CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

May 5, 2022

THE BUSINESS OF FRAUD:

Travel, Hospitality, and Loyalty Fraud

Recorded Future®

Recorded Future analyzed current data from the Recorded Future® Platform, dark web and special-access sources, and open-source intelligence (OSINT) between January 2021 and January 2022 to observe the primary tactics, techniques, and procedures (TTPs) used by cybercriminals to perform fraudulent activities against airlines, travel, and hospitality organizations and services. This report expands upon findings addressed in the first Insikt Group Fraud Series report, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized".

Editor's note: This research covers January 2021 to January 2022. Since then, the following dark web sources are no longer in operation: ToRReZ Market (January 2022) and Dark0de Reborn (February 2022).

Executive Summary

Airline and hospitality fraud is a general term that refers to illegal activities that target airlines, hotels, booking platforms, and other travel accommodation services providing car rentals, excursions, and more. Many of these services use loyalty programs where regular customers are rewarded with points that can be redeemed for free rewards. The popularity of these loyalty programs has led many other industries outside of travel and hospitality to begin implementing similar programs; the programs have also attracted the attention of scammers.

Airline and hospitality fraud includes various tactics, techniques, and procedures (TTPs) and is performed by threat actors on various forums, marketplaces, shops, and public messaging platforms. We analyzed our data sets from January 2021 to January 2022 and identified the most common TTPs used by threat actors to perform travel and loyalty fraud, the dark web and special-access sources that are popular among the threat actors engaged in this activity, and the specific threat actors who focus their efforts on advertising these criminal activities.

Key Findings

- Cybercriminals primarily use dark web forums, marketplaces, social media (such as Telegram) and shops to advertise services, counterfeit documents, and compromised user accounts that facilitate fraudulent activities against airline, hotel, and hospitality-related industries.
- The following TTPs were identified as being the most widely used by cybercriminals to target customers of airlines, hotels, and hospitality-related organizations: travel-themed phishing, fraudulent travel agency operations, sales and advertisements of travel fraud-related tutorials, and sales of compromised networks, user accounts, and databases that contain reward/loyalty points and personally identifiable information (PII) that could be used towards social engineering, money laundering, and other attack vectors.
- Cybercriminals are selling fake COVID-19 vaccination documents on dark web sources. There continues to be a high demand for such documents, which many countries require for travel.

Background

Services and activities that facilitate travel fraud have been both widely advertised and in high demand by threat actors since the inception of cyber-enabled crime. Cybercriminals primarily use stolen card-not-present (CNP) data and reward/loyalty points from compromised bank accounts to purchase flights, hotels, and other travel-related activity. Threat actors have continued to update their tactics in harvesting reward/loyalty points via compromised accounts, scamming victims into providing their travel-related documentation and data, and marketing updated how-to methods on defeating hotel and airline reservation services, among other activities. Despite the decline in air travel during the COVID-19 pandemic, an open source reported that the airline industry saw a 530% increase in cyberattacks directed at them. As the lockdowns from COVID-19 began to lift and international borders began to reopen, threat actors noticed an increase in demand for counterfeit COVID-19 vaccination documents and created a black market for them.

In 2021, Insikt Group observed approximately 4,000 references related to fraudulent activities targeting airlines and hotels worldwide. The following are the primary types of fraudulent methods being used:

- Advertisements for fraudulent travel agency services
- Listings of compromised accounts that contain rewards points
- Phishing and scam websites used to harvest PII and travelers' data
- Advertisements for counterfeit COVID-19 vaccination statuses and certificates
- Using compromised payment methods to purchase flight tickets and book hotels and other services

Threat Analysis

Fraudulent Travel Agencies and Affiliate Programs

The operation of fraudulent travel agencies on dark web sources as well as social media and messaging platforms is a primary attack vector used by cybercriminals to defraud airlines, hotels, and booking services. As a rule, cybercriminals use compromised payment cards to make purchases on various booking sites, and then direct witting and unwitting customers to send clean payments to cybercriminals' accounts. While stolen payment cards are most commonly used to make the bookings, some cybercriminals use loyalty rewards from compromised loyalty accounts or social engineering techniques to access corporate booking agents' accounts. Cybercriminals often offer additional discounts to customers who provide proof of travel, such as photos from exotic places with a sign or image naming the fraudulent travel service provider. Cybercriminals advertise these images to convince potential customers that the services are authentic.

Figure 1: Sun Aqua fake travel agency advertisement (Source: Dark web forum)

Table 1 below shows the most active threat actors who offer fraudulent travel agency services on dark web forums:

Threat Actor	Intelligence
"Serggik00" and "btckonvertbot"	Since 2018, threat actor Serggik00, a member of multiple Russian- and English-language dark web forums, has been offering airline ticket booking service, hotel bookings, and other travel-related services with an alleged 50% discount. The threat actor works in concert with another member of multiple forums, "btckonvertbot", who advertises the service on their behalf.
"Sun Aqua"	The threat actor is an operator of a fraudulent travel agency. According to the threat actor, they can book hotels with a discount of up to 25% for a 10-day period all over the world, excluding the following countries: Russia, Cyprus, Cuba, Egypt, the United Arab Emirates, China, Japan, and the Maldives. In Turkey they can book hotels only in Istanbul for up to 7 days. The threat actor also provides a 55% discount for all airfare ticket bookings, including to Russia. Sun Aqua provides the following booking instructions: • Book hotels via booking[.]com only starting from $530 • Minimum order is approximately $118 • Order the service 2-3 days before a planned visit • Do not use real payment cards or social media profiles during the stay at the hotel Cybercriminals recommend booking tickets 2-3 days before a trip because they use compromised payment cards. The chances of a legitimate cardholder alerting their bank when they see a suspicious transaction would be lower if the tickets were purchased a month or a week before. Also, for security purposes, fraudulent service providers do not recommend using real documents, payment cards, or social media profiles to avoid criminal prosecution or being forced to pay the actual charge if the fraudulent payment falls through.
"Patriarh"	The threat actor is a member of multiple Russian-speaking forums. Patriarh has been operating the fake travel agency "Patriarch Travel" since July 2017. According to the threat actor, they provide hotel bookings and airline tickets with up to a 50% discount.

