



# CYBERCRIMINALS TAKE A VACATION ON THE HOSPITALITY AND AIRLINE INDUSTRY

May 2011

Most cybercriminals have one motivation in mind: to make money. For that reason alone, every industry, not just financial services, is a target for a potential cyber attack. The hospitality and airline industry is lucrative just for the sheer volume of customers' personal and financial data they would like to have access to. But cybercriminals have also discovered other unique ways to exploit the industry.

## FRAUDSTER AIRLINE AGENCIES

Legitimate online travel agencies are getting competition from the darkest corners of the Internet – the black market. Fraudster travel agencies are springing up all over the cybercriminal underground and offering unbeatable prices for worldwide airline tickets to other fraudsters. How are they able to do it? There are two main ways they accomplish this:

- The most common way is to use stolen credit cards to purchase airline tickets. A recently released report<sup>1</sup> showed that airlines lost nearly \$1.4 billion in 2010 due to online payment fraud. As you can see in Figure 1, a criminal offering a fraudster-operated ticketing service offers to sell tickets for any kind of travel with a “99.99% assured success” rate and at only 20-30% of the face value of the ticket. (Of course, the criminal buyer pays the fraudulent ticket agency using a stolen card, as well).
- The second way, while not nearly as common but growing in popularity, is to secure access to consumers' loyalty and rewards program accounts and cash out available points in exchange for travel vouchers. RSA has witnessed multiple phishing attacks recently targeting airline customers with the goal of obtaining their login credentials in order to monetize their reward points.

## STOLEN DOCUMENT DEALERS

Consider a customer of the fraudster-operated travel agency that just got the travel deal of a lifetime. He was able to purchase a \$1,000 airline ticket for just \$200. But advised by the dealer to purchase his ticket under a different identity, the cybercriminal is then referred to another underground service provider that can provide him with a stolen passport to be anyone he wants to be to make his trip. The cybercriminal has decided he is going to take a European vacation so he will need a passport. Welcome to Scanlab... the largest collection of documents on the Web (see Figure 2).

