

Ticket to Ride: Abusing The Travel and Hospitality Industry for Profit

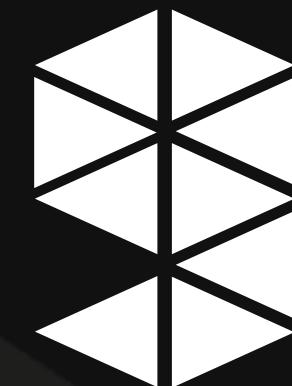
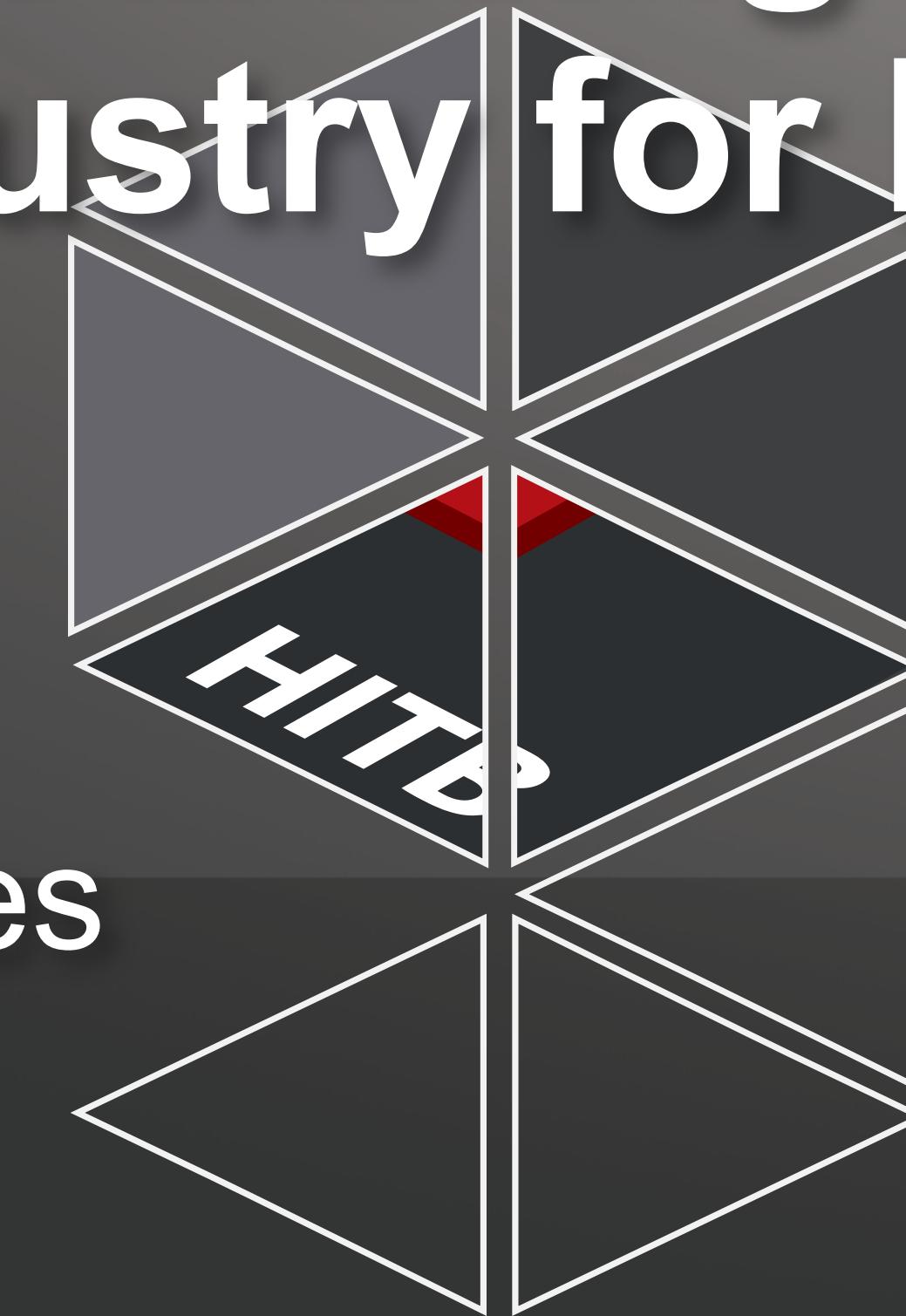
Fyodor Yarochkin

Lion Gu

Mayra Rosario Fuentes

Vladimir Kropotov

Trend Micro FTR Team



th annual **HITB** Security Conference in Europe

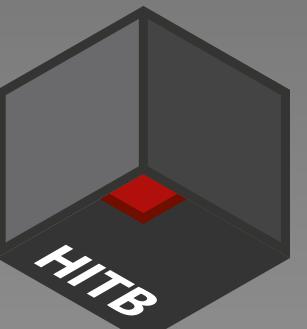
Agenda

Introduction to the travel fraud

Underground offerings

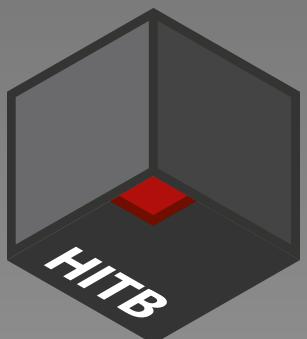
Criminal Backstage

Recommendations for the victims



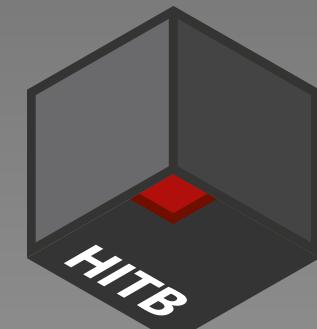
HITBSecConf2018
Amsterdam

Introduction to travel fraud



Have you traveled in last 5 years?

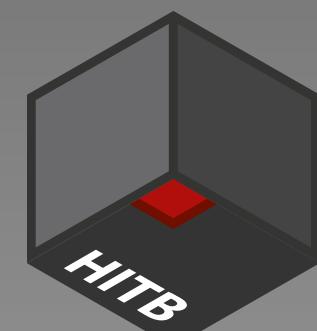
**If yes, you possibly were a
victim (or a customer?) of a
travel fraud?**



HITBSecConf2018
Amsterdam

Everyone is a victim

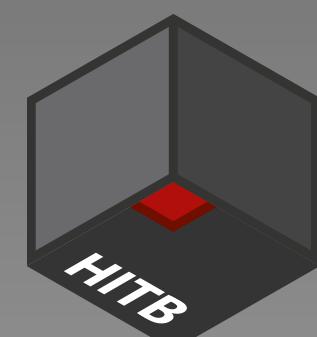
- Everyone is a potential victim
- if you travel with an airline, you are a potential victim
- if you travel by Taxi, UBER, whatever, you can be a victim...
- Customers and Victims of Travel Fraud, are distributed globally



HITBSecConf2018
Amsterdam

Who are the cost bearing Victims

- Travel agencies
- Airlines
- Car rentals
- Shared-ride services/Taxi
- Hospitality Industry
- Individuals (loyalty, uber)
- Insurance companies



The Reasons for Market Demand

- Normally it's 40-70% discount from the regular price
- You can buy a business class ticket for 25% of economy class
- Flexibility
- “Clean Money” is not needed



DUBLIKAT.ORG

NO AVATAR

Янаа

Заблокирован

Обратите внимание, если Вы хотите провести сделку с данным пользователем, на то, что он заблокирован.

Трикстер спасибо. Только что долетели. Всем рекомендую Летели бизнесом по цене 25% эконома.
Мы ваши клиенты теперь на постоянно.

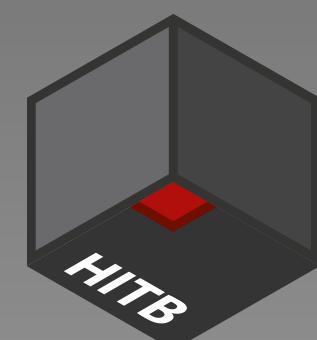
Янаа, 28 июн 2015

#12

Chelovek8000 и trickster нравится это.

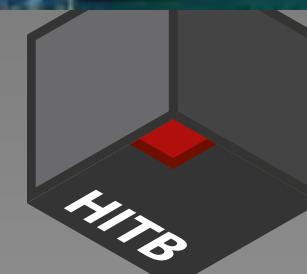
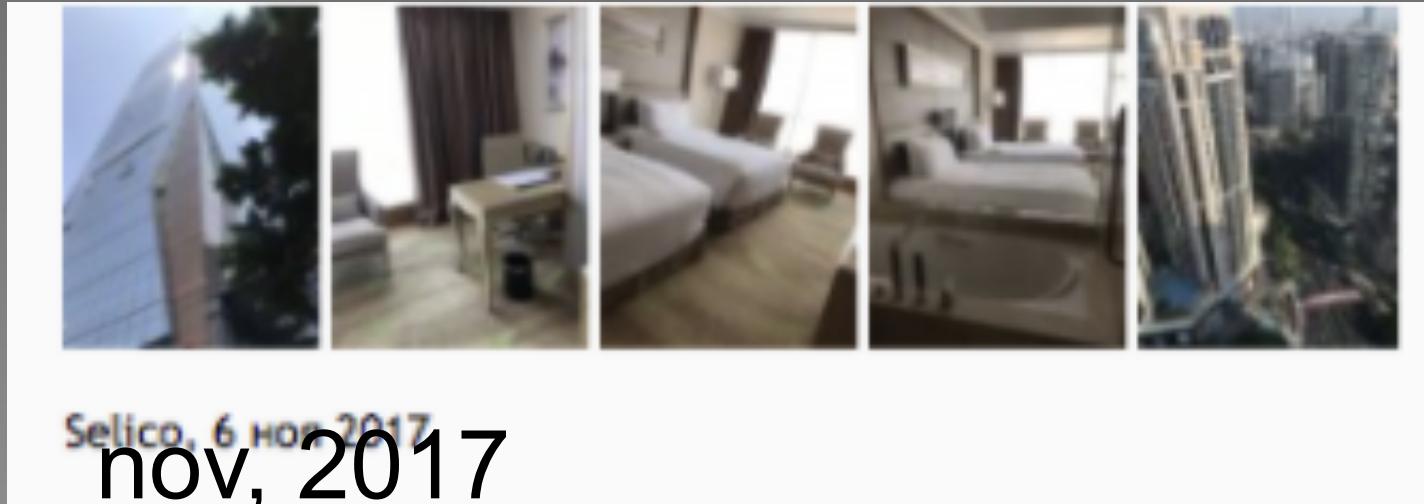


The view from the Underground: What the underground market offers



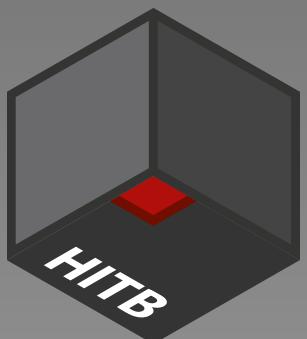
HITBSecConf2018
Amsterdam

Happy Traveler Needs



HITB SecConf2018
Amsterdam

Basic services



HITBSecConf2018
Amsterdam

Flights

ОТЕЛИ И АВИАПЕРЕЛЕТЫ
бюфFix

ОТЕЛИ И ДЕПОЗИТЫ
Депозиты и экскурсии за 50%
Минимальная стоимость отеля \$600 в кассе

ПЕРЕЛЕТЫ ПО ВСЕМУ МИРУ
40% для заказов от \$1000 в кассе
Минимальная стоимость билета \$300 в кассе

ОСТОРОЖНОСТЬ И БЕЗОПАСНОСТЬ
КРУГЛОСУТОЧНАЯ ПОДДЕРЖКА И ПОМОЩЬ
ОТЗЫВЧИВОСТЬ И СКИДКИ

35% 40 - 50%

651-697-813 service@jabber.pw hotel-service@jabber.at

СНИЖЕНИЕ БИЛЕТОВ ОТ DUMPINGTOUR

КУДА:

СОЧИ	ТАИЛАНД	ВЬЕТНАМ
БОЛГАРИЯ	ГРЕЦИЯ	ОАЭ
ЧЕХИЯ	ИСПАНИЯ	ДОМИНИКАНА
ИЗРАИЛЬ	КИПР	ИНДИЯ

60% НА ТУРЫ В ИЗРАИЛЬ

TELEGRAM: +7 962 323-24-03
SKYPE: DUMPINGTOUR
JABBER: DUMPINGTOUR@JABBER.RU

Flights

paypal logins for 3.5 \$ random
apple login 2\$

booking hotels and flight tickets 100% safe 50% of ticket price
⌚⌚ method for 100\$ with bins

أدوات الموضوع ▾ انواع عرض الموضوع ▾

#1

smtp inbox to all unlimite
make smtp Inbox

Mailer 10\$

🔒 🔒 sell

Methods

♥ prv shopping methods (6electro _ army tools _4 clothes) 15\$ for 1 method
♥ cash out method(make 1k\$ clean safe 100% from 500\$from cc (cpm method) 500\$
btc mining gears shopping methods (3 methods) 100\$ for method
cash out btc method 200\$
there's too many cash out method 1 for 50\$ working 100%

💕💕 vbv fullz

usa 15\$

\$ europe 25

australia 35\$

paypal logins for 3.5 \$ random
apple login 2\$

booking hotels and flight tickets 100% safe 50% of ticket price
⌚⌚ method for 100\$ with bins

👤👤👤 charge games

cross fire

league of legend

all fb games

of price 40%



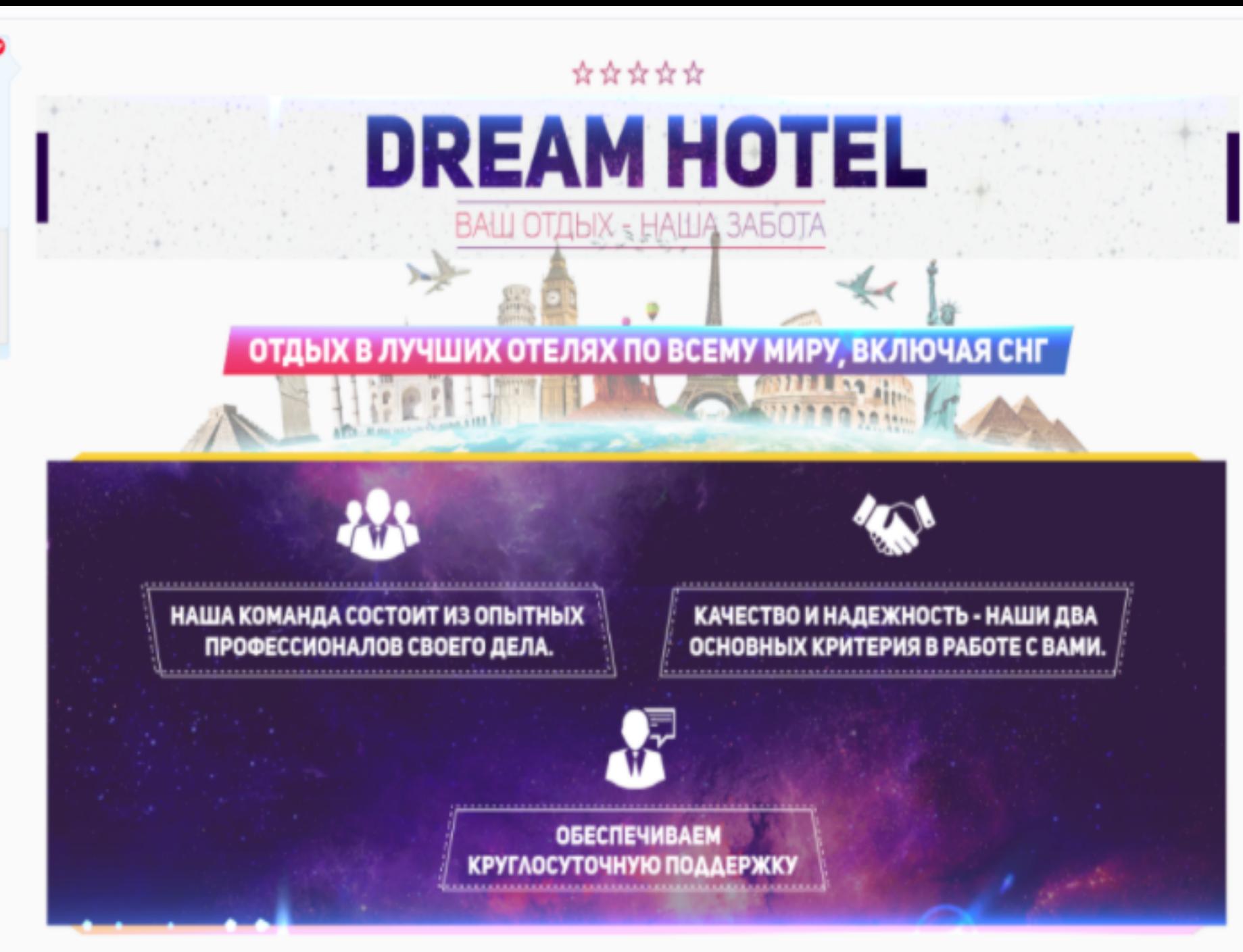
تاریخ التسجيل : Aug 2017

رقم العضوية : 45315

شارکات : 54

عدل : 0.22 يوميا

نقود السمعة :