Table 1: Threat actors advertising fake travel agencies on dark web sources (Source: Recorded Future)

Cybercriminals perform other types of travel fraud associated with fraudulent hotel and vacation bookings via various services. Typically they create fake listings on different travel services to illegally book services or launder money.

One of the techniques to create fake listings involve using brute-forced accounts, which can be purchased on dark web forums or marketplaces. The second technique involves using information from stolen log files, which can contain logins, email addresses, passwords, user-agents, user IP addresses, and cookies associated with the accounts, which can be purchased on dark web shops. The third technique is based on the use of self-registered accounts.

Cybercriminals usually collaborate to make fictitious reservations, accept payments, and split profits. There are 3 main ways cybercriminals conduct this type of fraud:

- Cybercriminals create fictitious host accounts and fictitious booking accounts, then use stolen CNP cards to make the bookings themselves.
- Cybercriminals gain access to legitimate accounts and use stolen CNP cards on accounts that have legitimate booking history on them. These accounts could be used to make real bookings, which can later be resold, or if they have access to host accounts, they could process transactions to themselves.
- Cybercriminals can also find legitimate hosts that would agree to process payments without actual guests staying at the property (so-called "dark" hosts).

Airline Ticket Fraud

In September 2021, Travel Weekly reported that "through mid-September, fraud detectors at ARC had found approximately 80 instances of unauthorized ticketing, accounting for approximately $1.2 million". In the report, it was also noted that criminals often use compromised account credentials from the travel advisor's global distribution system (GDS), the worldwide conduit between travel bookers and suppliers, such as hotels and other accommodation providers. Threat actors obtain access to those credentials through phishing attacks on travel agencies or service providers.

According to Interpol, threat actors typically use the following fraudulent techniques to purchase airline tickets:

- Threat actors use stolen payment cards to purchase airline tickets.
- Threat actors advertise these tickets for discounted prices at websites or social networking accounts that impersonate legitimate travel agencies or agents.
- Fake travel agents ask for immediate payment, typically by cash, bank transfer, or virtual currencies.
- After receiving payments, victims receive the airline booking confirmation, but with their original purchase details deleted.