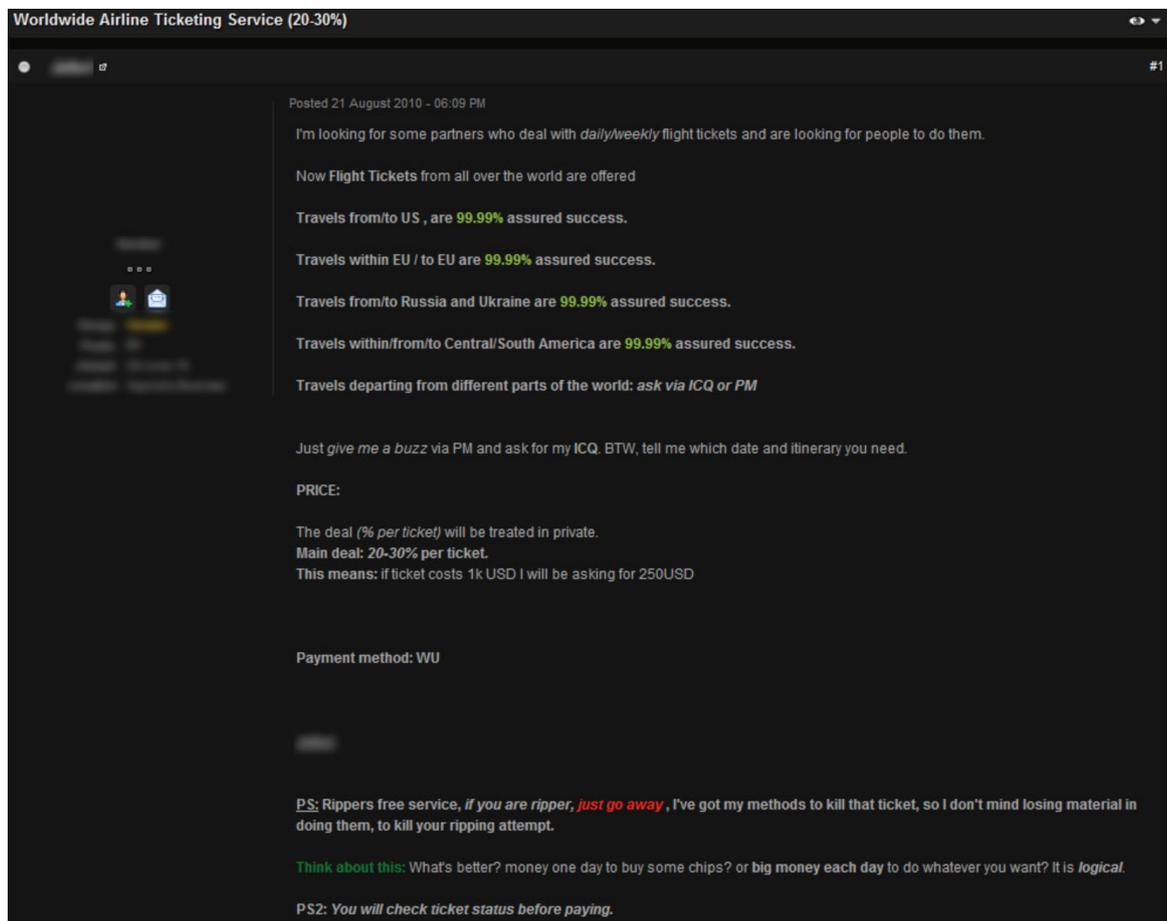


Figure 1: A cybercriminal sells airline tickets purchased with stolen credit cards

## AMUSEMENTS AND ATTRACTIONS

While in Europe, the cybercriminal plans to meet up with some of his fellow fraudsters and is looking for something to do. What better way to have fun than to visit an amusement park? The fraudster wants a bargain - and needs to look no further than the black market for more amazing deals. Amusement park tickets - purchased from the seller with a stolen credit card - can be had at a fraction of regular admission prices (see Figure 3).

## LODGING AND ACCOMMODATIONS

The cybercriminal now needs a place to stay during his whirlwind European vacation. Forget boarding houses or low-budget motels. He has fine taste and wants to stay at the best international hotels. His plan: to launch phishing attacks against customers of the world's top hotels in order to obtain access to their loyalty and rewards points. With this information in hand, he can stay in the finest suites across Europe – all at the expense of unsuspecting consumers.

While presenting just a fictional use case, these types of events are taking place every day within the black market. At the end of the day, there are many victims in these fraudulent schemes. The industry, which suffers from chargebacks from purchases made with stolen cards. Then there are the effects on reputation from cybercriminals abusing the brands of reputable airlines, hotels, amusement parks and other hospitality service providers through targeted phishing attacks against their valued customers. And finally, there is the loss to the consumer who is unwittingly scammed into divulging personal and financial information.