Hotels



凯悦酒店集团金护照的10000积分，可用于积分兑换集团内酒店的免费房间，包含国内外，
柏悦、君悦、凯悦、茂悦、安达仕等酒店。

由我们代订房或我们提供账号，客人自行预订，
积分兑换房间为普通房型，不含早餐。

[兑换参考说明](#)

凯悦8000-15000

君悦/茂悦/安达仕15000-20000积分

柏悦20000-30000积分、

10.03.2015, 02:27

FIX
Продавец

Группа: Продавец

Регистрация: 16.12.2014

Сообщений: 100
Сказал(а) спасибо: 140
Поблагодарили 102 раз(а) в 40 сообщениях
Поставил(а) Дизлайк: 1
Поставили Дизлайк 0 раз(а) в 0 сообщениях

Репутация: 121

Авиабилеты, отели и депозиты от FIX. 35-50%. Высокий уровень качества и сервиса

ОТЕЛИ И АВИАПЕРЕЛЕТЫ by FIX

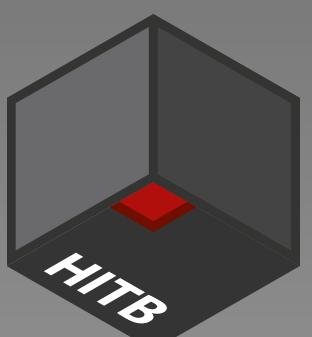
35%

ОТЕЛИ И ДЕПОЗИТЫ
Депозиты и экскурсии за 50%
Минимальная стоимость отеля \$600 в кассе

40-50%

ПЕРЕЛЕТЫ ПО ВСЕМУ МИРУ
40% для заказов от \$1000 в кассе
Минимальная стоимость билета \$300 в кассе

ОСТОРОЖНОСТЬ И БЕЗОПАСНОСТЬ
КРУГЛОСУТОЧНАЯ ПОДДЕРЖКА И ПОМОЩЬ
ОТЗЫВЧИВОСТЬ И СКИДКИ



HITB SecConf2018
Amsterdam

Hotels

Отели/Авиа/Экскурсии по всему миру

Отели по миру за 30% от стоимости

Отели Ру, СНГ, ОАЭ - 50% от стоимости.

Авиа-перелеты со скидкой от 50% от стоимости.

кроме внутренних РФ

Поддержка практически круглосуточная! Пишите по контакту
не стесняйтесь друзья!



Отели со скидкой 50-75%

Авиа со скидкой 50%

<https://t.me/yourlovelyhotel>

Напишите нам @LetsTopHotel

Мы с удовольствием поможем вам быстро и
качественно сменить обстановку

Mobility

ПРОВЕРНО Поездки на такси почти даром.
Тема в разделе "Услуги", создана пользователем Taxi200, 23 янв 2017.

TС Taxi200

Приветствуя вас уважаемые форумчане!
Предлагаю ездить на такси почти даром!
Одна поездка стоит всего 200 рублей, а вы можете проехать на сумму до 1000 рублей. Выгода очевидна.
Модератору сделают поездку бесплатно для прохождения проверки.
Пока актуальна Москва.
Для заказа пишите в телеграм: @Taxi200
Taxi200, 23 янв 2017
hoottt нравится это.

Яндекс

11.03.2016, 15:43

[edrenbaton](#)
Студент

Группа: Пользователь
Регистрация: 11.03.2016
Сообщений: 47
Сказал(а) спасибо: 2
Поблагодарили 32 раз(а) в 20 сообщениях
Поставил(а) Дизлайк: 1
Поставили Дизлайк 0 раз(а) в 0 сообщениях
Репутация: 32

Такси UBER от edrenbaton СНОВА В РАБОТЕ [X450/BL]

УРА! Мы возобновили работу по длительным поездкам!

Новые тарифы! Для постоянных пользователей, как

UBER

= - = - = Непродолжительные поездки, для

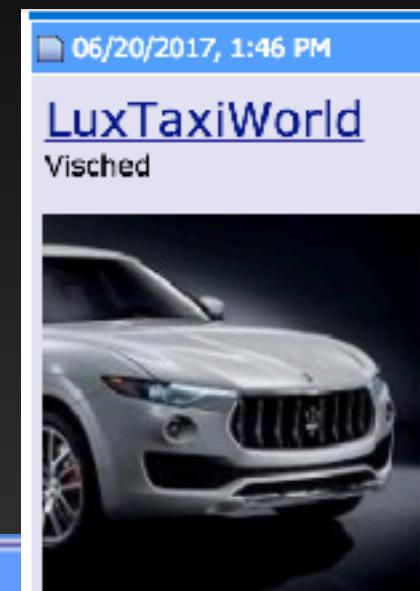
uberX - 200р. (заказ до 40 минут)

uberBLACK - 200р. (заказ до 20 минут)

= - = - = Длительные поездки от 1 до 6 часов

uberX - 450р. (заказ 2 часа, при большей длительности)

uberBLACK - 650р. (заказ 2 часа, при большей длительности)



Group: Members
Joined: 6-June-2017
Address: Mauritius
0 posts
Thanks: 6
Thanked 10 Times in 4 Posts
Put by (0) Dislike: 0
Поставили Дизлайк 0 times in 0 posts
Reputation: 0

@LuxTaxiWorld - World Taxi Service (Gett / Uber)

Welcome to **@LuxTaxiWorld** service we provide taxi services on the World (Gett / Uber).

We always go to meet our customers and try to please them with low prices!
:)



OUR RATES:

VIP (Audi A8, Mercedes S-class, BMW 7-series, Hyundai Equus, etc.):

[1 Hour] - 850 RUB.
[Airport] - 900 RUB.

Business (Audi A6, Mercedes E-Class, BMW 5-Series and others):

[1 Hour] - 500 RUB.
[2 Hours] - 650 RUB.
[Airport] - 750 RUB.

- 200 RUB = 3 USD for 40 minutes trip
- UberBLACK for 650 RUB = 10 US for 2 hours ride



What else do happy travelers need??



Travel Documents, residency permits

Stolen passport on the sale

A screenshot of a classified advertisement from a Russian-speaking platform. It features a profile picture of a man with a beard and a military-style cap. The post is titled "Филиппинский загранник био 6 тр" (Philippine passport bio 6 tr). Below the title, there is a green button labeled "Проверенный продавец" (verified seller). The post includes several small thumbnail images of passports and two attachments: "20171102_061116.jpg" (450,8 KB) and "20171102_060820.jpg" (339,4 KB). The date "mikailforero, 24 ноя 2017" is visible at the bottom.

EU passports with customer provided PII for 2500\$

Продам Паспорта, личные карты (ID), водительские удостоверения ЕС (Болгария)

Тема в разделе "Ксыны, удостоверения, паспорта, справки, бланки", создана пользователем parcal, 8 сен 2017.

A screenshot of a forum post from a Bulgarian-speaking community. The post is titled "Паспорта, личные карты (ID), водительские удостоверения ЕС (Болгария)" and includes a note: "на оригинальных бланках" (on original forms). It specifies a price of "2500 евро, доставка в любой город, в болгарии возможна закладка" (2500 euros, delivery to any city, in Bulgaria it is possible to use a envelope). A note for potential buyers says: "Для желающих оценить качество предоставим фото." (For those who want to assess the quality, we will provide photos). A red box contains a warning: "Профиль пользователя не подтвержден! Работа с ним может быть не безопасна!" (The user profile is not confirmed! Work with him may not be safe!). Below the post, the user "parcal" is listed as "Начинающий" (beginner).

РН(налоговая)
«Роспаспорт»
ВУ по твоим данным
ВУ под твой возраст и регион
рописан по домовой книге
ей кредитной историей под
человека «2 НДФЛ» с налогом
фон предприятия). -Проверка на судимости
по базе НБКИ -Проверка п
по базе ОКБ финансовый



HITB
SecConf2018
Amsterdam

residency permits and travellers blacklisting

The screenshot shows two posts from a Russian dark web forum.

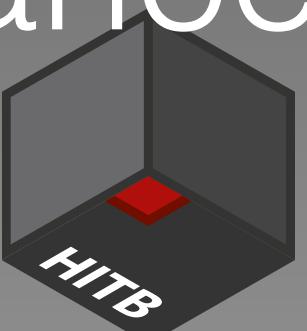
Post 1: "Продам Закрытие въезда в РФ."

Text: "Приветствую уважаемые форумчане. Предлагаю услугу "закрытие въезда" для граждан СНГ на территорию РФ кроме стран с визовым режимом. Срок запрета от 3 до 8 лет. Гарант за ваш счёт!!! Цена за услугу 50к" (Hello respected forum members. I offer the service "closure of entry" for citizens of CIS countries to the territory of Russia except for countries with a visa regime. The ban period is from 3 to 8 years. The guarantee is for your account!!! Price for the service is 50k).
User: Klon999, 6 окт 2017

Post 2: "Иммиграционная программа "Green Card" (Diversity Immigrant Visa Program) – это Ваша реальная возможность "выиграть" Green Card и переехать в Соединенные Штаты Америки.

Text: "Мы все сделаем за вас !!!
Вам не нужно выигрывать !!!
Мы вам сделаем этот выигрыш !!!"
Text: "Green Card – так называют Американский документ - Permanent Resident Card, документ подтверждающего статус законного жителя США с правом на постоянное проживание, работу, учебу, свободный въезд и выезд из США."
Text: "Возможности обладателей "Green Card"
Text: "Вы сможете легально Жить, Работать и Учиться в Соединенных Штатах Америки, с правами, приравненными к гражданам США!"
Text: "Вы сможете взять с собой в США всю свою семью!"

- Unique service - travel blacklisting from entering to Russia for 3-8 years, price 50k RUB = 850 USD
- Win US green card almost without chance to loose



Airport VIP and CIP Services

- Commercial for Important People
 - Involves Star Alliance, SkyTeam, American Airlines
- Benefits
 - Priority check-in
 - Fast lane of security check
 - Free Airport lounge
 - Free extra luggage check-in
 - Opportunity of a free class upgrade
- Cost for one-time use
 - \$10 for one international flight
- Insider threat? Or BPC?

起飞前的贵宾礼遇

本卡仅限AA航空可以使用
由于机场原因，国内出发的暂只提供升级主舱选座服务

Main Cabin Extra
商务舱座位的经济舱的座位
必须位于主舱附近。
Preferred seats
商务舱的座位，靠近机头或机尾。

价值150美金，折合人民币1000多元哦！
一个座位即收回成本，超值超划算！

注意事项

使用方法：店家代网络值机。（一旦在AA网站上输入常旅客号以后，无法在网上修改。需要打电话给AA客服才能修改。所以店家帮您输入，防止出现错误，引起不必要的麻烦）
里程累计：里程无法累计到您自己的卡号上。
登机事项：拍下付款后，卖家会将您的预定记录中添加蓝宝石卡号，请您先自己填写好预定记录里的个人护照信息、美国住址等。否则无法操作。
卖家承诺：买家付款后，卖家立刻给您输入卡号。座位可以立即解锁。不成功，不收卷！

登机牌显示Sapphire或Emerald，则视为成功

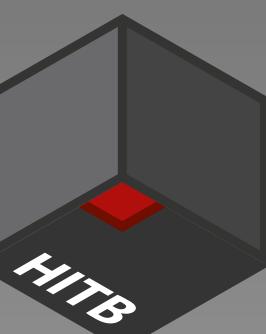
从国外起飞的美国航空还可以享受更多蓝宝石权益

贵宾室使用权
全球超过600个，星级餐饮与放松体验

优先行李
海外托运一件行李，再也不用担心超重了

优先通道
优先登机，告别排队，告别等待

升级座位
在线选座，免费升级，不用担心座位不到了



Guided Tours 25% from real price

Авиа/Отели по всему миру от Трикстера

Тема в разделе "Заказ авиа / ЖД билетов, отелей, аренда авто", создана пользователем trickster, 23 апр 2015.

Страница 1 из 3 1 2 3 Вперёд >



trickster

Начинающий

- * Отели от 15%
- * Экскурсии - 25%

Telegram : @travelx

ICQ : 681192999

Jabber : trickster@wwh.so

Заказы принимаем стандартно, за 0 - 4 дня до заселения.

Работаем ежедневно больше 4х лет с 11-00 до 01-00 по МСК. бе-

Добро пожаловать к нам. Для постоянных клиентов скидки.

РФ и СНГ - не делаем. Минимальная стоимость заказа от 5,000

- * Наш сервис один из первых вошедших на рынок бронирования с
- * Работаем на 110% более четырех лет!
- * Мы ценим каждого нашего клиента!
- * Гибкая система скидок для постоянных клиентов!

trickster, 23 апр 2015

Stefani, bubuka69 и LPB нравится это.

03/22/2018, 10:49 AM

Selective
Seller

Photo call of our satisfied customer - straight from Jamaica
May the Rasta Fa Jha bless you! !!!

Group: Seller
Joined: 9-September-2017
47 posts
Thanks: 116
Thanked 36 Times in 23 Posts
Has put (1) Disak: 1
Posted by Dizlayk 1 time in 1 message
Reputation: 0

Food services, Restaurants Logins and Gift Cards to Order food

COSTCO .COM LOGINS WITH CREDIT CARD ADDED

Vendor crazycoke (580) (4.65★) (a 417/13/24) (d 1/0/0)
Price \$0.0003388 (\$5)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow No

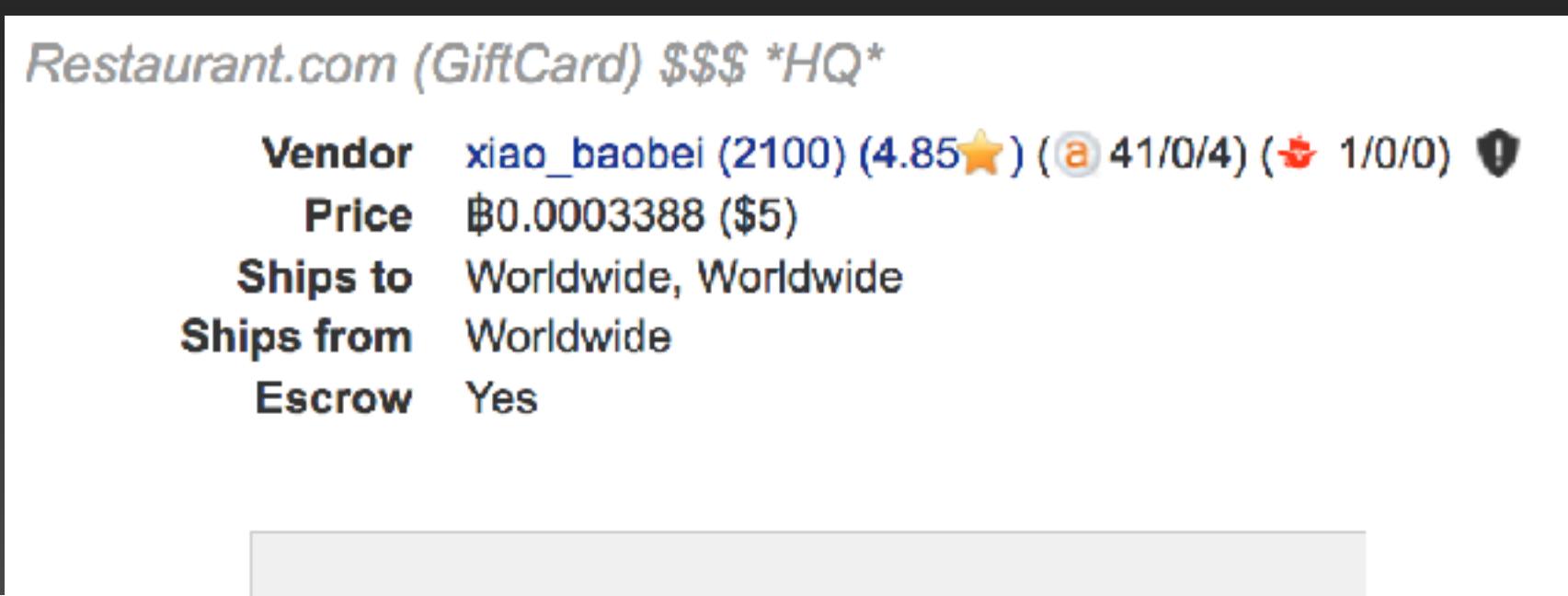


Product description

You will get:
 mail / password
 sometimes comes with additional info such as address , cc link , gift , etc ...
 Rules:
 I'm not responsible for the 'Security Measure'. Refund or Replacement is NOT provided for such accounts.
 You have only 1 1/2 hour after delivery for replacement, No refund