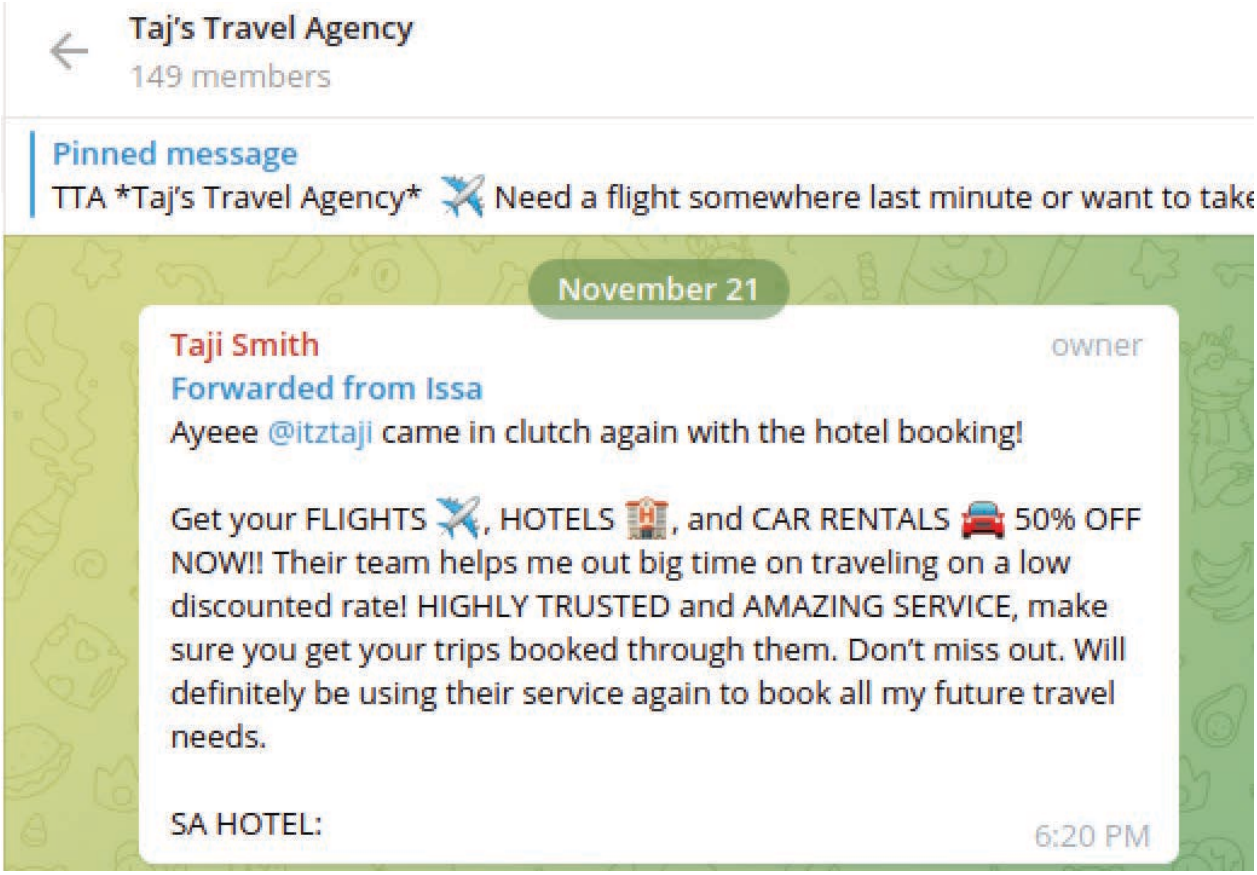


Figure 2: Fake travel agency offering a 50% discount on airline tickets and hotel and car rental bookings (Source: Telegram)

A search for the airline tickets for sale on various messaging platforms in the Recorded Future database found 156 references linked primarily to Telegram channels and groups that perform the sales of airline tickets and operate as fraudulent travel agencies.

In one Telegram channel, instructions were shared for how cybercriminals use airline tickets for money laundering schemes:

- The fraudster should be connected to NordVPN or VyprVPN.
- The fraudster purchases compromised payment cards with full cardholder personal information on unspecified sources.
- The fraudster visits the website kiwi[.]com, a Czech online travel agency, and buys airline tickets.
- After receiving an email confirmation, the fraudster chooses a refund option using a new wallet created to launder money.

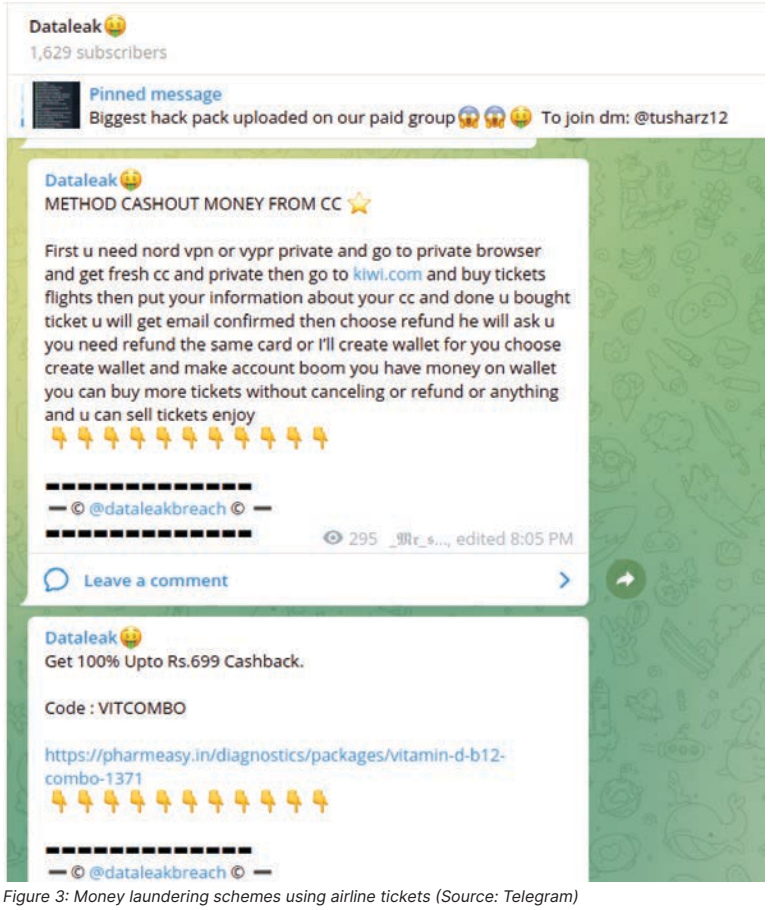


Figure 3: Money laundering schemes using airline tickets (Source: Telegram)

Sale of Compromised Accounts With Reward Points

Compromised accounts and data do not only contain data points that a cybercriminal can use to access a victim's account or perform identity theft, but can also contain valued rewards points that can be used to purchase tickets or merchandise or be cashed out for hard currency. Many of these same dark web and special-access sources, as well as attack vector methods for compromising and harvesting PII, also list travel and hospitality-related accounts with rewards that can be used fraudulently.

Loyalty Fraud

Cybercriminals use stolen payment card data or, less often, access to bank accounts with air miles and hotel points to book air tickets or hotel reservations, and request that their customers provide payment for this service upfront. After payment, users receive booking confirmations; however, these bookings are usually active for a short period and could be canceled by companies that flag and identify the activity as fraud. This is why cybercriminals providing these types of services often recommend making bookings right before travel and for a short duration.

Booking services using compromised payment cards is a more popular method on the dark web than using bonus points. Once cybercriminals have obtained air miles, they can extract the value by booking travel, but they also have access to a variety of products and services, including gift cards. These gift cards are highly desirable to threat actors because they do not require an identification document (ID) or personal identification number (PIN).

Loyalty fraud is difficult for security professionals and travel industries to detect. Fraudsters usually obtain enough information, through social engineering or other means, to get access to these accounts and appear to be the genuine user. Considering the poor security of reward points, this makes them easily accessible to fraudsters. Often, the victim of loyalty fraud will not know of their loss until they check their balance or decide to use the points. Due to the difficulty in detecting loyalty fraud, the value of loyalty points becomes no different than actual currency that threat actors can use to book travel. And given the financial success of hotels and airlines rewarding repeat customers through points, other sectors have begun to also include loyalty programs, including e-commerce, retail, food and beverage, gaming, and more. It is projected that the global loyalty market will reach a value of $11.4 billion by 2025.

