PM) & ... Rate Details	$209	Select

View packages and promotions for this room

Look for the pillow on hyatt.com as deal indicator.

‘This looks a bit larger than usual’



Derbysoft support portal (2016)

- Found support portal by accident
  - Unprotected on the internet
  - Search key was rate code on my Hilton New York folio
- Escalated issue to Derbysoft
  - No answer. Never.
  - Fixed via Booking.com security team

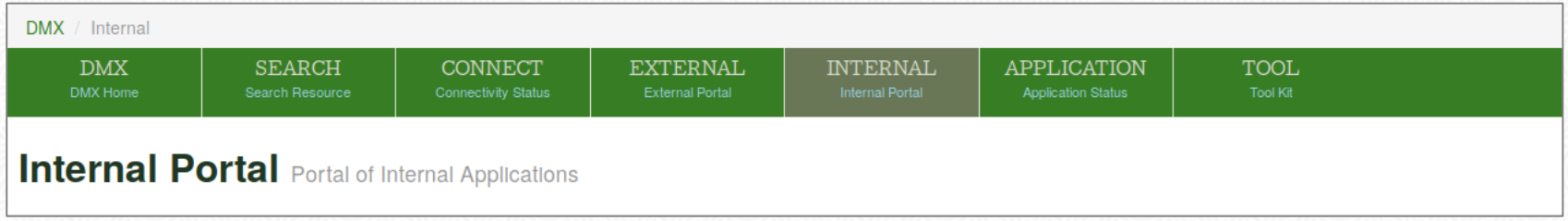
Derbysoft support portal (2018)

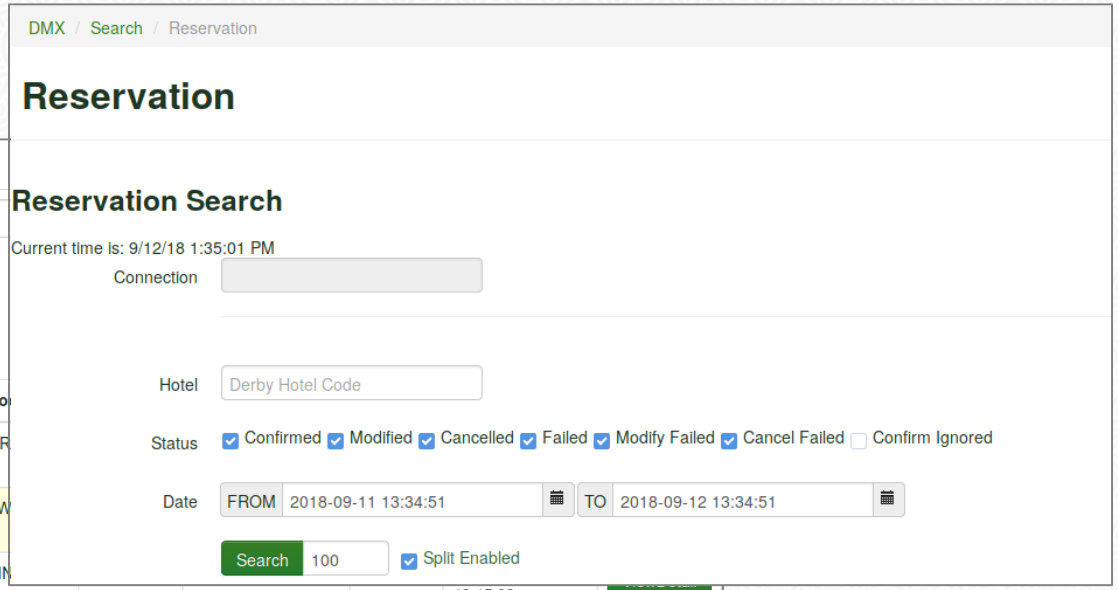
- Revisited old support website
- Saw a familiar green website flash on my screen
- Redirected to login page

‘My adblocker can also block login windows.’