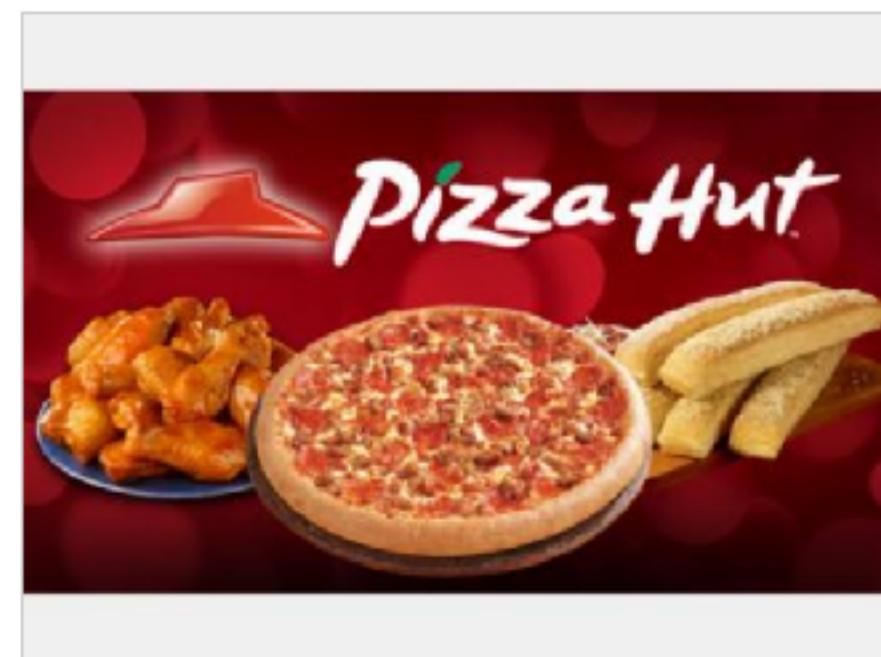
Restaurant.com (GiftCard) \$\$\$ *HQ*

Vendor xiao_baobei (2100) (4.85★) (a 41/0/4) (d 1/0/0) ⚡
Price \$0.0003388 (\$5)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes



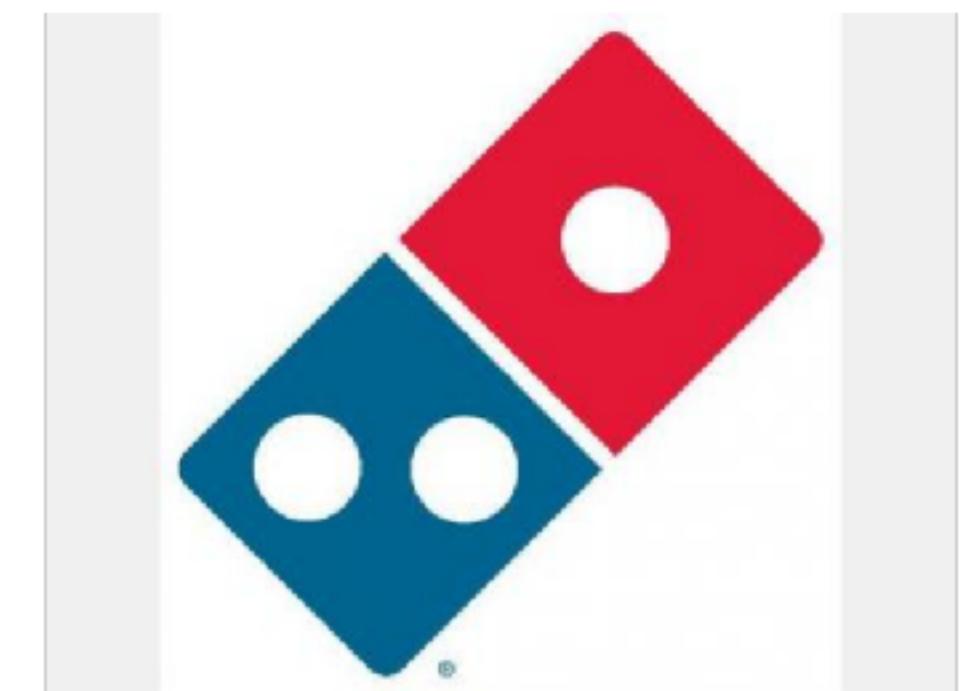
PIZZAHUT .COM LOGINS WITH CC ADDED + POINTS

Vendor crazycoke (580) (4.65★) (a 417/13/24) (d 1/0/0)
Price \$0.000237 (\$3.5)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow No



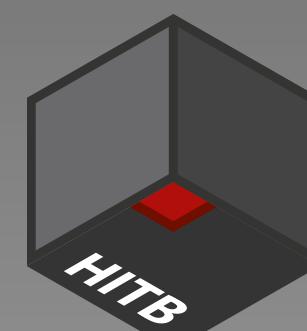
DOMINO'S ACCOUNT WITH POINTS

Vendor TheShop (12500) (4.88★) (a 866/41/20)
 (d 1399/47/47)
Price \$0.0002026 (\$2.99)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes



Product description

ACCOUNT WITH POINTS!
 Domino's Pizza is an American pizza restaurant chain and international franchise pizza delivery corporation headquartered at the Domino Farms Office Park (the campus being owned by Domino's Pizza co-founder Tom Monaghan) in Ann Arbor Charter Township, Michigan, United States, near Ann Arbor, Michigan. Founded in the United States in 1960, Domino's is in 81 countries, making it the second-largest franchised pizza chain after Pizza Hut.
 -You'll receive the infos within 24h from ordering-



HITB SecConf2018
Amsterdam

Entertainment

Возможность посещать VIP залы +1000₽ к цене за любой абонемент

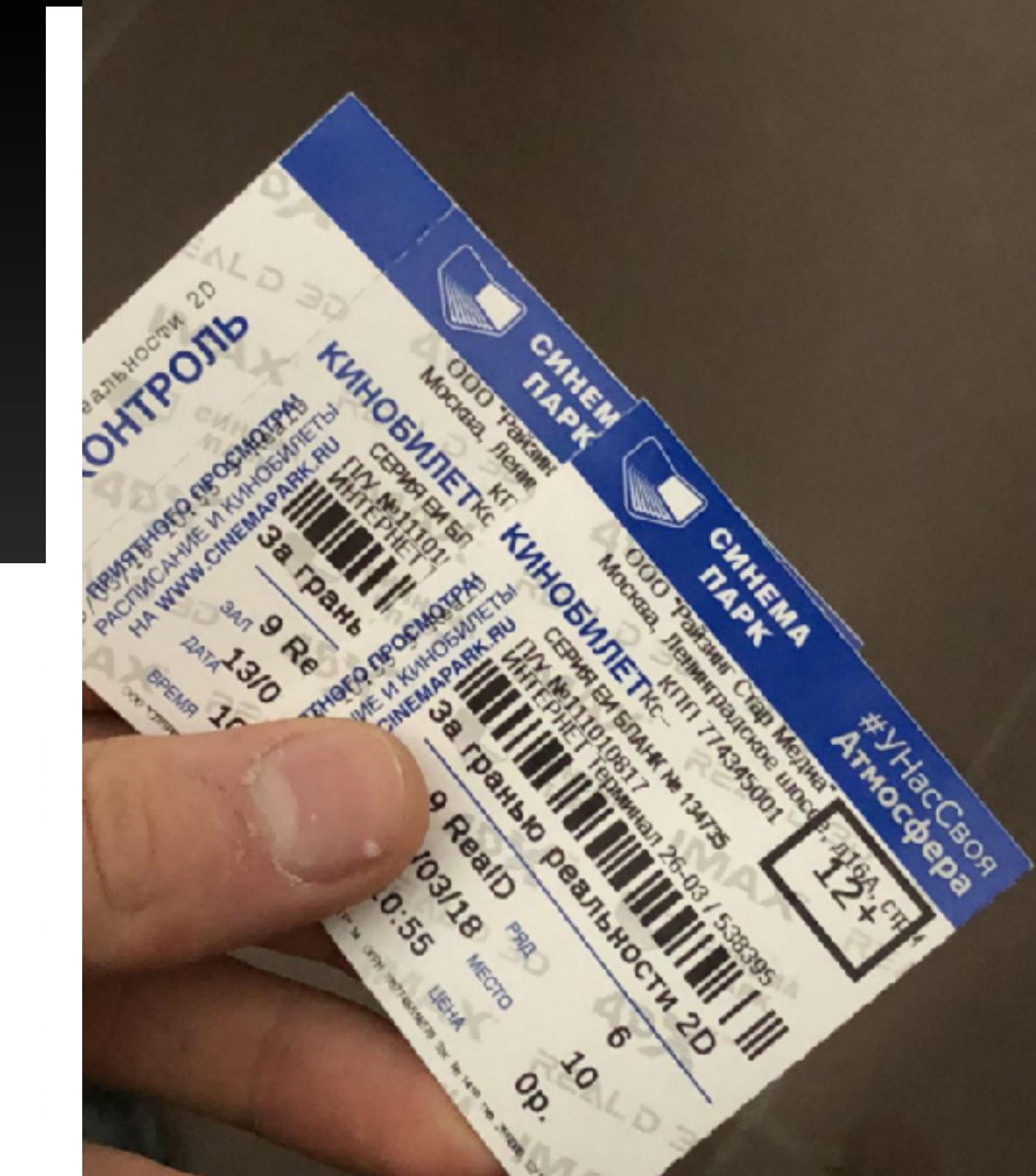
Чтобы получить билет надо сделать следующее:

1. Заходим на www.kassa.rambler.ru
2. Выбираем фильм, кинотеатр, сеанс и места
3. ПИСАТЬ [@GET20MANUAL](#) информацию о сеансе
4. Готово. Приятного просмотра

ВНИМАНИЕ!

ДАННЫЕ АБОНЕМЕНТЫ ДАЮТ ВАМ ВОЗМОЖНОСТЬ ВЫБИРАТЬ ЛЮБОЙ СЕАНС КРОМЕ VIP ЗАЛОВ

Возможность посещать VIP залы +1000₽ к цене за любой абонемент



так просто и дёшево!

ФИРМЕННЫЙ АБОНЕМЕНТ В КИНО

ОТ [@СОКАСОТКА](#)

Любые кинотеатры, любые города,

любые сеансы. Билеты в кино будут стоить

МЕНЕЕ 100₽.

За подробностями пишите [@СОКАСОТКА](#)

Карты под ГЕТ

карты под GETакси и не только

10 карт - 1500₽

15 карт - 2000₽

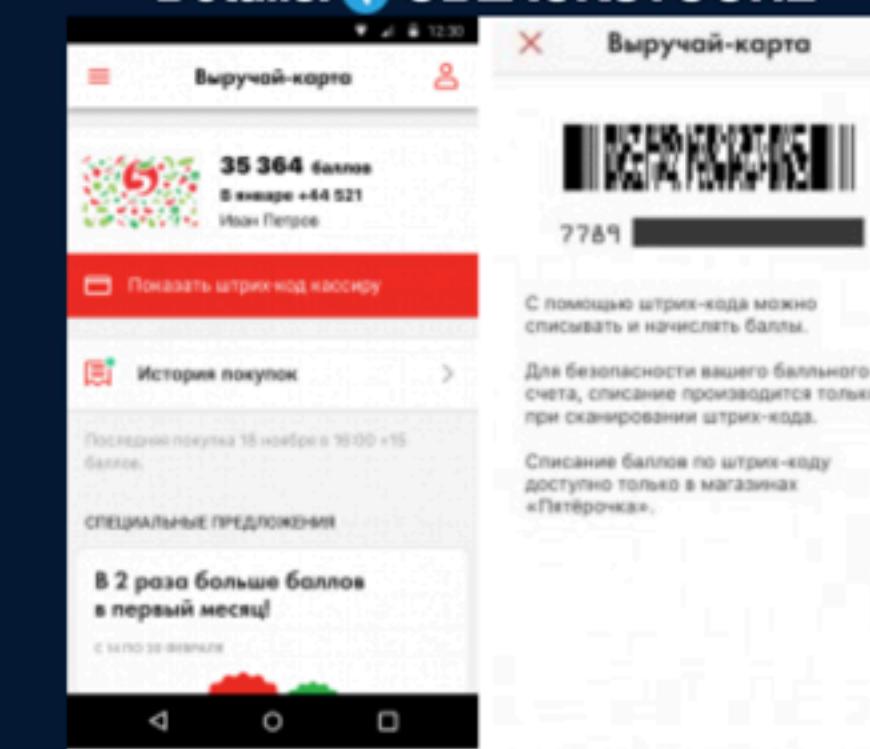
20 карт - 3000₽

[@СОКАСОТКА](#)

All in one shop example

Kinomax			
Y Kinomax [2 875 bonuses]	1	650.00 v / 650.00 \$	
Y Kinomax [2,500 power-ups]	1	580.00 v / 580.00 \$	
Y Kinomax [1 600 - 1 699 bonuses]	5	400.00 v / 400.00 \$	
Y Kinomax [700 - 799 bonuses]	4	170.00 v / 170.00 \$	
Y Kinomax [600 - 699 power-ups]	8	140.00 v / 140.00 \$	
	7th	80.00 v / 80.00 \$	
B Burger King twist the crowns themselves (manual NEW)			Yandex promo MULTIPLE on 500r throughout the RF 12 200.00 v /
B Burger King Wapper + King Free (Coupon)			Promotional code 70% discount for the first three trips... 35 25.00 v /
B Burger King Any combo to choose from (Coupon)	14	150.00 v / 150.00 \$	GETT promo MULTILOAD on 500r throughout the RF 42 150.00 v /
BurgerKing			
PizzaHut			
8+ PizzaHut Balance: 1100	1	280.00 v / 280.00 \$	
8+ R			
Accor Hotels			
✓ Accor Hotels 2000 points	10	800.00 v / 800.00 \$	
✓ Accor Hotels 4000 points	13	1500.00 v / 1500.00 \$	
✓ Accor Hotels 6000 баллов	5	2100.00 v / 2100.00 \$	
✓ Accor Hotels 8000 points	12	2800.00 v / 2800.00 \$	
✓ Accor Hotels 10000 баллов	1	3500.00 v / 3500.00 \$	
OneTwoTrip.com			
■ OneTwoTrip 10000+ TRIPOUTS	8	4000.00 v / 4000.00 \$	
■ OneTwoTrip 3000+ trypoyunov	10	800.00 v / 800.00 \$	

Warranty for accounts is 6 hours .
Did the account fail? Write to us, we will replace under warranty .
Do you doubt the authenticity of the goods? Buy by the piece :)
VALID accounts are checked every day.
The consultant never issues the goods in Telegram / ICQ.
All sales are exclusively through the store.
Attention !!!
In the presence of bonus cards Pyaterochka!
Price - 50% of the price
Details: @BLACKSTOORE



HITB SecConf2018
Amsterdam

[Travel service] Avia, Hotels, Auto, Willy

The topic in the "Garbage" section, created by the user PPmaster, 07/21/2016.

РЕАЛИЗУЙ СВОИ МЕЧТЫ в жизнь
СТАБИЛЬНЫЙ ВЫСОКИЙ ЗАРАБОТОК



РАБОТА ПО ВСЕЙ РФ
ЗП ОТ 160 000 РУБ. В МЕСЯЦ



PPmaster

DARKWEB	НОВИЧОК
DARKWEB	НОВИЧОК
DARKWEB	НОВИЧОК

Deposit:	0 р.
Guarantor of transactions:	0
Status:	Offline
Check in:	07/19/2016
Posts:	14
Reputation:	+8 / -0



The

Air tickets:

1) Carzh - practically any direction of RU / Europe / World.

Prices from 35% for the ticket, the minimum order is 15.000 rubles.

Reservation from 5 minutes before departure, up to 5-7 days.

All cargin tickets are made through a fake-seller website, in case of force majeure, they will point to where they took the ticket.

2) No carg - flights, throughout the world, including RU-RU.

Only business class.

The price is 70-80% of the cost.

The minimum order is 15000 rubles.

Although half a year before departure, because not carve - nothing can fly.

Hotels (All World):

The cost is from 35%, the minimum order is 15.000 rubles.

Deposit in your hotel, the cost is 40% of the deposit amount.

Auto:

Transfer to / from the airport, to a car of a representative class from 2000 rubles.

Car with a driver for the whole day at your disposal (from the minivan to the S class), from 3000 rubles / day.

Concerts and excursions:

We will help you book almost any excursions for you, such as: helicopter rides, dinner on a yacht, fishing, visiting museums, observation platforms and much much more.