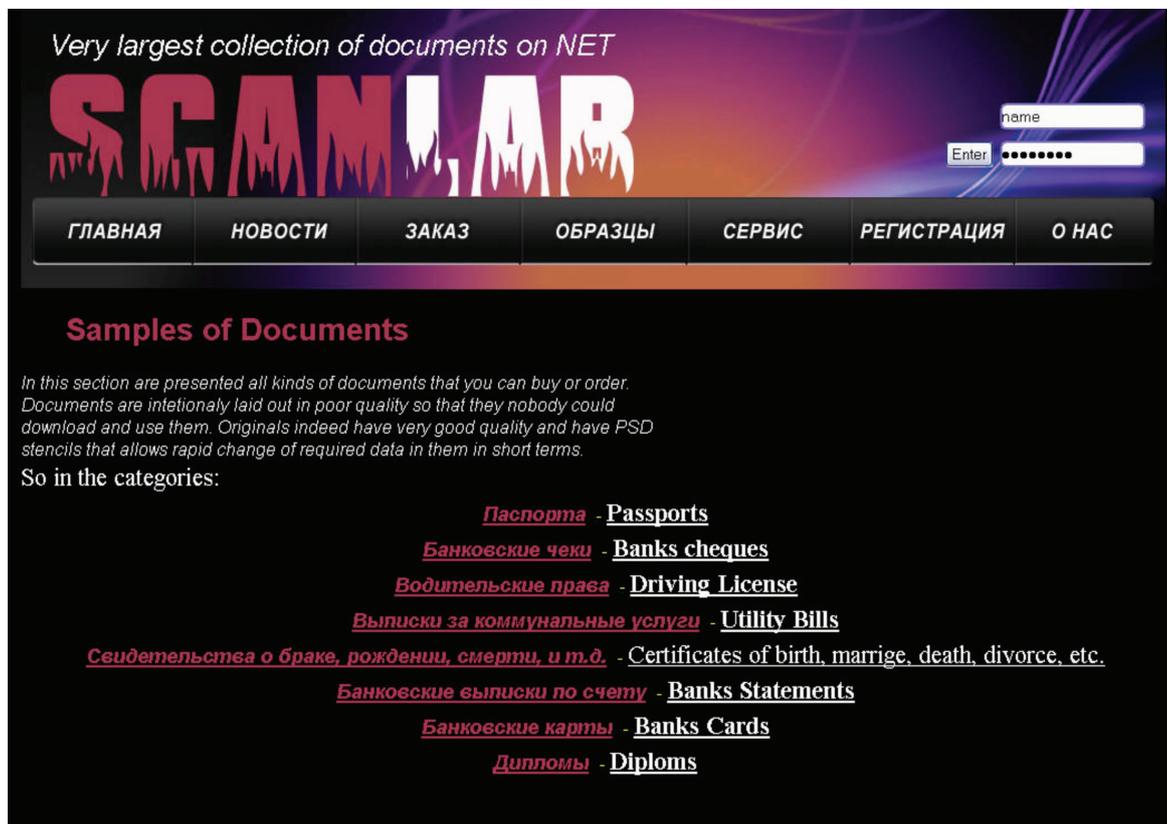


Figure 2: A cybercriminal shop that specializes in selling stolen documents

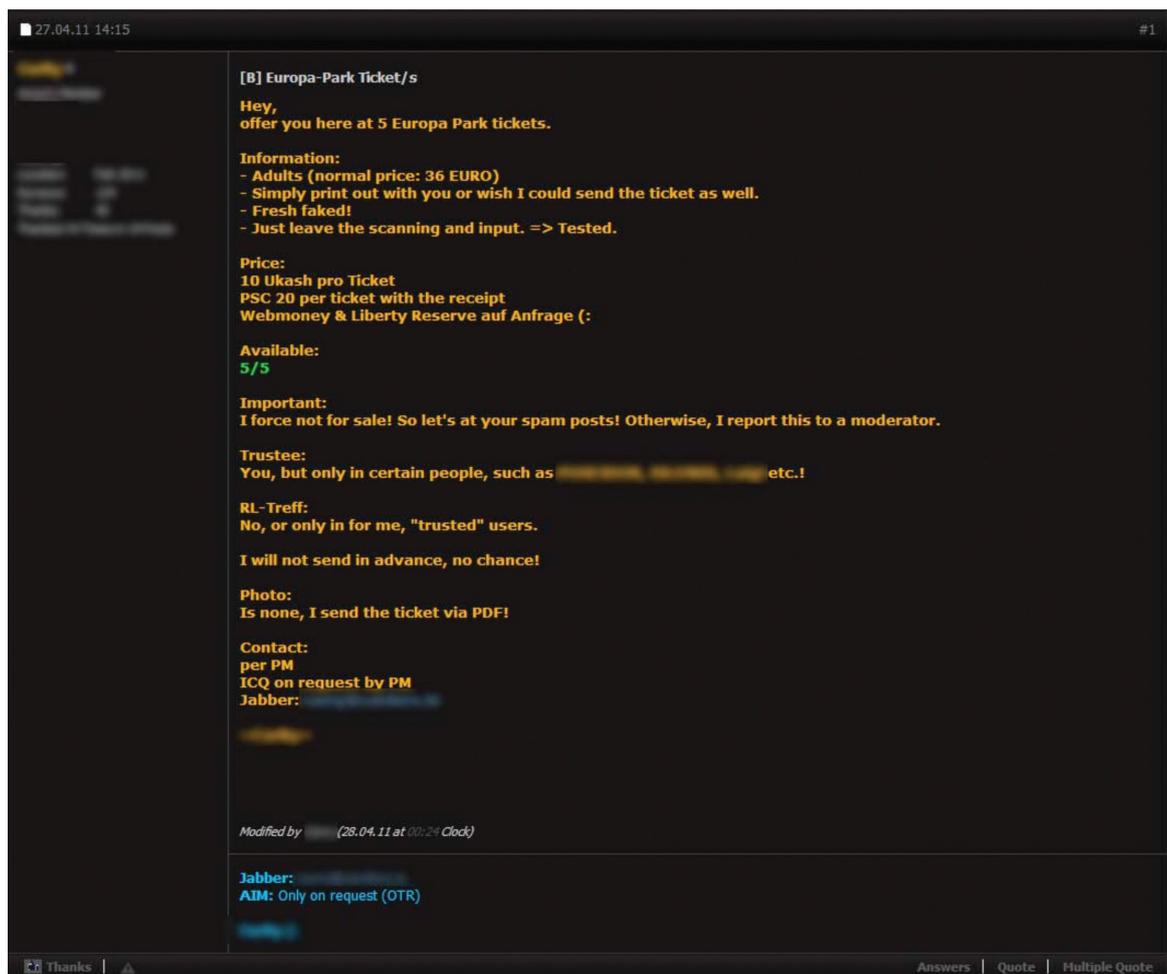