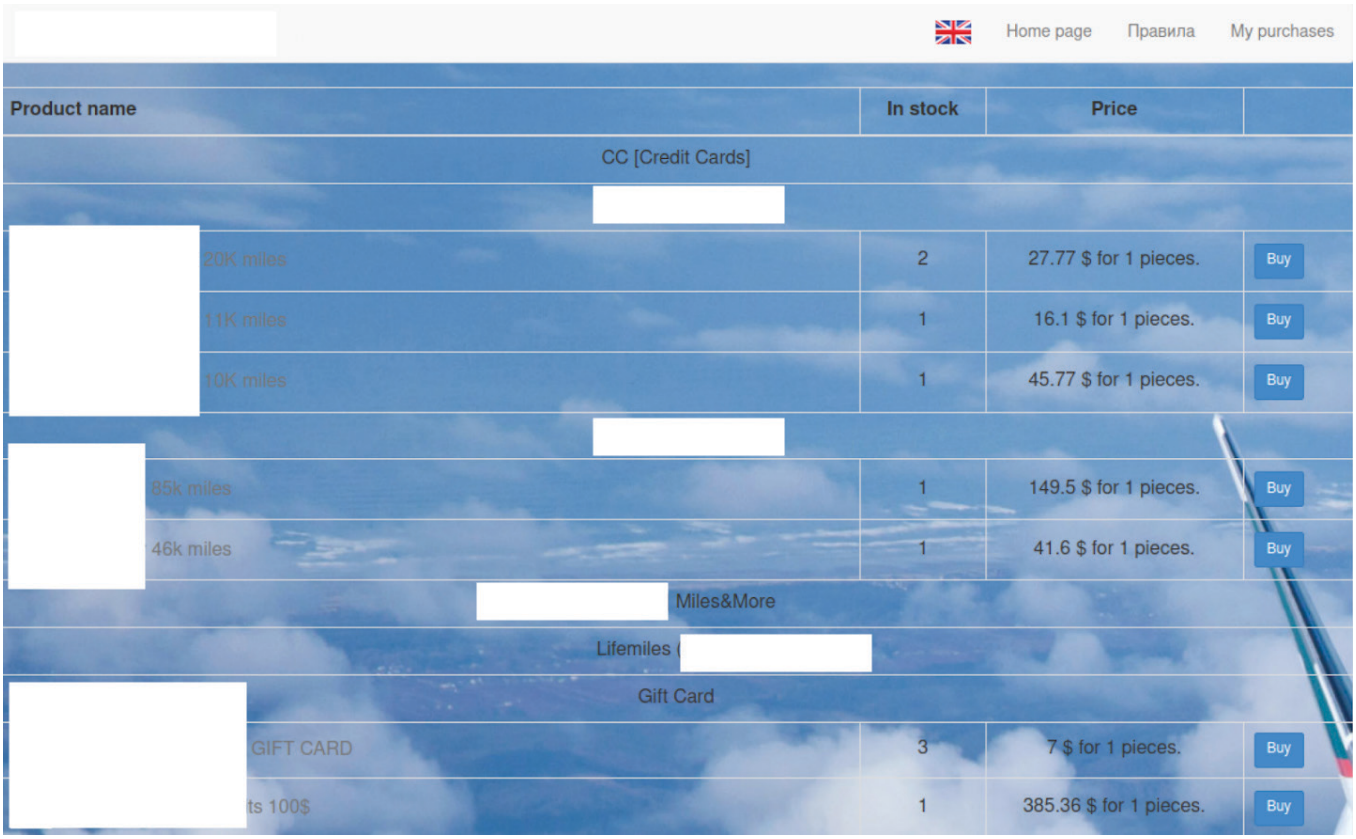
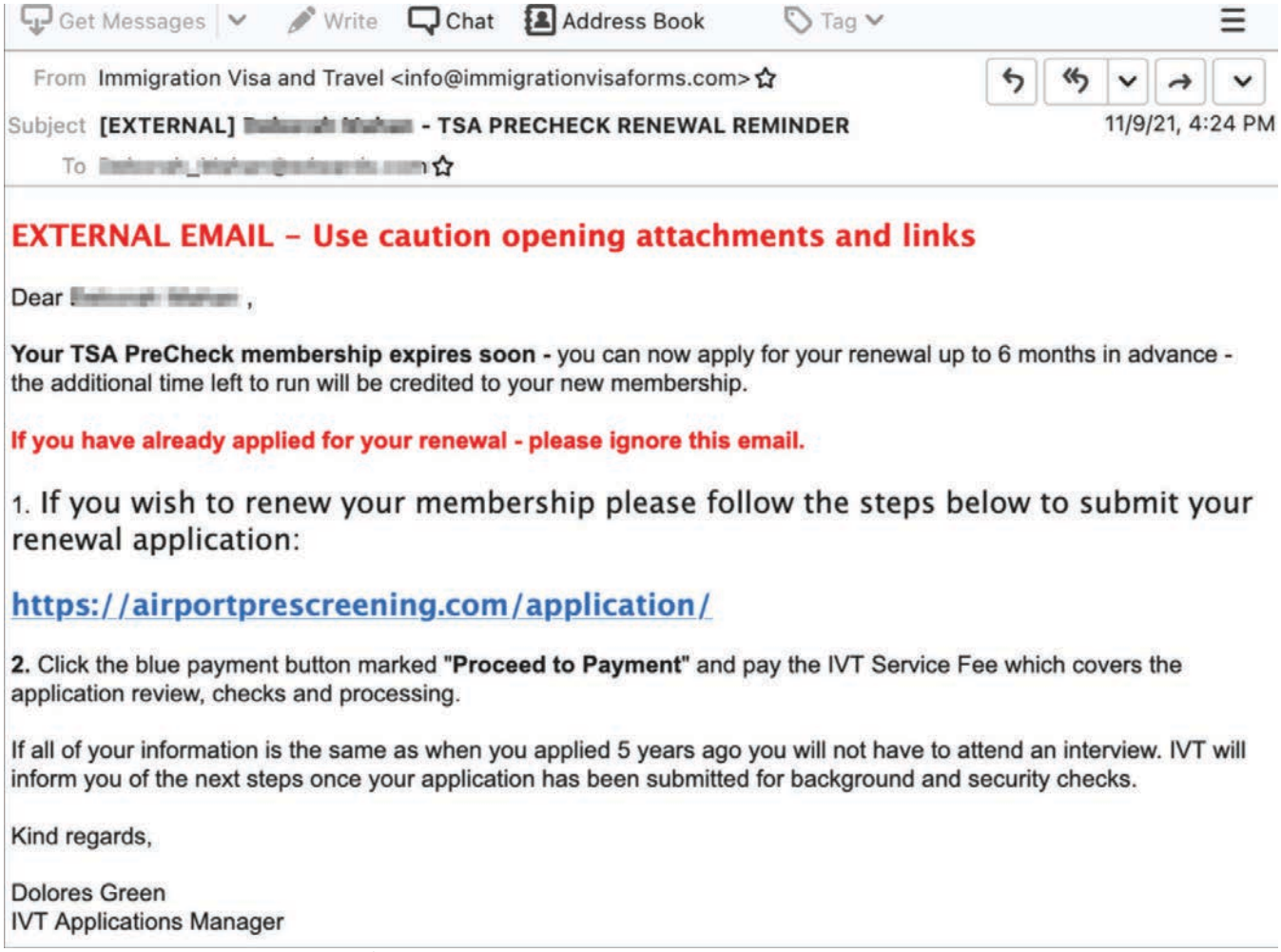