Warrior Projects

Channel	Supplier-Res	Supplier-ARI	Tools
Ameropa Pusher	Accor Adapter	DStorage(GoPlatform UAT)	Config Center Manage
ATI Pusher	Accor Endpoint	DStorage(GoPlatform UAT)	Config Center Manage(QA)
BestDay	Altura Adapter	DStorage(GoPlatform CN)	Config Center Manage(IHG Portal)
Bookit	Amadeus Adapter	DStorage(GoPlatform US)	Schedule Center
Bookit Pusher	AO Endpoint	DStorage(TravelClick)	Import Changes
Doorway2	AO Endpoint	DShopStorage(GoPlatform CN)	ARI NoChange Report
Doorway2Demo	AO Adapter	DShopStorage(GoPlatform US)	Rate-Monitor/Setting
Doorway for Despegar	AO Adapter	DShopStorage(Hilton Common)	Rate-Monitor/Report
Elong Endpoint	Bestwestern Adapter(For IT)	DShopStorage(Meta Hyatt)	Dashboards
Elong Pusher	Bestwestern Adapter(For All Channel)	DStorage(UAT)	Availability Reporter
Expedia Automation	Bestwestern Adapter	Shop Storage	IHG Portal Hotel Content
ETA	Bico Adapter	DStorage(US)	HSE(redis)
Expedia Res Endpoint	Bookingsuite	DStorage(Accor)	HSE(ardb)
Expedia	Carlson Adapter	DStorage(Marriott)	Hallway
Etstur	Carlson-Schedule	DStorage(DSONE)	Doorway Hotel Content
GetARoom	Carlson-Schedule (Standard Rate For All Channel)	DStorage(GTA)	DSwitch Peak10
GTA	Carlson-Schedule	DStorage(Micros)	DSwitch US
GoPlatform		DStorage(Expedia-Hilton)	DSwitch CN





Reservation

Date: **Channel:** **Hotel:** **ErspNo:**

HotelResNo: **Result:** Search

Page: 1 / 38894, GO

First Previous 1 2 3 4 5 6 7 8 9 10 ... Next Last

Channel	Hotel	ErspNo	HotelResNo	ChannelResNo	CheckIn	CheckOut	Rooms	RatePlan	Ro					
GTA	NYCGH				2018-12-20	2018-12-25	1	14425_WPAWPM	GR					
HOTELBEDS	BKIKI				2018-09-23	2018-09-24	1	20751_IPRTF	TW					
GTA	JOHPH				2018-10-28	2018-10-29	1	14425_WPAWPM	KIN				12:15:38	
GTA	RUHHR				2018-09-21	2018-09-22	1	14425_IPRPM	KING	2/0	440.7|485.88|SAR	Confirmed	2018-09-21 12:15:27	ViewDetail
HOTELBEDS	NINPH				2018-10-09	2018-10-11	1	20753_IPRTM	KING	1/0	1872.0|2152.8|CNY	Confirmed	2018-09-21 12:14:16	ViewDetail
GTA	JOHPH				2018-10-28	2018-10-29	1	14425_WPAWPM	KING	1/0	2223.0|2245.23|ZAR	Confirmed	2018-09-21 12:13:17	ViewDetail
GTA	YVRRV				2019-05-02	2019-05-04	1	14376_WADPF	KING	2/0	618.2|729.87|CAD	Confirmed	2018-09-21 12:11:41	ViewDetail
GTA	JOHPH				2018-10-28	2018-10-29	1	14425_WPAWPM	KING	1/0	2223.0|2245.23|ZAR	Confirmed	2018-09-21 12:10:22	ViewDetail
HOTELBEDS	BOSTO				2018-10-08	2018-10-09	1	26741_IPRPM	RM1K	1/0	241.02|275.85|USD	Confirmed	2018-09-21 12:09:42	ViewDetail
GTA	NYCGH				2018-12-20	2018-12-25	1	14425_WPAWPM	GRND	3/0	1170.0|1360.08|USD	Cancelled	2018-09-21 12:08:34	ViewDetail

Derbysoft status

- Escalated issue via suppliers.
- Somewhat fixed. Somewhat.
  - More sites found
  - Still sending clear text passwords
  - Still doing client side security
- Derbysoft ~~never replied.~~ ~~replied once~~. Replied.
  - Slow process
  - Promised fixes

Social Engineering

They know they messed up and want to talk

Social Engineering

- Book obvious mistake (e.g. $5 room) and wait for contact
  - “Just give me the stay credit. I don’t have to stay.”
  - Allow them to save face and minimize damage
- Book more than you need
  - Book two weeks on cheap rate
  - If they cancel offer to meet in the middle and keep one
- Negotiate on (and accept) downgrades
  - Get soft benefits (breakfast, lounge access) instead of larger room
- Don’t be too persistent.
  - Accept points compensation

Mandatory travel

When you absolutely have to be at a specific place at a specific time

Saving money on mandatory travel

- Try best rate guarantees
- Use corporate codes
- Use points
- Use meta search engines
- Use cashback sites
- Look for promotions

Summary

- Lots of deals available
  - No 100% success guarantee
- Less exposure compared to air travel deals
  - Great chance of deals being honored
- Be prepared to spend lots of time with analytics/Excel/CSVs
- Hotel hunting is a fun sport

Hendrik Scholz
hs@123.org

Don’t forget to return key to front desk upon departure!