Tickets for the most popular shows and concerts around the world!

Bonuses:

Constant clients are pleased with bonuses, gifts and upgrades of classes of service.

How to order:

To clarify the availability of tickets, directions, cost and other issues, write to the drug

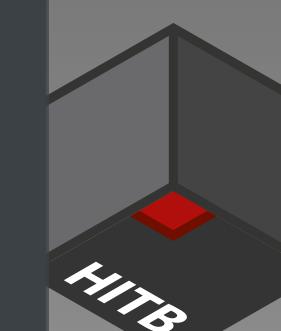
Conditions:

I work only through the guarantee-service.

Tickets / Hotels search on any aggregator (skyskanner, kayak, etc.) and copy the link of a specific offer (with dates, number of places, directions, prices, etc.).

payment:

BTC , QIWI



HITBSecConf2018
Amsterdam

Almost any Extra Service for the Traveler is Covered

- Taxis, car rentals, tour guides, event tickets, covered directly by offered services
- Loyalty points could be exchanged for almost anything for the travel

custom Disney tickets

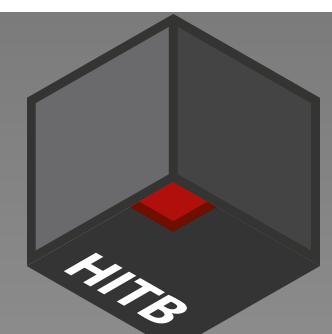
Vendor	europe (500) (4.88★) (a 132/5/7)
Price	฿0.03359 (\$200)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	No

NO

10x TICKETMASTER HACKED ACCOUNTS INSTANT DELIVERY

Vendor	crazycoke (460) (4.69★) (a 417/13/24) (d 1/0/0)
Price	฿0.001679 (\$10)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	No

ticketmaster



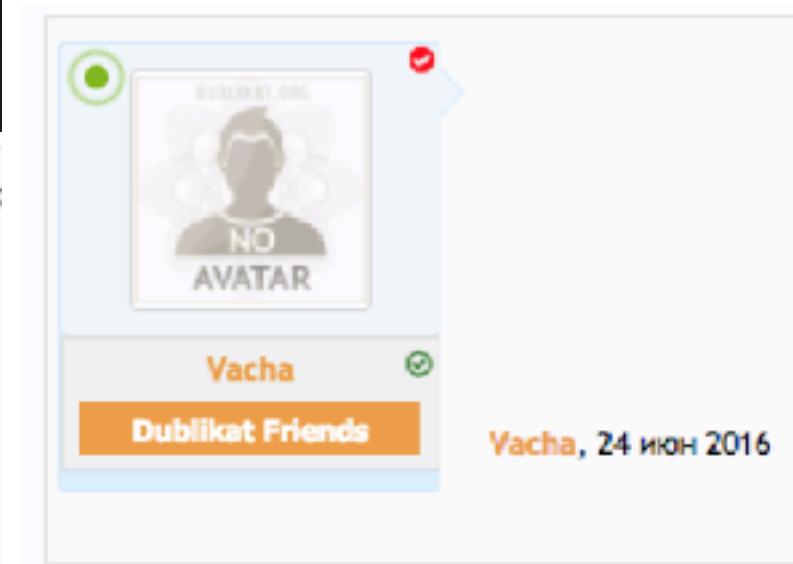
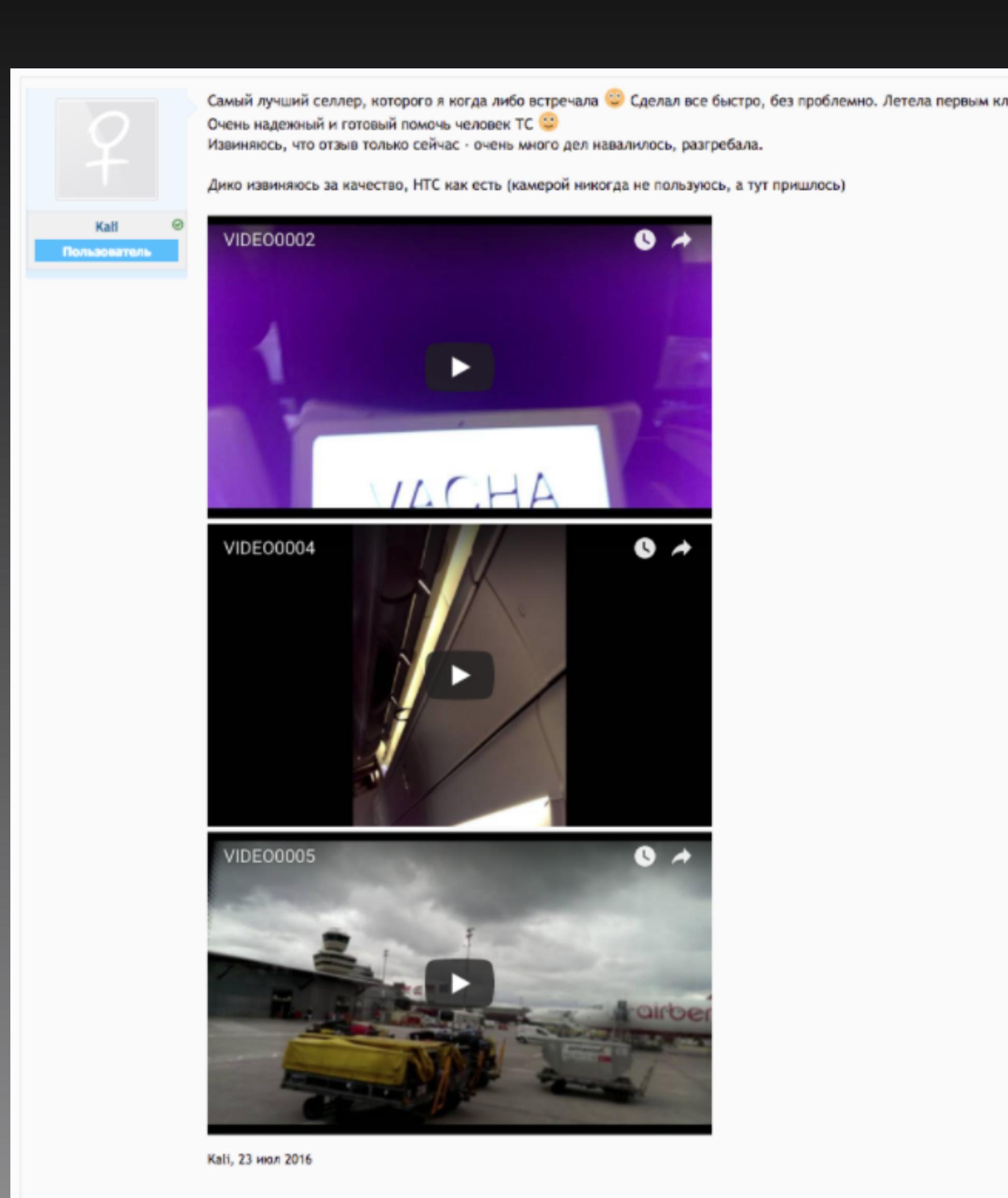
HITBSecConf2018
Amsterdam

Anonymous postal service



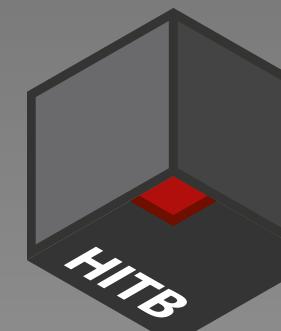
- Prices from 400 RUB = 7 USD
- Payment after delivery
- Approved on Darkmarket and Dublikat underground forums
- Accepts cards from many payment systems

Happy Travelers Feedback



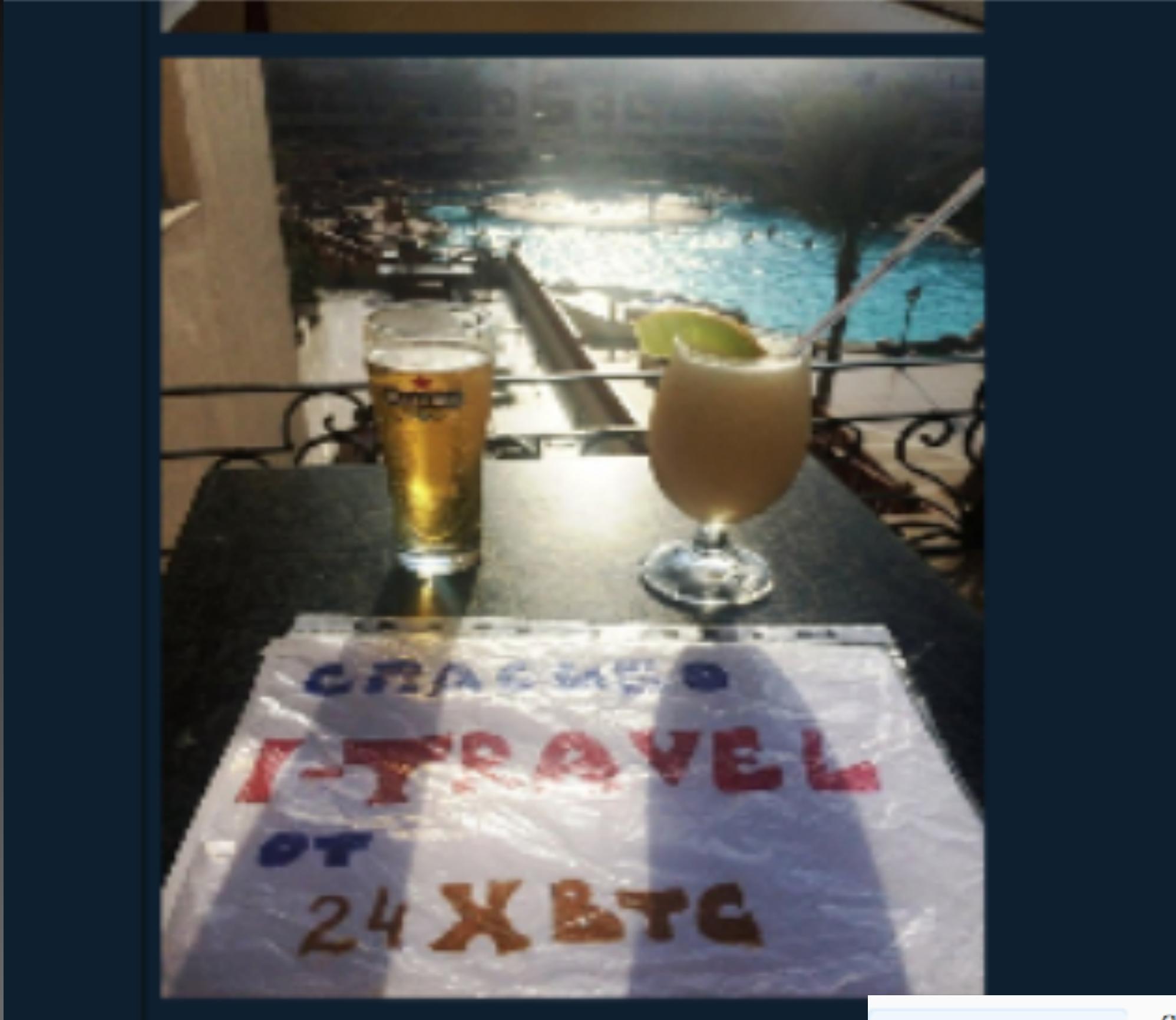
До конца июня акция! за **ВИДЕО ОТЗЫВ СКИДКА до 70%** на все направления
Авто, авиа, гостишки по всему миру включая ру и ру-ру
!!!!минималка 7000 в нашу сторону!!!
для оперативного ответа писать за 3 дня до даты отдыха, перелета
успей за 30%!

- 70% discount till the end of june for video review



HITBSecConf2018
Amsterdam

Happy Travelers Feedback

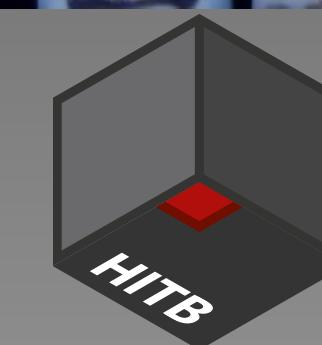


Следом были сделаны так же два отеля в Miami
Всё без вопросов, на стойке остается лишь получить ключи

Maikl_X

Интересующийся

Maikl_X, 2 апр 2017



HITBSecConf2018
Amsterdam

Forwarded message
From Оффшорный Типок



Благодарю за предоставленный
перелёт и отель в 5★, будем
путешествовать ещё🔥

Happy Travelers Feedback

30.03.2018, 21:24 # 401

ctuf1
Newbie

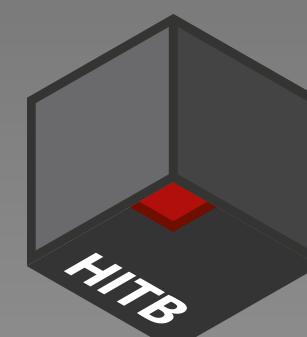
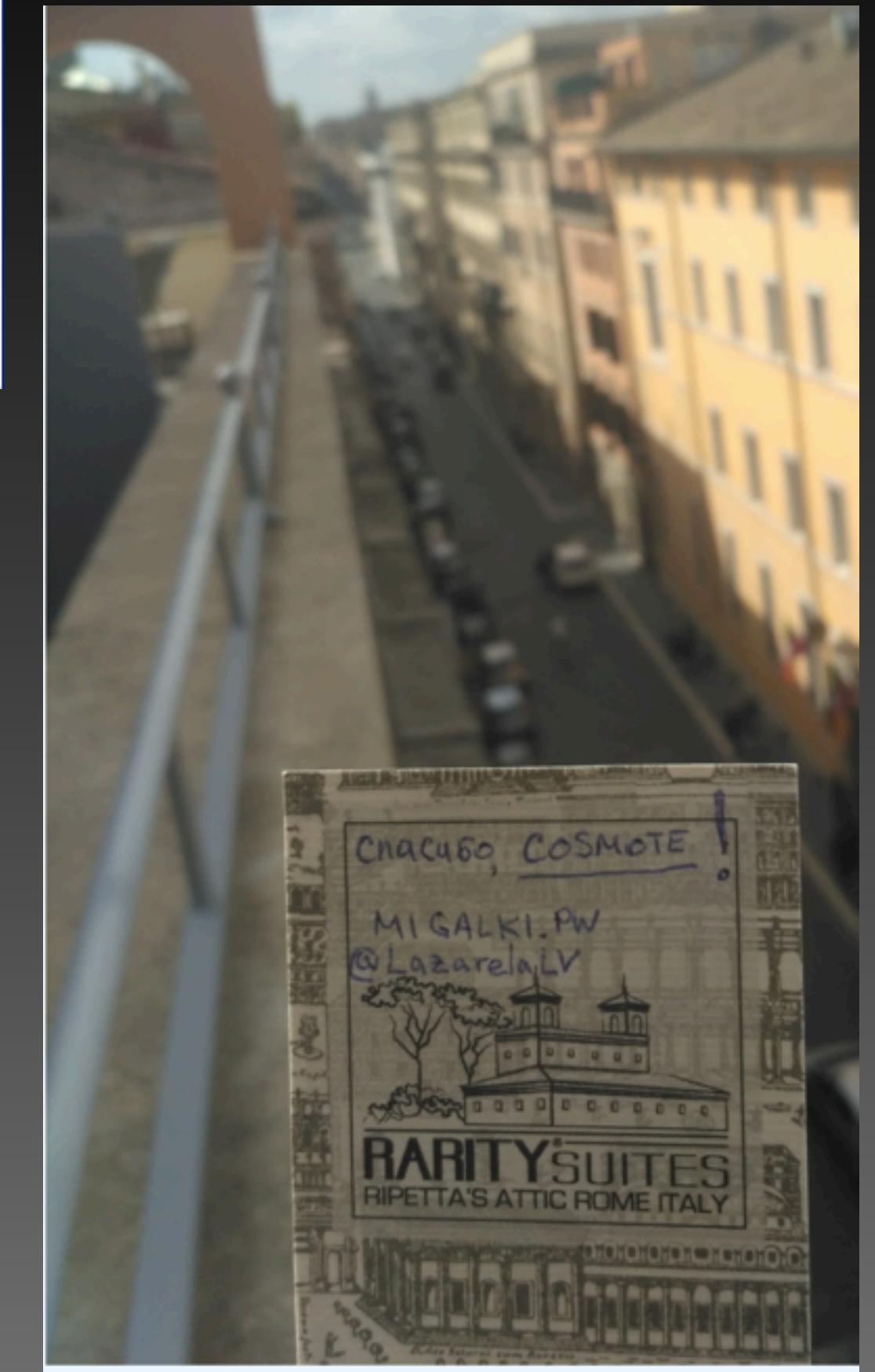
Group: Members

Hotel
Hyperion hotel Hamburg
So I did not rest! Cosmote is the best! Now I'm sitting ordering Riga!
Only through it! Thank you very much!