Figure 4: Air miles and gift cards for sale on the dark web (Source: Dark web shop)


Get Messages | Write | Chat | Address Book | Tag

From Immigration Visa and Travel <info@immigrationvisaforms.com>

Subject [EXTERNAL] [redacted] - TSA PRECHECK RENEWAL REMINDER 11/9/21, 4:24 PM

To [redacted]

EXTERNAL EMAIL – Use caution opening attachments and links

Dear [redacted],

Your TSA PreCheck membership expires soon - you can now apply for your renewal up to 6 months in advance - the additional time left to run will be credited to your new membership.

If you have already applied for your renewal - please ignore this email.

1. If you wish to renew your membership please follow the steps below to submit your renewal application:

https://airportprescreening.com/application/

2. Click the blue payment button marked **"Proceed to Payment"** and pay the IVT Service Fee which covers the application review, checks and processing.

If all of your information is the same as when you applied 5 years ago you will not have to attend an interview. IVT will inform you of the next steps once your application has been submitted for background and security checks.

Kind regards,

Dolores Green
IVT Applications Manager

Figure 5: Fake TSA PreCheck renewal applications (Source: Abnormal Security)

There are many shops on the dark web that advertise compromised airline accounts containing miles, hotel accounts with bonus points, gift cards, and credit cards with linked bonus miles or points. The prices for bonus miles usually depend on their amounts and airline brand and can range between $6 to $200.

Compromised Databases, Networks, and Credential Leaks

As a rule, network intrusions and subsequent database breaches provide the underground economy with an influx of new data, which can be subsequently used in various ways, including credential stuffing, spamming, phishing, social engineering, SIM swapping, and business email compromise (BEC) attacks. A search in the Recorded Future Platform found over 4.4 million leaked credentials related to airlines, travel, and hospitality organizations worldwide since January 1, 2021. We also observed many network intrusions and database breaches related to the travel and hospitality industry in 2021. A sample of threat actors advertising this kind of access can be found in Appendix A.

Phishing Against Trusted Traveler Program Websites

Threat actors have also deployed phishing campaigns against users of travel security programs to harvest user logins (PII) and data. In 2021, threat actors used phishing techniques to defraud users of the Transportation Security Administration's (TSA) PreCheck, Global Entry, and NEXUS application service websites. The first evidence of these attacks was identified in March 2021.

TSA PreCheck is a program that allows people who have completed criminal history vetting to pass through a quicker and easier screening process at the airport. The TSA PreCheck needs to be renewed every 5 years for $70. Threat actors sent their victims the renewal reminders via email and urged them to submit an alleged application that hosted various domains and, as a result, stole their login account credentials. The malicious domains that were detected during the phishing campaign were as follows:

- airportprescreen[.]com
- airportprescreening[.]com
- applyfornexuscard[.]com
- assist-gov[.]com
- applyglobaltraveler[.]com
- easynexusapplication[.]com
- fastpassapplication[.]com
- lowrisktraveler[.]com
- immigrationvisaforms[.]com
- travelauthorizationusa[.]com

COVID-19 Vaccination Documents for Sale on Dark Web Sources

As domestic and international travel continues to increase following the tight regulations associated with the COVID-19 pandemic, threat actors are already redeploying established fraud schemes and unveiling new schemes to defeat security measures. We identified threat actors using both dark web forums and marketplaces to list offers for COVID-19 vaccination certificates, passports, pre-departure PCR tests, or other relevant documents that permit a person to bypass security/border measures in order to travel internationally.