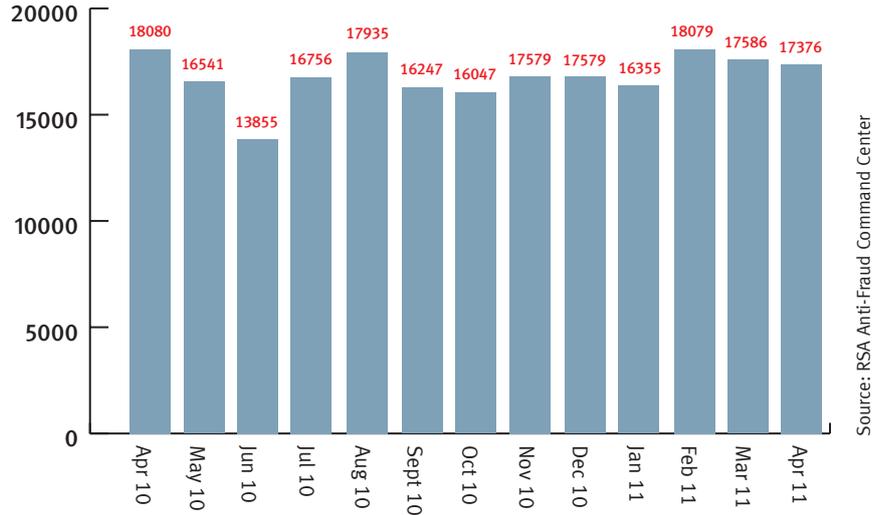


Figure 3: Another way to cash out stolen credit cards is to purchase amusement park tickets and resell them in the underground.