04/01/2018, 5:30 pm # 402

Gadsden
Visched
Group: Members
Joined: 10-October-2017

cosmote master of his craft. Made 2 hotels in Italy. All than the agent
settling without asking questions. The cost was more than
negotiated, did not pay anything. I worked with him without a
guarantor and will work again! I recommend unequivocally.



Special request Feedback

03/08/2018, 11:23 # 38

cosmote
Seller

Group: Seller
Registration Date: 12/09/1484
0 posts
Thanks for you: 144
Thanked 116 Times in 50 Posts
Put by (10) Dislike: 10
Поставили Дизлайк 0 times in 0 posts
Reputation: 1

The old and good client was very much asking to congratulate his lady in Paris, not a little work was wasted on what would be done, but the result turned out very even!
Congratulations to the female half of the Forum on the Holiday of All Beautiful!

Photo of flowers from Paris:



Important

Offer on the sellers of the subject: air tickets, hotels, etc.

iRu1 · 13 Апр 2015



iRu1

Beginning

check in : 30.08.13
Posts : 14
Sympathy : 3
Deposit : 0
Shopping : 0
Selling : 0



13 Апр 2015

#1

I propose to enter a deposit for sellers of this topic or compulsory work through the guarantor and ban for refusing this. Kidok in this direction can carry not just financial losses. You can stay in a foreign country on the street for a few days, until relatives or friends pull out. For reliable sellers, working exclusively through a guarantor or deposit, increases the credibility of them.

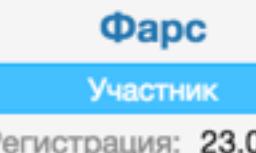
I liked this Djon108



13 Апр 2015

#

Брони, билеты, депозит имеют места слетать, это ведь карж, нужно быть готовым к этому, а чтобы не остаться на улице в чужой стране, лучше не пользоваться этими услугами, если не осознаешь риски.



Фарс

Участник
Регистрация: 23.02.15

13 Апр 2015

2

Armor, tickets, deposit have places to fly, it's a carve, you need to be prepared for this, and not to stay on the street in a foreign country, it's better not to use these services if you do not realize the risks.

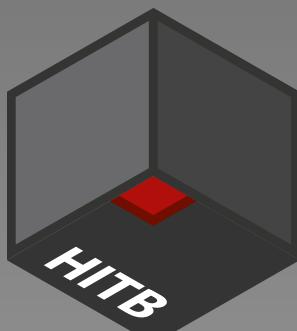
Not Happy Travelers Feedback

3. 60 thousand rubles were sent directly to the seller, 65 thousand rubles transferred to the guarantor - <https://dublikat.info/conversations...-members-vacha-47693.1252814/#message-1644447>

4. Return tickets were on the 9th of May. On May 8, the seller notified that the tickets had left. After the meeting, they agreed on the fact that the tickets will be canceled by the 11th May, can not earlier. Another meeting occurred on the 10th, the seller called to a friend and said that it is possible to solve the issue through him, I paid 28 thousand rubles, since the cost of tickets was 200,000 rubles. at the register. Arriving at the airport and starting to register, a man approached and said that there was no option to fly away, since we necessarily need a card with which the cardholder was also paid. Seller got in touch promptly, they tried to resolve the issue by calling, but without success. Desperate, I bought tickets at the cost of the ticket office on the 12th of May for 125,000 rubles. with 3 transplants and the total number of hours of flight - 27. Seller made operatively manibek.

The bottom line is that we lived from 9 to 11 in another hotel, for which we paid 12 thousand rubles, it's very cheap, but we understood that money could be useful to us. Seller could not score a hotel for these days, other services did not accept orders, since the minimum cash desk did not satisfy them. And from 19.00 on 11.05.2017 to 14.00 on 12.05.2017 we had to spend a night and spend the night at the airport, because the seller also could not solve anything with the hotel.

Please consider the legitimacy of my desire to return at least 12,000 rubles for the hotel, which we paid ourselves because of the flight tickets. For the rest of the money I have no complaints.



HITB
SecConf2018
Amsterdam

Not So Happy customer...

A buyer contacted the escrow company complaining about abuse because he didn't received the tickets on time and it's now been 15 hours overdue. The Escrow company gives 48 hours for explanations from the service provider. Service provider claims that tickets had been issued and cancelled by the issuer 3 times already and now it's the 4th attempt. If it doesn't work, the service provider will cover the Escrow costs.

The screenshot shows a messaging interface with two participants:

- ответчик ParaLIL icq 667540283**:
 - Profile picture: A red cartoon character.
 - Topics: 0
 - Messages: 0
- Грязный Санчес**:
 - Profile picture: A red cartoon character.
 - Topics: 0
 - Messages: 0

Both participants have a message box with the following text:
Скрытое содержимое, Вам необходимо войти или зарегистрироваться.
Вы не можете просматривать этот текст.

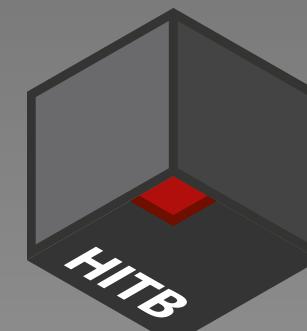
тема продавца

Скрытое содержимое, Вам необходимо войти или зарегистрироваться.
Вы не можете просматривать этот текст.

сделка была через гарант
предмет сделки 3 авиа билета Стоимостью 9000 рублей. Гарант (условились 50/50)
В обещанное время, билеты так и не были предоставлены, хотя за 10 минут до договоренного времени ТС был на связи и сказал что билеты будут готовы через 10 минут, но после 10 минут ТС перестал отвечать на сообщения и включил полный игнор. Прошло уже почти 15 часов как ТС обещал выдать билеты, но от него до сих пор тишина. Билеты были куплены за свои.
п.с. Пошел на встречу ТУ и предложил услуги гаранта поделить 50/50, но ввиду такой ситуации, что ТС включил игнор было бы справедливо если услуги гаранта, полностью перейдут на него.
п.п.с. ответчика уведомил через ЛС и через ICQ

Последнее редактирование модератором: 1 окт 2015

Грязный Санчес, 30 сен 2015

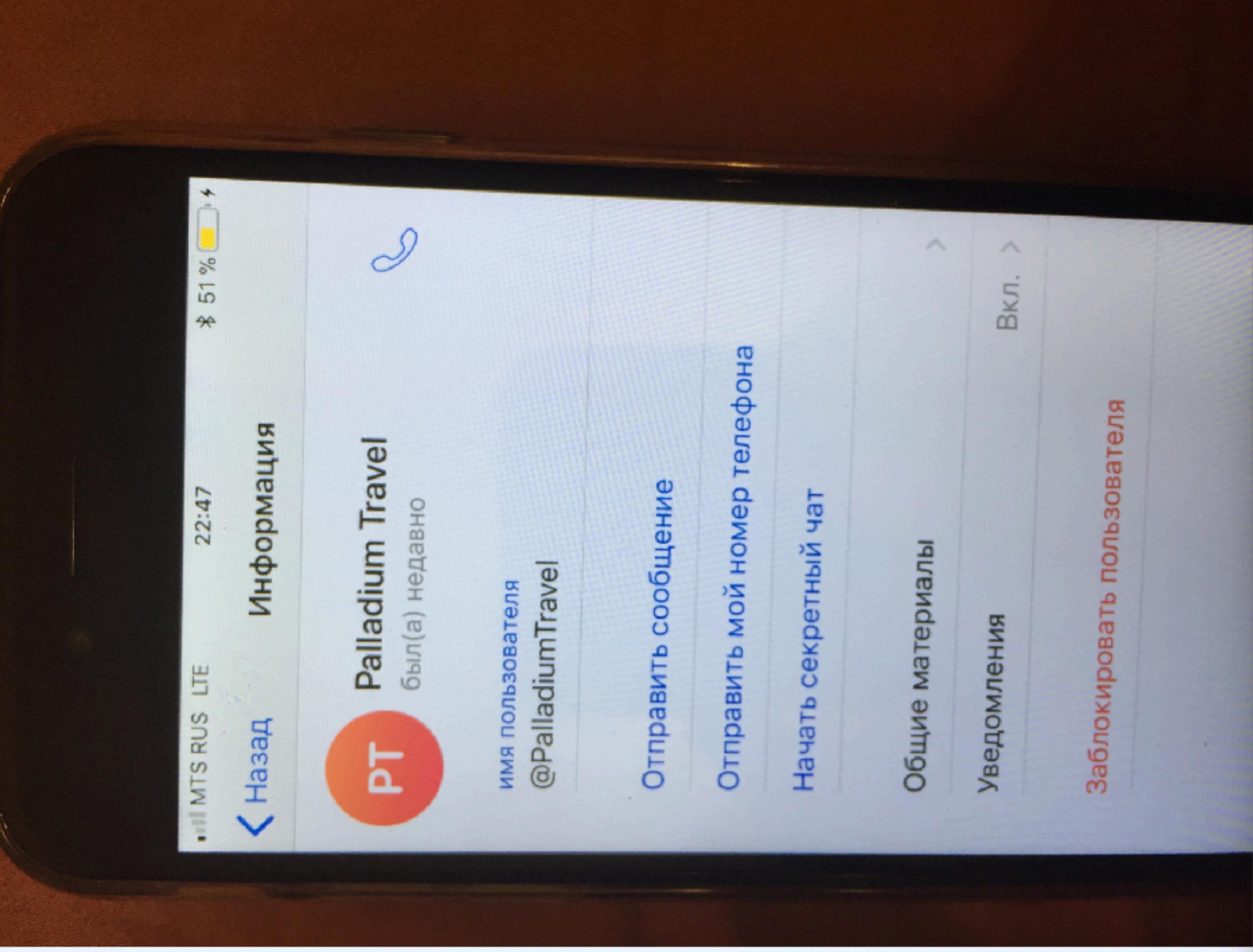


Ripers and clones...

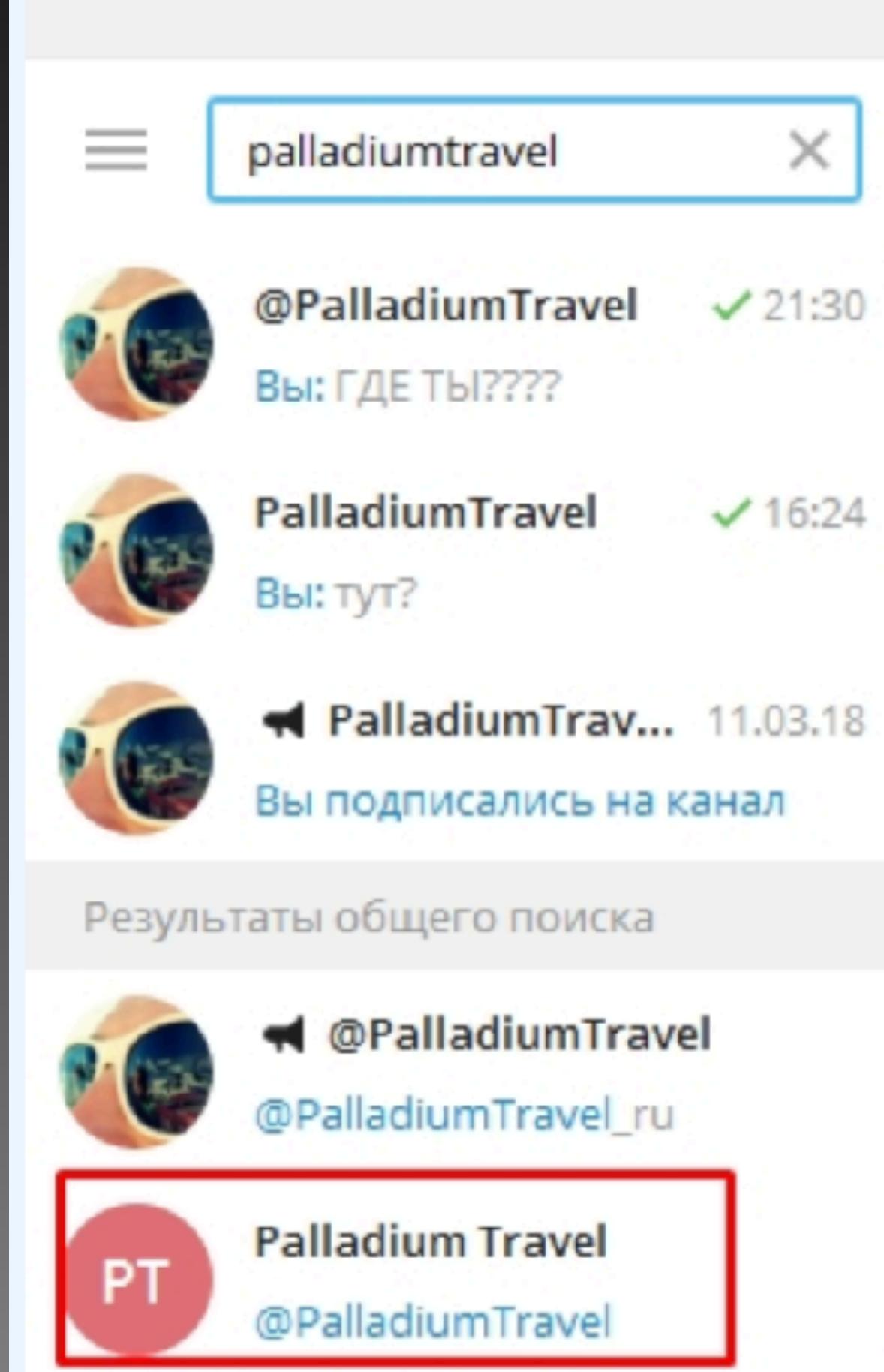
Palladium-Travel
Seller


Group: Seller
Join Date: 10/29/2015
0 posts
Thanks for you: 198
Thanked 57 Times in 30 Posts
Put by (10) Dislike: 10
Поставили Дизлайк 6 times in 6 messages
Reputation: 0

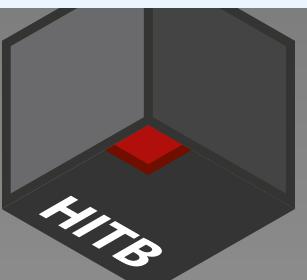
Good day!
Here are my Contacts and all the clients who have contacted me have confirmed that I have never had avatars in the cart. And the victim has an avatar. We wrote off with him in HP with nikassan and he showed the swindler and he has an avatar.



The victim what amount was at least say?
Dear moderators, I ask you to help me understand the situation, while still somebody has not suffered.



@PalladiumTravel 21:30
Вы: ГДЕ ТЫ????
PalladiumTravel 16:24
Вы: тут?
PalladiumTrav... 11.03.18
Вы подписались на канал
Результаты общего поиска
@PalladiumTravel
@PalladiumTravel_ru
Palladium Travel
@PalladiumTravel



Ripers and clones...