Table 2 below provides a list of the most active sellers of the fake COVID-19 vaccination documents on dark web forums over the past year.

Threat Actor	Intelligence
"busyb0b"	In January 2022, the threat actor advertised on multiple Russian-language forums digital certificates for major vaccine manufacturers for 350 euros. According to the threat actor, the certificates would be registered in official Polish databases. The threat actor uses Telegram (busyb0b) as a primary method of communication.
"GOCHA200"	In December 2021 and January 2022, the threat actor was selling on one of the Russian-language forums fake vaccination digital certificates with QR codes issued in France and Poland for EU and non-EU residents. The prices for these certificates varied from 400 to 550 euros.
"docks_eu"	From November to December 2021, the threat actor, who operates on multiple Russian-language forums, advertised various services related to fake documents needed for travel: • Fake vaccination digital certificates for in all EU countries and Ukraine • Foreign passports with chips for all European countries and without chips for Romania, Slovakia, Czech Republic, Lithuania, Hungary, and Ukraine • Visas to Poland, Estonia, Hungary, France, Ireland, Spain, Germany, Lithuania, and more
"mail-tophse1231"	In October 2021, the threat actor, who operates on one of the top-tier Russian-language forums, offered Polish COVID-19 vaccination passports by registering them in the official database for $250.
"Outlawz"	In October 2021, the threat actor on dread Forum was selling COVID-19 vaccination passports and QR codes registered in Green Pass application for 150 euros. The threat actor could provide vaccination documents for all EU countries and the UK. Outlawz was also hiring re-shippers who can send 5 to 15 certificates in Europe weekly for 50 euros each.

Table 2: Threat actors advertising fake COVID-19 vaccination documents on dark web sources (Source: Recorded Future)

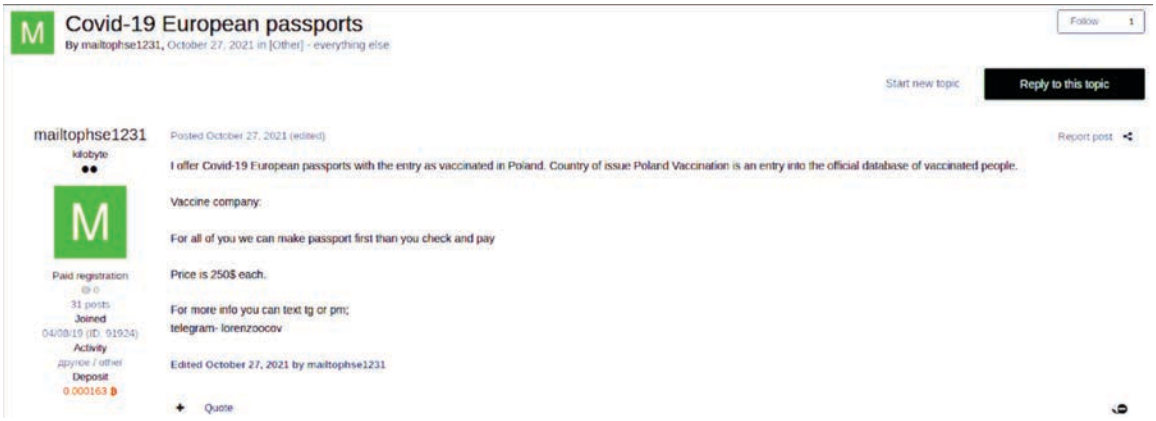


Figure 6: Fraudulent COVID-19 vaccination passport listing on the dark web (Source: Russian-language dark web forum)

