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

Fyodor Yarochkin
Lion Gu
Mayra Rosario Fuentes
Vladimir Kropotov

Trend Micro FTR Team

9th annual HITB Security Conference in Europe
Agenda

Introduction to the travel fraud

Underground offerings

Criminal Backstage

Recommendations for the victims
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?
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
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
The view from the Underground: What the underground market offers
Happy Traveler Needs

nov, 2017
Basic services
Flights

OTELI I AVIAPERELETY by FIX

35%

40% - 50%

OTEI I DEPOZITY

Dепозиты и экскурсии за 50%

Минимальная стоимость отеля $600 в кассе

PERELETY PO VSEMU MIROU

40% для заказов от $1000 в кассе

Минимальная стоимость билета $300 в кассе

OTZVYLOVICHIVOST I SKIDKI

60% NA TURY V NRUIYA

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

KUDA:

SOCHI BOLGARIA CHECHIA ISPAHIA KIPR

TAILLAND GRECIA OAE DOMINKANA INDIYA

TELEGRAM: +7 962 323-24-03

HITB SecConf 2018

Amsterdam
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

smtp inbox to all unlimited
make smtp inbox

- Mailer 10$

- Methods
- prv shopping methods (electro _ army tools _ clothes ) 15$ for 1 method
- cash out method( make 1ks 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 full
  - usa 15$
  - europe 2$
  - 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%
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 🐘(ball)
Mobility

- 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

EU passports with customer provided PII for 2500$
residency permits and travellers blacklisting

- 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?
Guided Tours 25% from real price
Food services, Restaurants Logins and Gift Cards to Order food
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
All in one shop example
Air tickets:
1) Carsh - 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 cangular tickets are made through a fake-site website, in case of force majeure, they will point to where they took the ticket.
2) No cargo - 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 serve - 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, kayk, etc.) and copy the link of a specific offer (with dates, number of places, directions, prices, etc.).
payment:
RUB, QIWI
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
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

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

Vacha, 24 May 2016

До конца июня акция! за ВИДЕО отзыв скидка до 70% на все направления!
Авто, авиа, гостиницы по всему миру включая руру
<<<имя, 7000 в нашу сторону!>>>
для оперативного ответа писать за 3 дня до даты отдыха, перелета
успей за 30%!
Happy Travelers Feedback
Happy Travelers Feedback

ctuf1

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

Gadsden

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.

Upon arrival, we were met, we took passports. As usual they copied - that's all. Love!!
Special request Feedback

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 well.

Congratulations to the female half of the Forum on the Holiday of All Beautiful.

Photo of flowers from Paris.
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.

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.
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.
Not So Happy customer...

A buyer contacted the escrow company complaining about abuse because he didn't receive 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.
Ripers and clones...

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.
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.

САМОЗВАНЕЦ (КИДАЛА)

НАСТОЯЩИЙ ПРОДАВЕЦ
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

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.

At the same time, the authors of the letter emphasize that they were told in the booking center that hacking of private offices is not the first time. "Similar cases began to be repeated. In 2016, the same happened to several Crimean agencies. Anyway, now the reservation system waits for us to pay 47 thousand rubles. We wrote an application to the Ministry of Internal Affairs, provided all the documents, requested from ttbooking.ru the IP-addresses from which the booking was made. We are waiting for the results. Under the contract, ttbooking.ru is not responsible for security, but if such cases are repeated, perhaps the company management should think..."
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.
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
CC Kiddies Fraud

Юрий
Продам CC деп 200$, от себя
На гаrant-не согласен!

Тимур

Юрий
Продам CC деп 200$, от себя

Я думаю тебе не жалко будет он уже баблик

Я по отработке кардера работаю

Что он дает то и сую

Блин!
Exploitation of Vulnerabilities in Traveling systems

- "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"
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

VLAD
для водителя Яндекс!
Список снятых ограничений таков:
+ Конечный адрес всегда виден до принятия
+ Таксометр не видит Xposed и Fake GPS
+ Можно сменить статус без приближения к месту под 500 метров и позвонить без приближения к месту под
+ Нет необходимости в обновлении фотоосмотра (толь первый раз).
+ Увеличенное время автоотклонения
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
Hotel Loyalty

Hilton Hotel Gold Status Upgrade Valid to MAR 2019
Vendor: coronacheked (180) 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.

Hotels.com Free Night Account(s)
Vendor: dopegeo (130) 4.94% Price: $0.001006 ($5.99)
Ships to: Worldwide Ships from: Worldwide Escrow: Yes

Product description
This purchase is for hotels.com accounts that get 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 work 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.
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. Просьба 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.

Кanal 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

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 000150771
Target Corporation 000888400
FedEx 109207

Can Hyatt Corporate Rates really
Mighty Travels
Hyatt Corporate Rates

SPECIAL RATES (AAA, GOVT, ...)
Select a Special Rate
- None
- Government
- AAA / AAI Member
- Senior
- Special Code
- Corporate or Contract Code

Check Availability
BEST RATES guaranteed

Related images:
fake corporate ID card
What can be done to address this problem
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
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
Q&A Session
Thank You