- Aviation 40-50% • Hotels 25% • Car rental 25% • Pripfum 60% dyuti freezers •

Contact by contact:

► ICQ 725934085

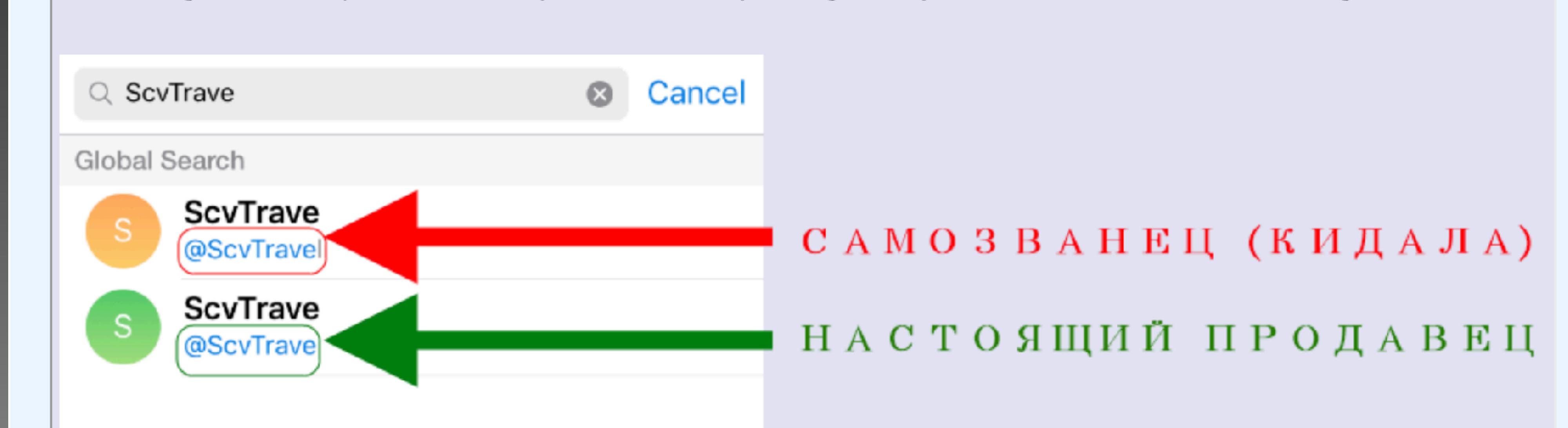
► Telegram @ScvTrave

► Be sure to confirm the information through the drug

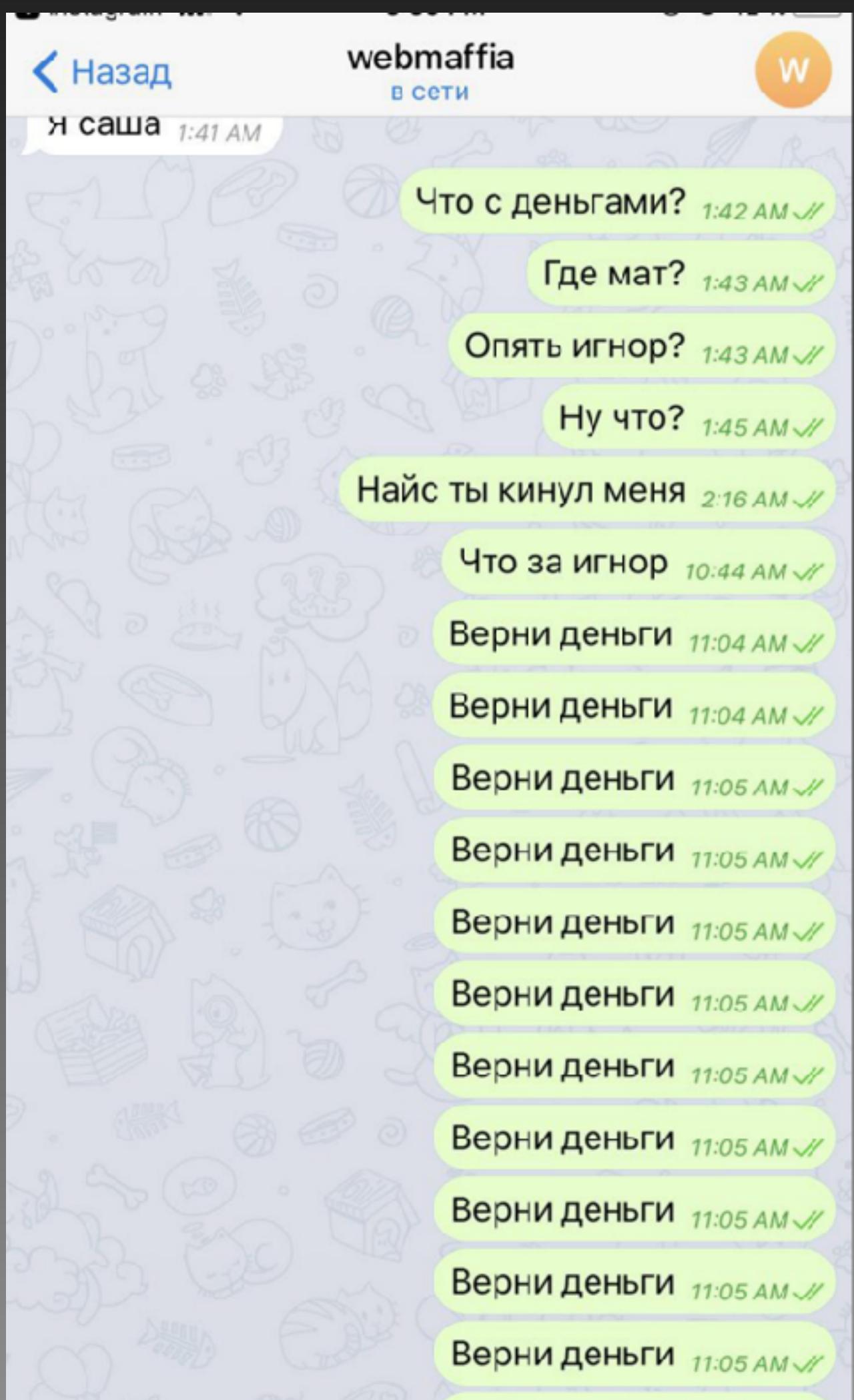
Quote:

ATTENTION!

Telegrams have impostors! Attentively add the number (the image below) and confirm the communication through the LAN.



funny: give me money back

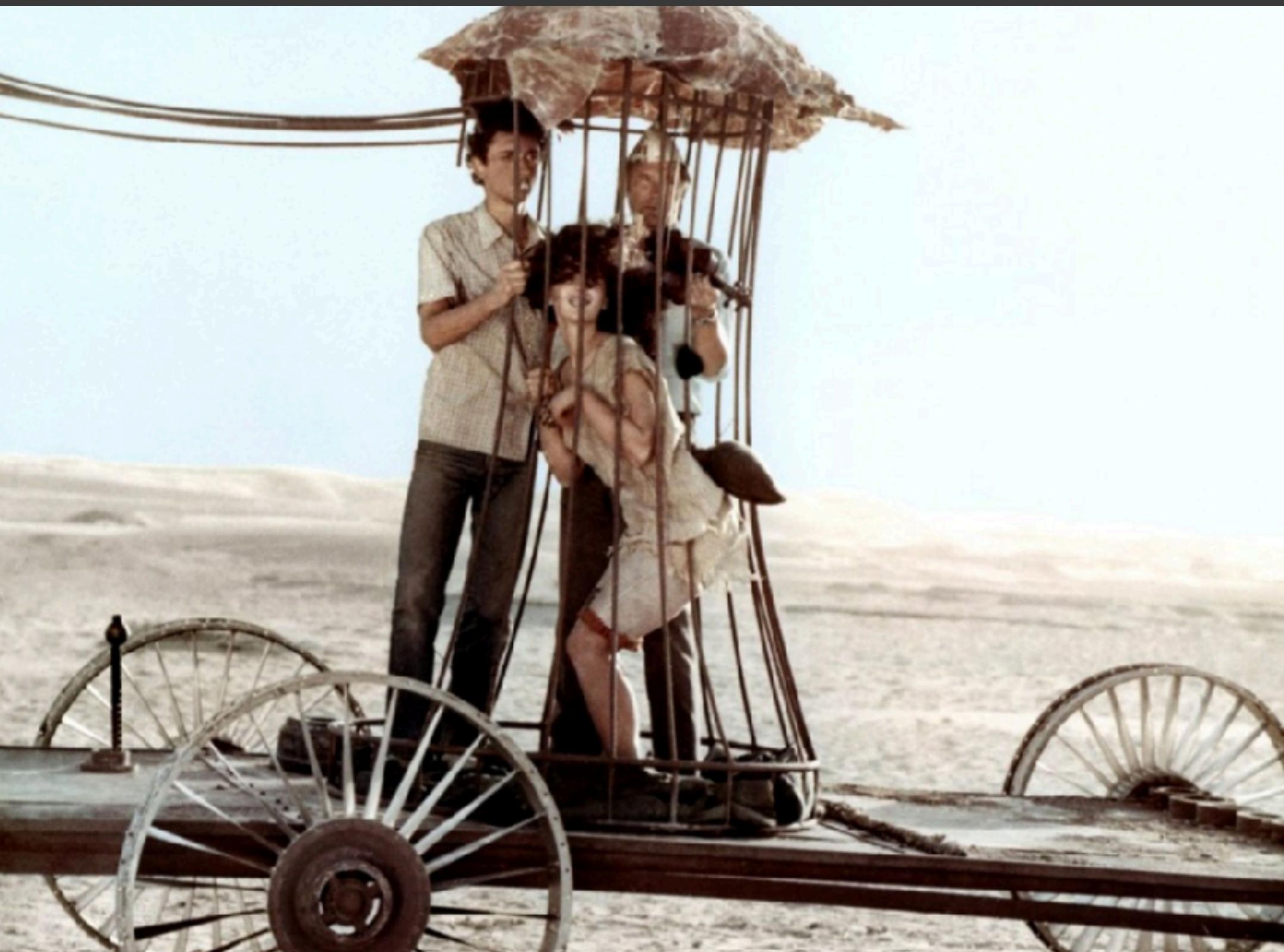


=> I'm Sasha,

<=

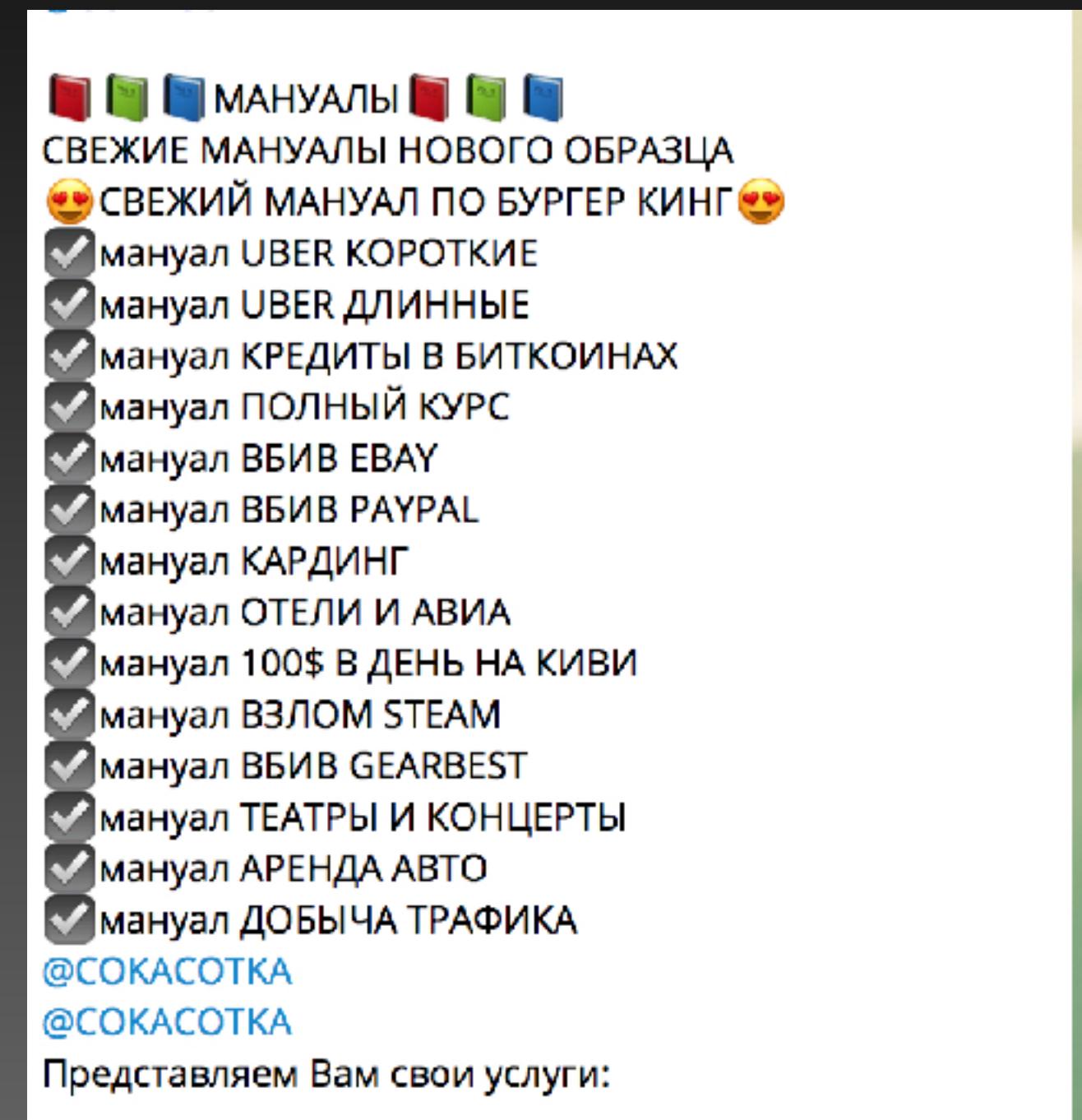
- What's with money,
- Why you ignoring me
- What's UP?
- You ripe me
- Give me money back...

The criminal backstage: Travel Fraud Schemes



Types of travel frauds schemes

- Stolen credit cards
- Abuse of loyalty programs
- Abuse of Promo programs
- Abuse of physical and logical vulnerabilities in websites and systems



Compromise of booking portals

<https://www.tourprom.ru/news/35170/>

The screenshot shows a news article from the website tourprom.ru. The header features the logo 'Турпром' and navigation links for 'НОВОСТИ', 'МАРКЕТ', 'ПУТЕВОДИТЕЛЬ', 'ОТЗЫВЫ', and 'КАТАЛОГ ТУРАГЕНТСТВ'. Below the header, a sub-navigation bar includes 'news', 'Market', 'Guide', 'Reviews', 'Catalog of travel agencies', and 'Архив'. The main headline reads: 'Attack of hackers: the travel agencies began to hack into private offices in the booking centers'. The article text discusses the difficult situation of Russian travel agencies due to the crisis, mentioning that fraudsters are hacking private offices on tour operator and booking center websites.

The difficult situation of Russian travel agencies, which, due to the crisis, the temporary absence of Turkey and still closed Egypt, lost a significant part of their clients and finances, was aggravated by a new negative trend: fraudsters are increasingly hacking the private offices of travel agencies on the sites of tour operators and booking centers, persons of these agencies. At the same time paying for these orders, booking centers are forced precisely by the affected travel agencies.

So, one of these days in the editorial office of "TURPROM" received a letter from one of the regional travel agencies, which faced such a problem. "On the site" ttbooking.ru "(Turn-Trans) the personal cabinet of the subagent has been hacked again, and tickets have been booked by scammers for 47 thousand rubles," the message says.

юложение российских турагентств, которые из-за кризиса, временного отсутствия Турции и открытого Египта потеряли значительную часть своих клиентов и финансов, усугубилось

и новой тенденцией – мошенники всё чаще взламывают личные кабинеты турфирм на сайтах

турфирм

и це

тесь за

тур

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

и

</

Computer scientists are tried for hacking bank accounts of two dozen tour agencies

In the Sverdlovsk region, a group of hackers will appear before the court, who raised about one and a half million rubles to return railway tickets purchased with the help of hacking accounts of 18 travel agencies, the press service of the Ural transport prosecutor's office said.

Residents of Ekaterinburg - Nikita Selyunin, Yaroslav Bobrov and Vladislav Skipin are charged under part 4 of Art.

159.6 of the Criminal Code of the Russian Federation (fraud in the sphere of computer information committed by an organized criminal group).

According to the investigation, the accomplices were part of a criminal group organized by a resident of St. Petersburg to steal funds from travel companies

They hacked passwords of bank accounts of travel agencies and bought railroad tickets for front men on their money. Subsequently, the attackers issued a return ticket, receiving cash at the ticket office of the railway station of the station Yekaterinburg-Passenger.

According to the fulfilled scheme, the accomplices stole 1.4 million rubles from 18 Russian tourist companies.



PHOTO TKGOROD.RU

Abuse of business process

Airfare tickets sale case

- Buy tickets for a New Year vacation on the sale for 499 RUB = 8.5 USD
- **Tickets not refundable, but..**
- It's possible to change the name for 5000 RUB = 85 USD
- Sale tickets for 15000 RUB
- $15000 - 5000 - 499 = 9501$ RUB or about 150 USD profit per ticket



Даркнет

На сайте авиакомпании Победа (<https://www.pobeda.aero>) началась распродажа билетов по 499 рублей.

Вернуть такой билет назад нельзя, но можно изменить данные пассажира за 5000 рублей.

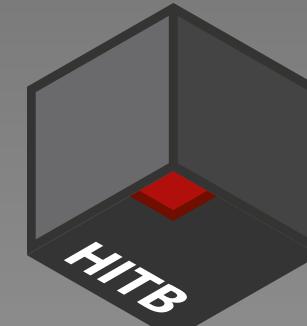
Есть рискованная, но очень простая схема заработка на билетах авиакомпании Победа.

Покупаем на распродаже билет на праздничные дни. Дожидаемся когда цена на него поднимется выше 8 тысяч рублей. Это размещаем объявлением в группах пассажиров Победы о продаже билета на 1000-1500 дешевле, чем на сайте. Договариваемся и получаем прибыль.

https://vk.com/topic-72437932_33257310?offset=180

Чтобы схема сработала, нужно правильно выбрать рейс и день. Лучше всего подходят рейсы из Москвы в Сургут, Нижневартовск, Новосибирск, Красноярск и все европейские города. Вылет 29-31 декабря. Перед Новым Годом цена рейсов может подняться до 15 000 тысяч рублей и желающие перекупить ваш билет найдутся с высокой вероятностью.