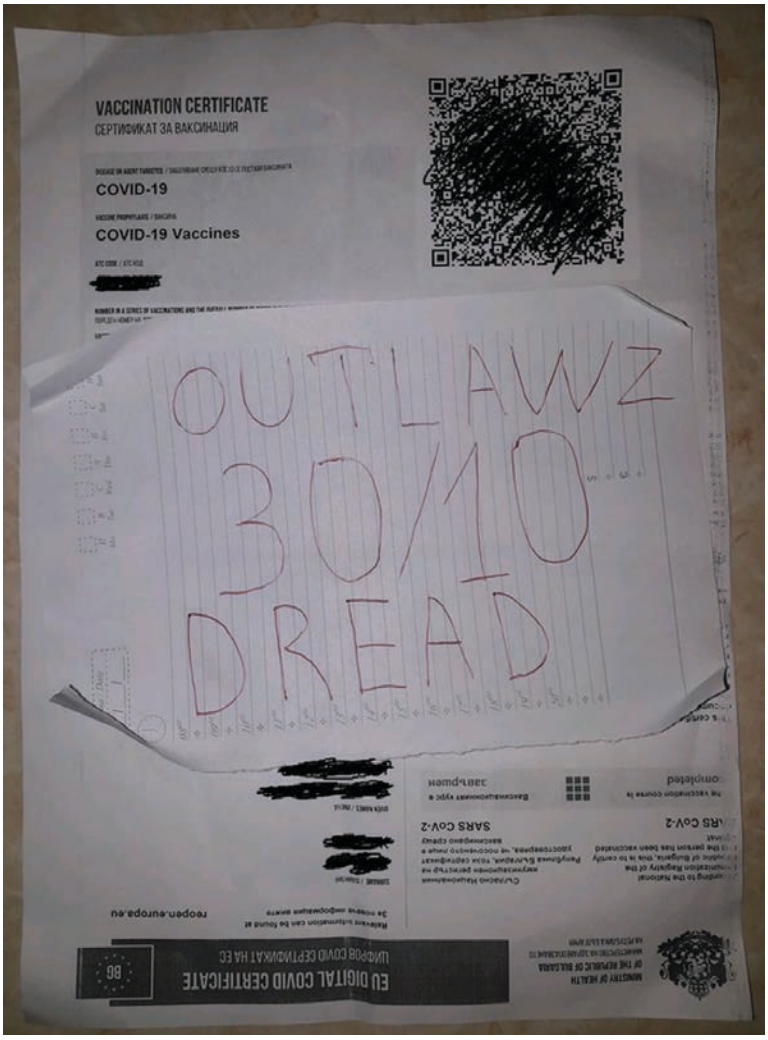


Figure 7: Outlawz advertising COVID-19 vaccination certificates (Source: dread Forum)

Analysis of Recorded Future data over the last 1 year identified multiple dark web marketplaces to be the most active for listing COVID-19 counterfeit vaccination certificates and documentation. We identified at least 20 separate threat actors using dark web marketplaces to advertise COVID-19 false documentation, with a sample of these threat actors listed below:

Threat Actor	Intelligence
"apple"	In September 2021, the threat actor posted for sale on a dark web marketplace COVID-19 vaccine cards with barcodes for $420 CAD. In addition to listing false COVID-19 vaccination cards, the threat actor stated that they also create counterfeit health passes with QR codes.
"bestshop"	In October 2021, the threat actor advertised on a dark web marketplace COVID-19 vaccination cards described as from an unspecified physical vaccine site in the US for $550. From the purchased date, the negative test result would arrive within 3 to 5 business days.
"fastfrance"	In January 2022, the threat actor listed for purchase on a dark web marketplace a French Sanitary Pass that confirmed vaccination status for 450 euros. The threat actor stated that they work with France-based doctors and that the certification will appear within an Amelie account (required login). Orders are processed and uploaded within 24 to 48 hours.
"Quantom"	In January 2022, the threat actor advertised on a dark web marketplace COVID vaccination cards for $250. The threat actor states that they are in the medical field, have access to vaccination databases containing vaccine lot numbers (validation), and that buyers will receive a PDF of their vaccine card (physical copy will be shredded).

Table 3: Threat actors advertising fake COVID-19 vaccination documents on dark web marketplaces (Source: Recorded Future)

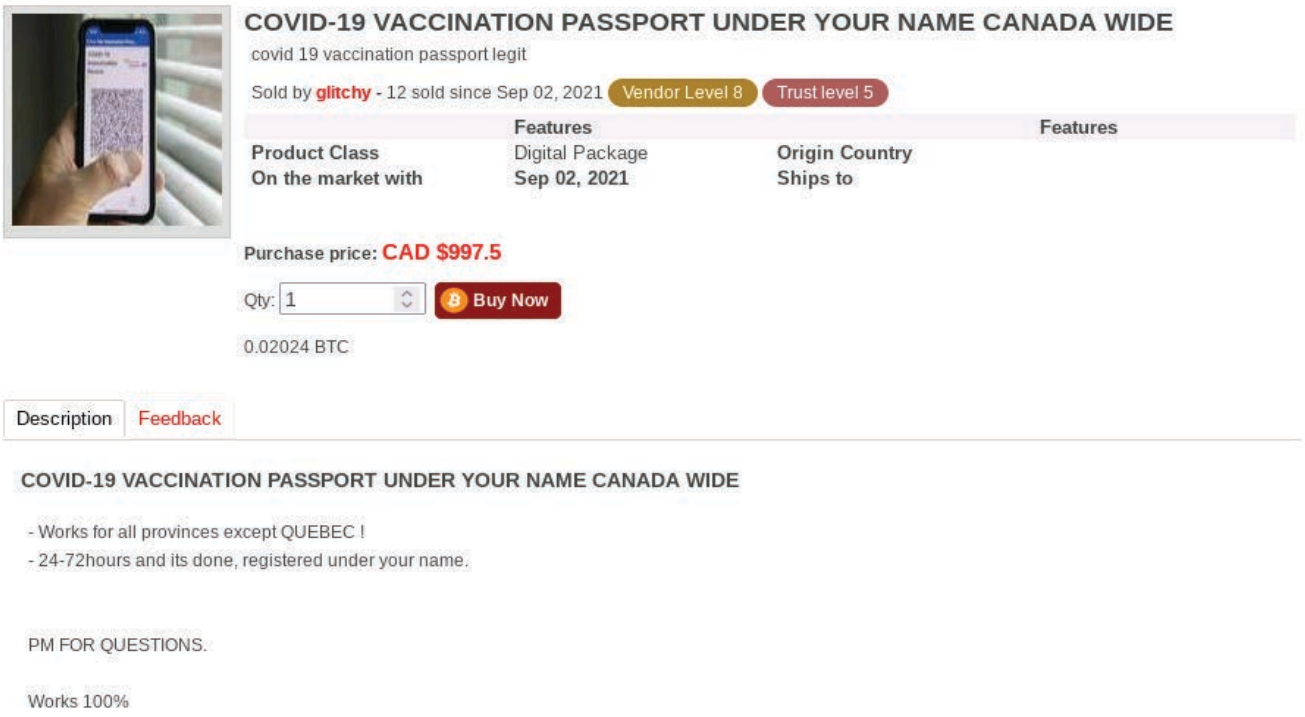


Figure 8: COVID-19 vaccination passport as advertised by "glitchy" (Source: Dark web market)

Mitigations

The following mitigation techniques can reduce the damage caused by various types of travel and hospitality fraud:

- Purchase airline tickets and book hotel reservations only on legitimate airline or well-known service provider websites.
- Do not use social media for purchasing airline tickets.