P.S.: Канал Даркнет не несет ответственности за ваши возможные финансовые потери.



HITB SecConf2018
Amsterdam

СС Kiddies Fraud

Чаты 3

РАБОТАЕМ!!!! Taxi Uber
был(а) 11 минут назад

Юрий
Продам СС деп 200\$, от

Тимур
Юрий
Продам СС деп 200\$, с

На гарант-не согласен!

Это спам

Я думаю тебе не жалко будет он
уже баблик 22:16 ✓

! 22:16 ✓

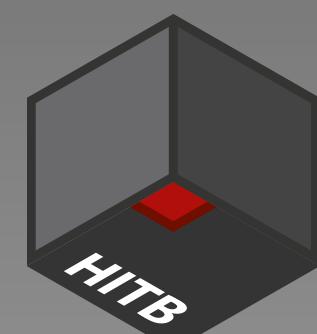
Я по отработке кардера работаю 22:16

Что он дает то и сую 22:17

Блин! 22:17 ✓

Exploitation of Vulnerabilities in Traveling systems

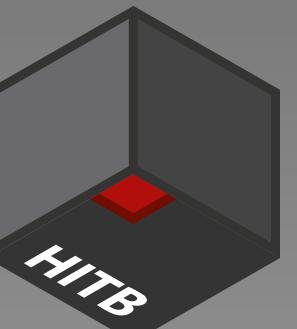
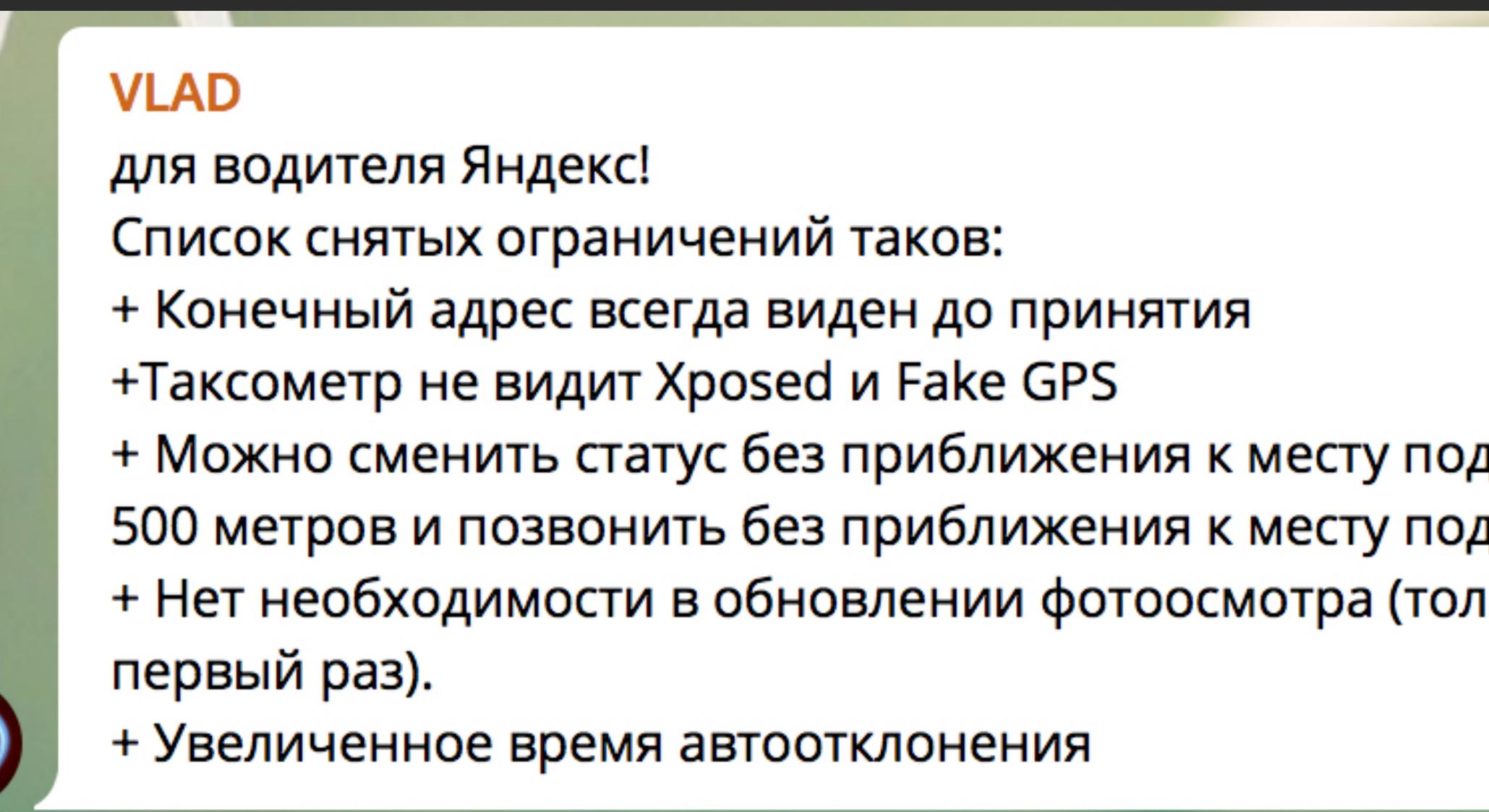
- Bug bounty challenge for Defense Travel System
<http://www.nextgov.com/cybersecurity/2018/04/pentagon-letting-hackers-loose-its-travel-management-system/147147/>
- Sabre hacked <https://www.forbes.com/sites/leemathews/2017/07/06/travel-giant-sabre-confirms-its-reservation-system-was-hacked/#670ae9594b20>
- Reservation systems hacked <https://www.rt.com/news/372033-online-booking-security-gaps/>
- *"Today's GDSs go back to the '70s and '80s, built around mainframe computers and leased lines. The systems have since been interwoven with web services, but still lack several web security best practices"*



HITB SecConf2018
Amsterdam

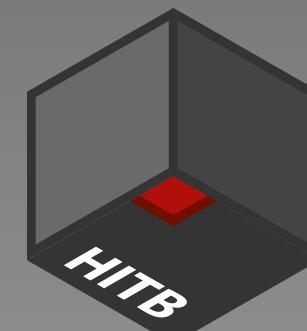
Modified "Tuned" Version of Taxi App

- Address is visible before the order was taken
- App doesn't see Xposed and Fake GPS
- It is possible to call without being close to the client
- No need of regular photos of car review



Platforms and Mileage Programs

- uber/taxi fraud and GPS spoofing (CC monetization)
- article from march 2018-<https://rntfnd.org/2018/03/07/gps-spoofing-a-growing-problem-for-uber-solid-driver/>
- June 2017- instructions how its done <http://soliddriver.com/GPS-Spoofing-A-Growing-Problem-for-Uber>



Airline Loyalty

SOUTHWEST AIRLINE 10,000 points.

Vendor philobeto13 (7400) (4.80★)
Price \$0.00503 (\$29.99)
Ships to Worldwide, Worldwide
Ships from canada
Escrow Yes



Product description

SOUTHWEST AIRLINE 10,000 points. These are the best airline rewards. Easy to use and you can get lots of different stuff plus gift cards galore.

Alaska (Virgin) Airlines Miles Account and Guide

Vendor dopedge (130) (4.94★) (2/0/0)
Price \$0.0001696 (\$1.01)
Ships to Worldwide
Ships from Earth
Escrow Yes



Product description

Product description

This purchase is for hacked Alaska Airlines miles account with appropriate package (since Alaska has bought Virgin America, you can also use Alaska miles to redeem Virgin flights).
Please indicate the package that you want to purchase by selecting different shipping options.
Nevertheless, try use the account asap since I cannot predict account owner's behavior.
The guide is not included with the account, and it has to be purchased separately; however, if you choose to purchase the guide, it will provide instructional steps of how to use the account properly through social engineering's point of view from spending the miles needed for an ordinary award ticket till you finally land it safely. It will also include a free email bomb tool invitation, so you can perform your own account takeover (ATO).
If you need an account with large miles, please send me a message for quote.
(PLEASE READ THE TERMS & CONDITIONS BEFORE YOU BUY)

Продажа аккаунтов с милями от Авиакомпаний [Отели, билеты]

Тема в разделе "Корзина", создана пользователем iCore, 31/8/16.

Метки: • авиабилеты • авиамилия • билеты • мили • продажа

Статус темы: Закрыта.



Представляем вашему вниманию магазин с продажей
аккаунтов от авиакомпаний и др. разных сервисов

Ссылка на магазин:

<http://ico.deer.io>

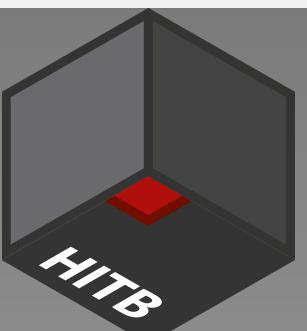
Реквизиты:

Jabber : ico@xmpp.ru

+7920***7660

Правила:

<http://ico.deer.io/info/>

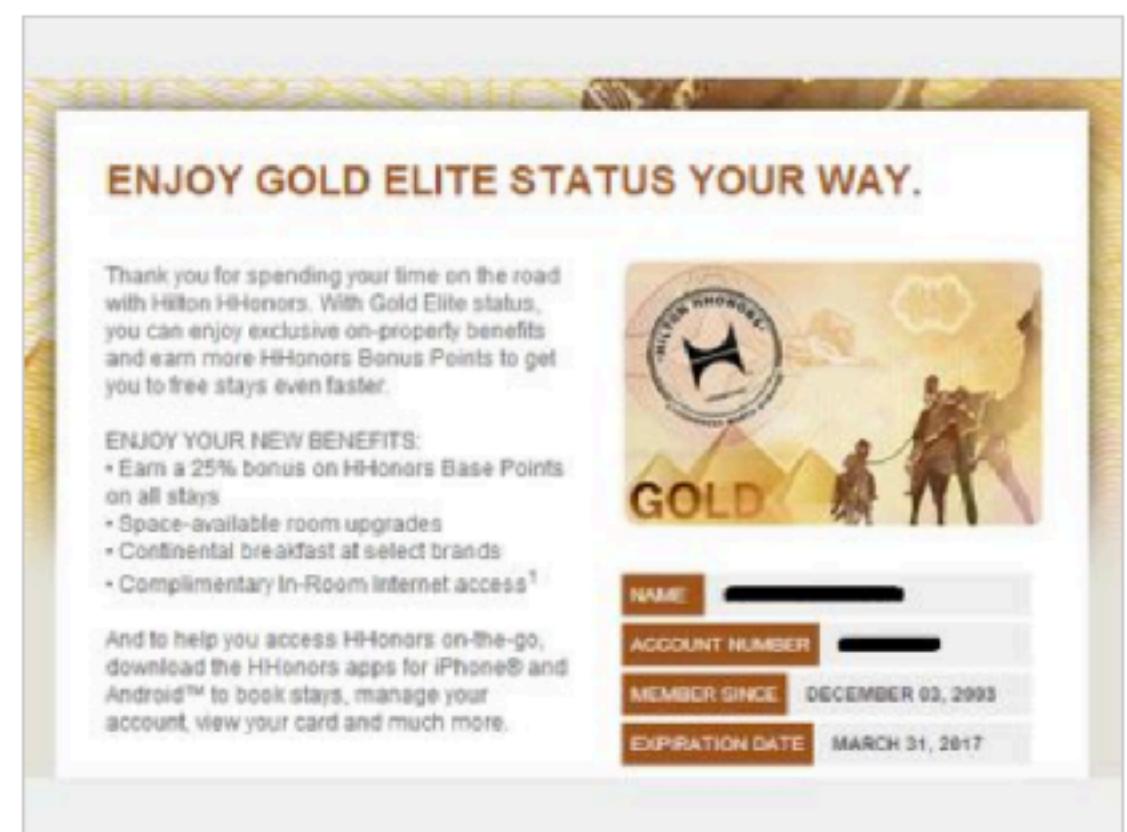


HITBSecConf2018
Amsterdam

Hotel Loyalty

Hilton Hotel Gold Status Upgrade Valid to MAR2019

Vendor coronacheeked (160) (4.93★)
Price ₩0.00503 (\$30)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes



Product description

I will create a hilton account for you and upgrade it to GOLD status! Start enjoying benefits such as FREE BREAKFAST, FREE ROOM UPGRADE, LATE CHECK-OUT and EXTRA POINTS!

Gold status will be valid to March 31, 2019. No stays required to keep your status. Not a challenge!

Detailed benefits of Hilton Honors Gold status can be found:
<http://hiltonhonors3.hilton.com/en/explore/benefits/index.html>

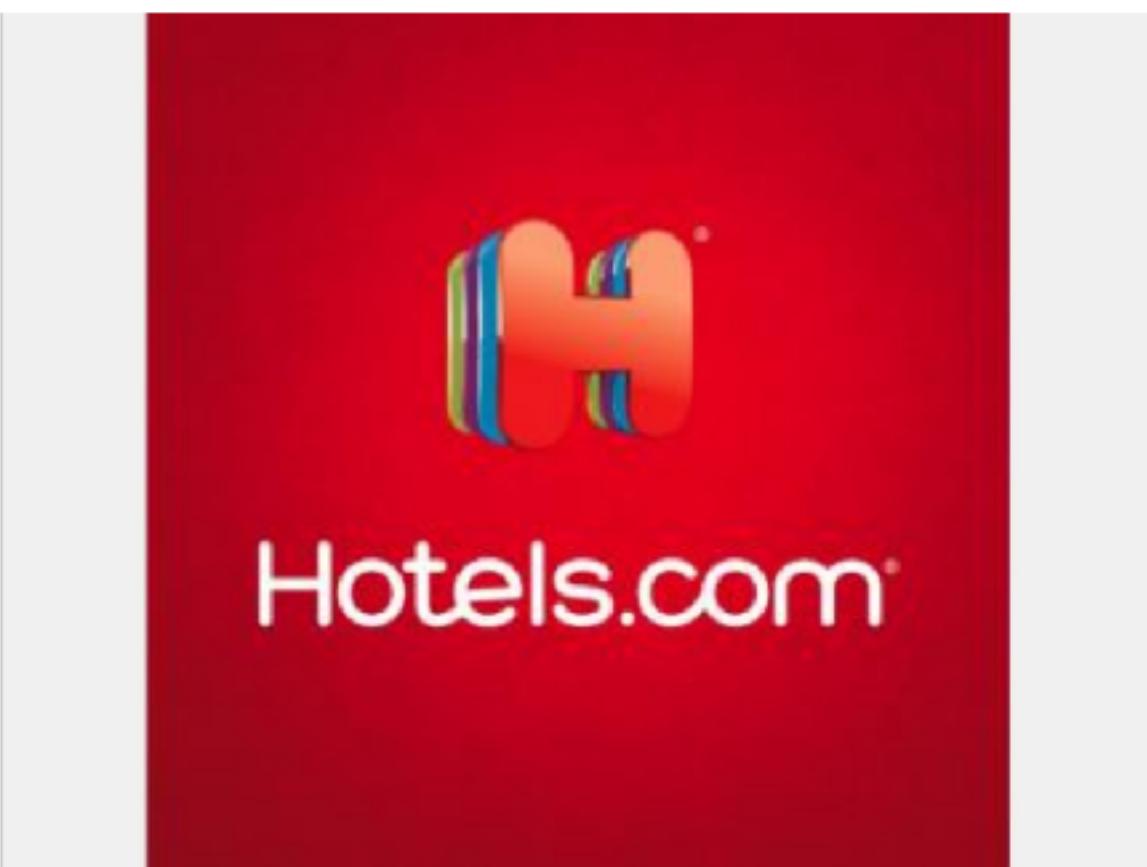
I will create a hilton account for you and upgrade it to GOLD status! Start enjoying benefits such as FREE BREAKFAST, FREE ROOM UPGRADE, LATE CHECK-OUT and EXTRA POINTS!

Gold status will be valid to March 31, 2019. No stays required to keep your status. Not a challenge!