Fake travel agency websites often use country-specific top-level domains (such as ".eu," ".ru," ".ua") and sometimes display inactive icons (for example, "AppStore," "Google Play") to appear authentic. Be aware of these characteristics, as they may assist in positively identifying a fictitious travel agency website.

Do not reply to unsolicited emails, texts, social media, or calls with holiday or other gift offers.

Communicate directly with the property owner or their agent and ask them questions about the booking, room, location, and area of the property.

Check the terms and conditions before making a purchase, in particular the refund policy and processes

Credential leaks and email exposure amplify the risks associated with phishing, network intrusions, and database breaches, as the data can be used to devise tailored spearphishing lures and serve as initial points of compromise via credential stuffing and account takeover. Recorded Future clients can use queries in the Recorded Future Platform to surface exposed credentials on dark web forums and marketplaces. Organizations should determine if the exposed credentials that appear alongside passwords are still active and, if so, force password resets for those users, specifically accounts that contain sensitive PII or PHI data.

Threat actors can attack networks using proprietary tools, vulnerabilities in networks, or other attack vectors. The following practices may mitigate the risks of threat actors targeting PII and PHI:

- Keep all software and applications up to date, especially operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of your system and store the backups offline, preferably offsite, so that data cannot be accessed via the network.
- Have a well-thought-out incident response and communications plan.
- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (for example, through device or account takeover via phishing).
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Employ host-based controls; one of the best defenses and warning signals to thwart attacks is to conduct client-based host logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like a network intrusion detection system (IDS), netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Be aware of partner or supply chain security standards. Being able to monitor and enforce security standards for ecosystem partners is an important part of any organization's security posture.

Outlook

We believe that threat actors will continue to use dark web marketplaces, forums, and shops to advertise, discuss, purchase, and request compromised account credentials and reward points of airlines, hotels, and various booking services that facilitate travel and loyalty fraud. Cybercriminals will use encrypted messaging platforms, specifically Telegram, to advertise, sell, and purchase travel-related products and services more often in the foreseeable future.

Among primary TTPs used by cybercriminals to defraud airlines, travel, and hospitality organizations are the sales and publicly sharing of the compromised PII, including account login credentials, reward points, and bonus miles; phishing attacks; and the operation of fake travel agencies. We believe that fraudulent travel agencies will remain in high demand, as these services provide anonymity in purchasing tickets and making booking reservations, as well as permit the use of compromised payment cards and bonus rewards in purchasing discounted tickets and book reservations. As the COVID-19 pandemic continues to evolve and remains unpredictable, sellers of counterfeit vaccine documentation will continue and are likely to update their listings (physical cards and digital passes) based on newly issued travel and government regulations.

Appendix A: Major Sellers of Travel and Hospitality Industry-Related Data on Dark Web Sources in 2021

Threat Actor	Intelligence
Injection, aka Inanimate	The threat actor is a known seller of stolen hotel and airline databases: • In December 2021, they were selling the database Singapore-Malaysia Hotels Group with 2,125,185 records from 2008 to December 2021 that include full names, email addresses, genders, and company names for $500. • In September 2021, they were selling 13 million compromised records (sized 1 GB) for $500 from an unnamed Malaysia-based airline that included the following PII: full names, dates of birth, nationalities, passport numbers, mobile phone numbers, and more. The threat actor uses Keybase (injecti0n) as a point of contact.
Novelli	On November 15, 2021, the threat actor Novelli sold RDP account credentials with local administrator privileges of a Costa Rican hotel with more than $50 million in annual revenue on one of the top-tier Russian-language forums. The starting price was $150 or it could be purchased directly for $350.
hackworld	On November 6, 2021, the threat actor on several Russian-language top-tier forums sold SQL injections to 2 versions of a customer management system (CMS) server (Microsoft SQL Server) that serves hotels primarily in the US and Canada. According to the threat actor, they identified 130 hotels using the product and 35,000 owners have access to it. According to the developer's statement, the service was used by more than 100 resorts. The starting price was $1,000 or it could be purchased directly for $5,000. The threat actor titled the SQL injection as "zero day"; however, as a rule, a unique zero-day exploit typically costs $50,000 or more on the dark web.
b00L	On August 3, 2021, the threat actor on a dark web forum was auctioning off PHP web shell access with administrator privileges to the website of a US hotel booking service and its database with full payment information. According to the threat actor, the website accepted direct payments. The starting price for the account credentials was $5,000 or they could be purchased immediately for $15,000.
xeda777	On August 3, 2021, the threat actor on a Russian-language forum was selling access to the network of an unspecified airline company via compromised Cisco AnyConnect credentials. The threat actor did not specify the price on the forum openly.
inthematrix1	On July 13, 2021, the threat actor inthematrix1 on one of the top-tier Russian-language forums sold RDP account credentials with administrator privileges to the server, web server, and entire database of an unspecified Greek hotel and access to the point-of-sale (POS) software used at the restaurant located at this hotel. The auction started from $500 with an immediate purchase for $1,000.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.