Detailed benefits of Hilton Honors Gold status can be found:
<http://hiltonhonors3.hilton.com/en/explore/benefits/index.html>

Hotels.com Free Night Account(s)

Vendor dopedge (130) (4.94★) (a 2/0/0)
Price ₩0.001006 (\$5.99)
Ships to Worldwide
Ships from Worldwide
Escrow Yes



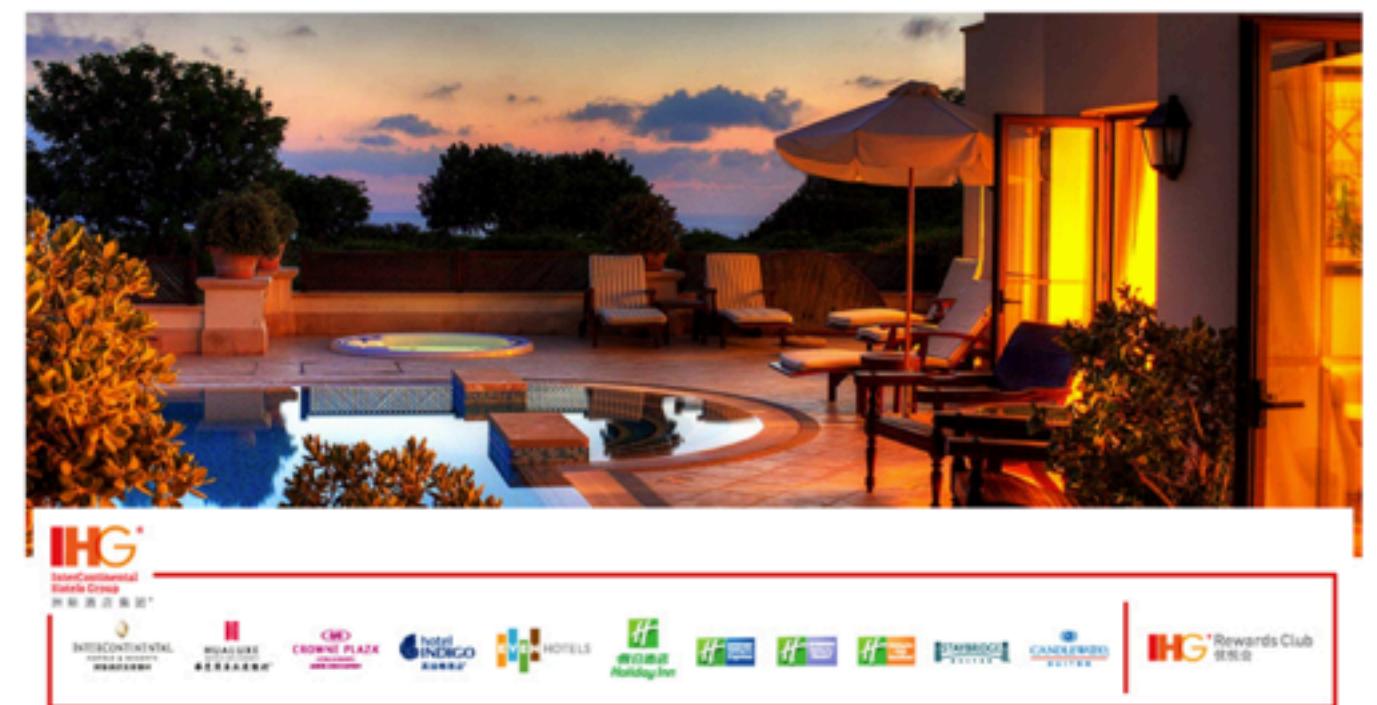
Product description

This purchase is for hacked Hotels.com accounts that got free night. The purchase only guarantees a login-able account, you should know how to use it properly before you buy! If you don't know how to use it and just want to buy one to test it out, you will be at your own risk.

If you need an account with reward dollar value, please send me a message for quote.

(PLEASE READ THE TERMS & CONDITIONS BEFORE YOU BUY)

Delivery will take between 1-3 days during week days from Monday 5pm EST to Friday 5pm EST. Any orders that's not received within the business hours will be accepted during the next business day.



洲际酒店集团优悦会的10000积分，可用于积分兑换集团内酒店的免费房间，包括国内外洲际、皇冠假日、英迪格、假日酒店、智选假日酒店。

由我们代订房或我们提供账号，客人自行预订，
积分兑换房间为普通房型，不含早餐。

一般假日及智选假日 10000–20000积分

皇冠 20000–40000积分

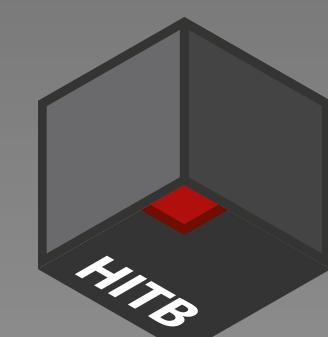
洲际 30000–50000积分

Hilton hotel room

The seller sells points in Hilton Honor accounts. Buyers can use the points to redeem free night award.

Price

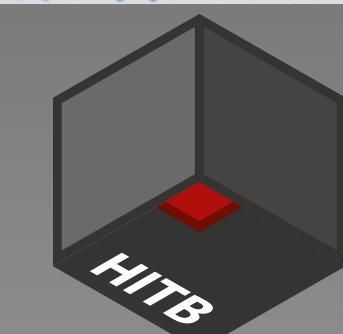
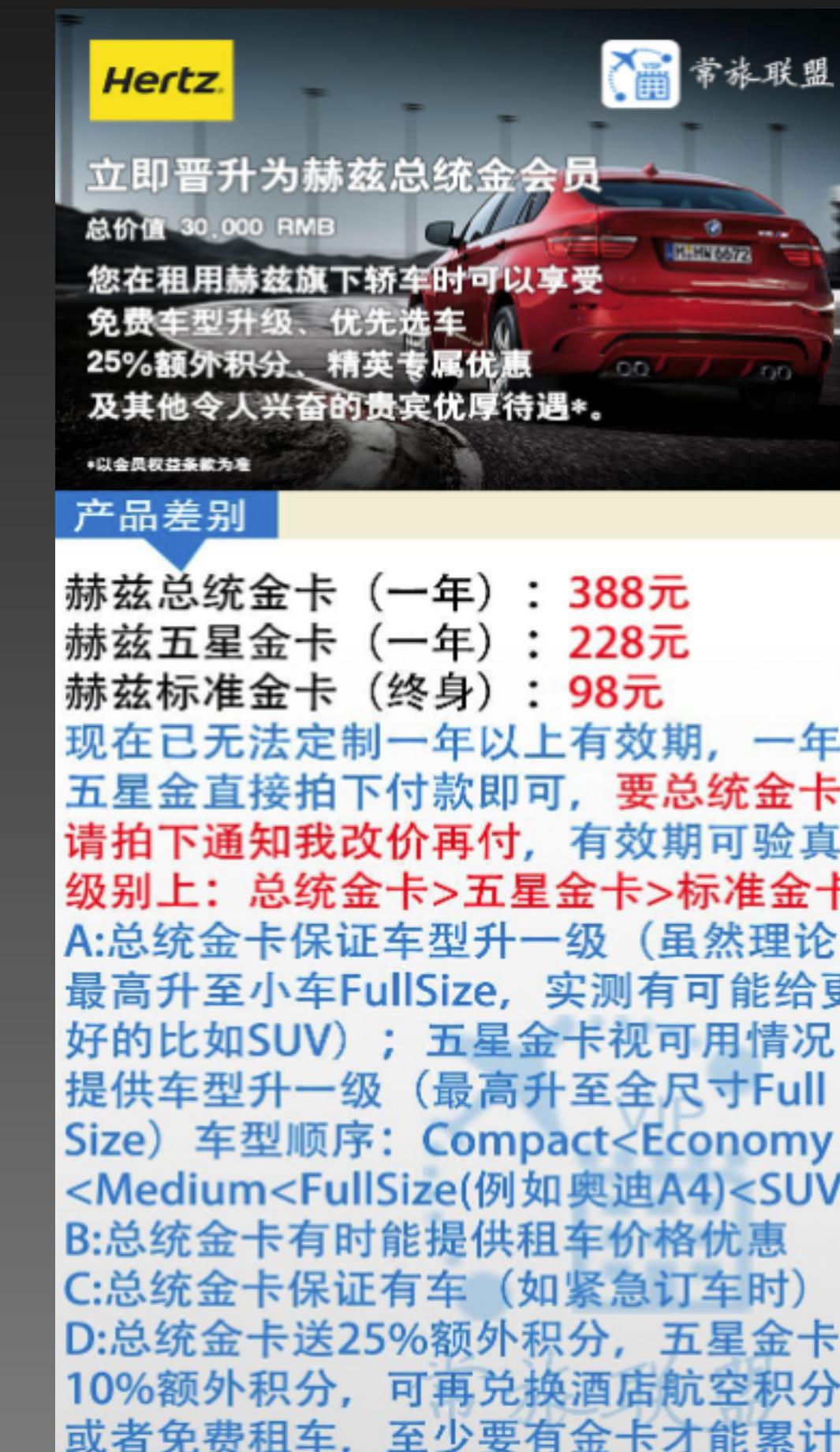
RMB 390 for 10,000 points



HITBSecConf2018
Amsterdam

Car Rental Loyalty Programs

- Involved services
 - Sixt, Hertz, Avis, National Emerald
- Benefits
 - Membership card
 - Free car upgrade
 - Free car rental
- Costs
 - \$40 - \$50



VPN service for telegram access!

- **Caution:** Since there's ongoing discussion about blocking Telegram in Russia, to maintain "Star Tours" service availability, please use Telegram @socks5_bot to setup VPN connection.....

Star Tours - путешествуй со скоростью света

⚡ В связи возможной блокировкой Telegram на территории РФ мы нашли решение. Прошу максимально распространить среди друзей и знакомых, дабы мы все не потеряли доступ к лучшему мессендеру на рынке. Коллеги, сделайте призывы в своих каналах тоже или просто репост этого сообщения.

Есть бот [@socks5_bot](#), который в несколько кликов позволяет установить внутренний VPN. Ниже прикладываю инструкцию как им воспользоваться.

Канал автора с обновлениями по боту: [@socks5ru](#)

1. Отправь боту /start, ты получишь приветственное сообщение.
2. Нажми «Получить», чтобы получить список с серверами
3. Выбери любой сервер, бот пришлет тебе данные для подключения
4. После получения сообщения с данными для подключения, нажми кнопку «Подключить», чтобы подключиться к серверу.

Studying the Victim Perspective of the fraud



Corporate Hotel Rates

IHG Corporate Codes 国际酒店协议价代码

Cisco 954410926

Oracle 100183394

IBM 000243132

General Electric 000102806

3M 000101672

Microsoft 100857558

Network Appliance 954284247

siemens 000104256

Motorola 128554

Dell 954284898

Wal-Mart Stores 000293512

Lenovo 100211707

AT&T 000150711

Target Corporation 000888400

FedEx 109207

MAKE A RESERVATION
Hyatt Centric The Pike Long Beach

ARRIVE DEPART
Nov / 07 / 2016 Nov / 08 / 2016

ROOMS 1
ADULTS 2
CHILDREN 0

SPECIAL RATES (AAA, GOVT, ...)

Select a Special Rate

None
 Government
 AAA / CAA Member
 Senior
 Special Offer Code
 Corporate or Group Code
13307

Check Availability

BEST RATES guaranteed



Can Hyatt Corporate Rates really

MightyTravels

Hyatt Corporate Rates

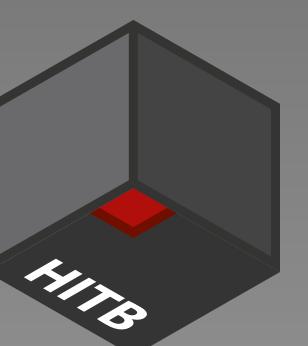
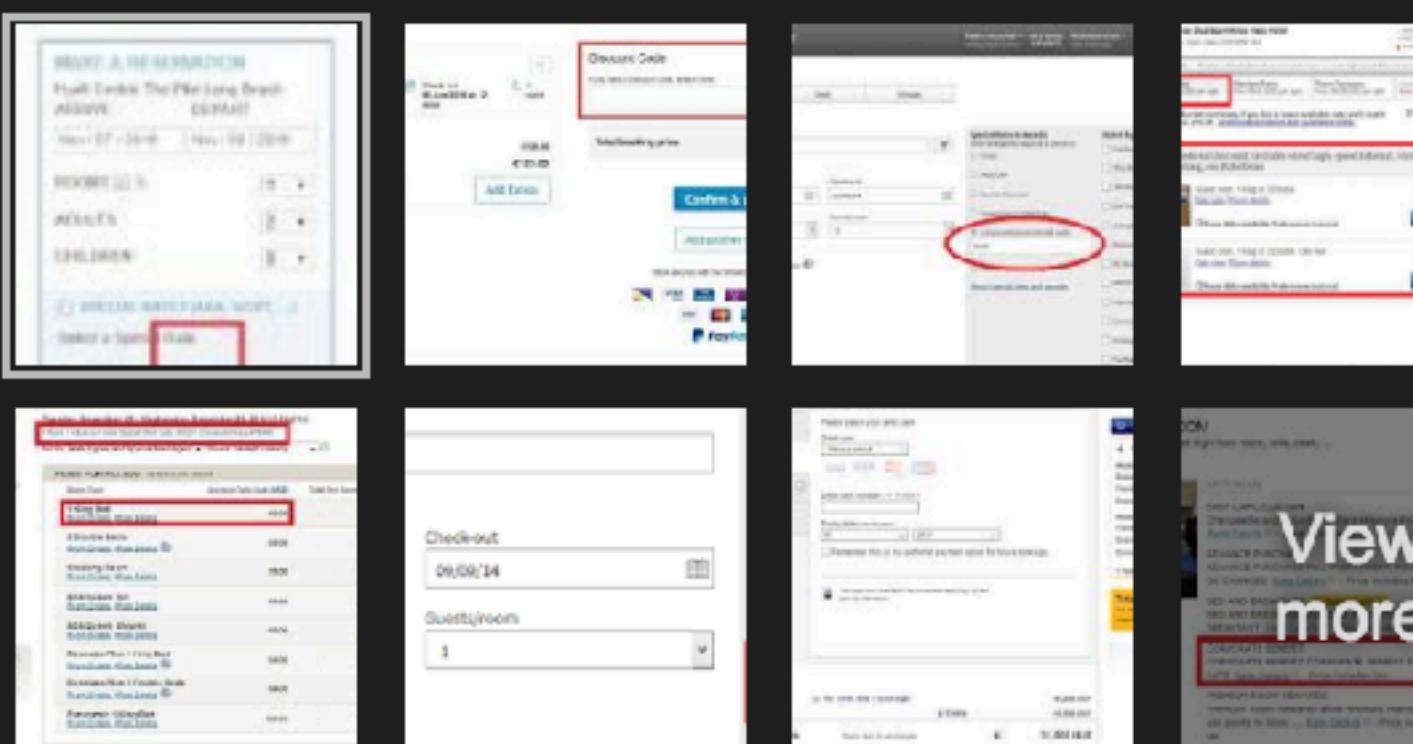
Visit

Save

View saved

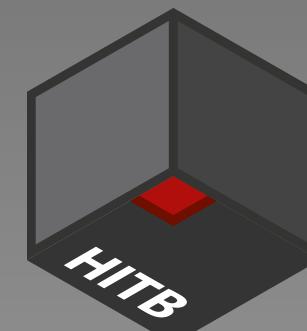
Share

Related images:



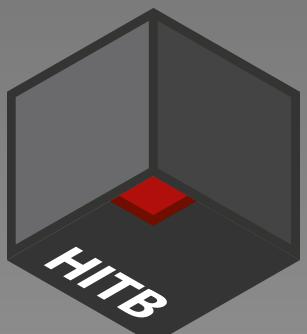
HITBSecConf2018
Amsterdam

fake corporate ID card



HITB SecConf2018
Amsterdam

**What can be done
to address this problem**



HITBSecConf2018
Amsterdam

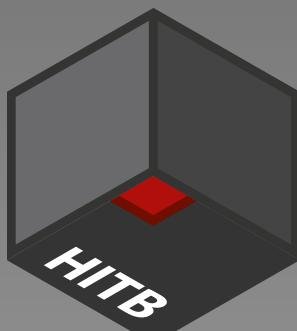
Hints for the Victim Organizations

Anti-fraud systems

For online booking - look for bookings done via
ToR, VPN, etc

Retrospective analysis of previous cases

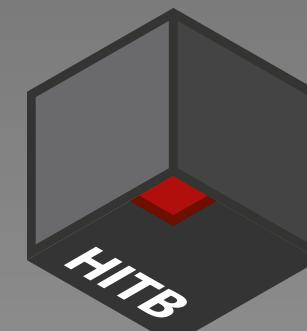
Know-Your-Customer: Due Diligence



HITBSecConf2018
Amsterdam

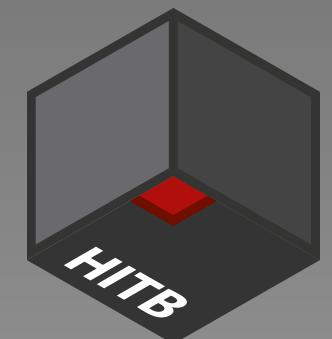
Hints for an Average Traveling Person

- check the hotel points often not just when you need them
- Your loyalty points and miles are money,
- do not protect them with easy to guess passwords ie:123qaz



HITBSecConf2018
Amsterdam

Q&A Session



HITBSecConf2018
Amsterdam

Thank You