**Phishing Attacks per Month**

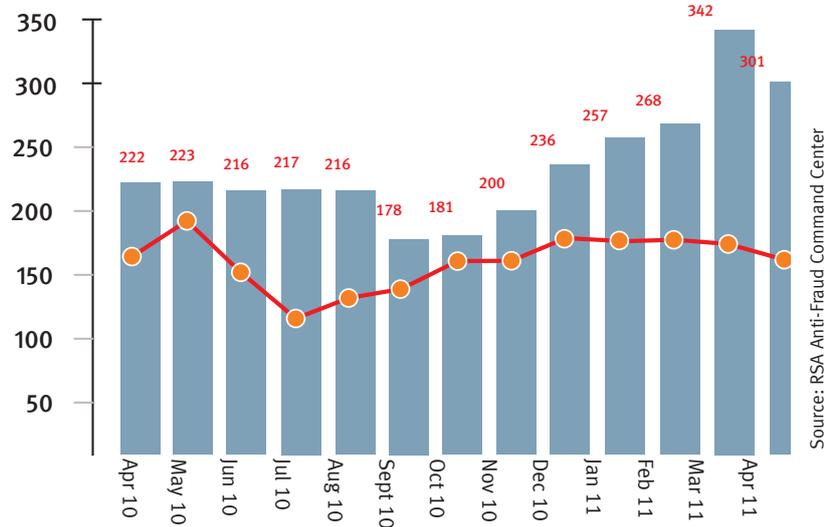
Worldwide phishing attacks remained virtually unchanged in April. A total of 17,376 attacks were identified by RSA, a decrease of barely one percent in. Still, despite the nearly identical number of attacks, the number of brands attacked dropped by 12 percent, signifying that virtually the same number of attacks targeted a narrower roster of brands (see Number of Brands Attacked chart).



Source: RSA Anti-Fraud Command Center

**Number of Brands Attacked**

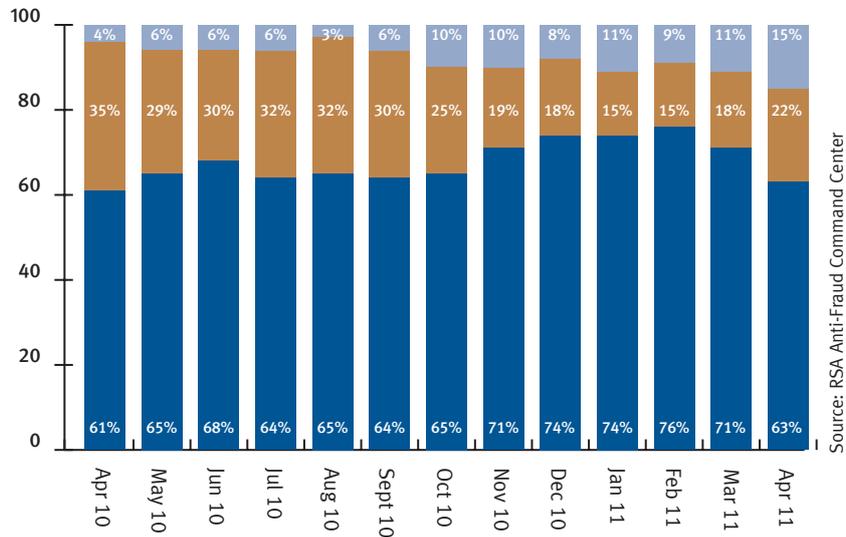
In April, we witnessed a 12 percent decrease in the number of brands attacked, with 301 brands targeted by phishing attacks worldwide. Despite this drop, the number of brands targeted in April 2011 is almost 30 percent higher than the past year's average of 236 targeted brands per month. In addition, eight brands endured their first phishing attack in April.



Source: RSA Anti-Fraud Command Center

**Segmentation of Financial Institutions Attacked Within the U.S.**

In the U.S. financial services segment, the number of attacks endured by credit unions and regional banks increased by four percent in April. Nationwide banks endured 63 percent of the attacks in April – the first time since October 2010 that they have accounted for less than 70 percent of attacks.

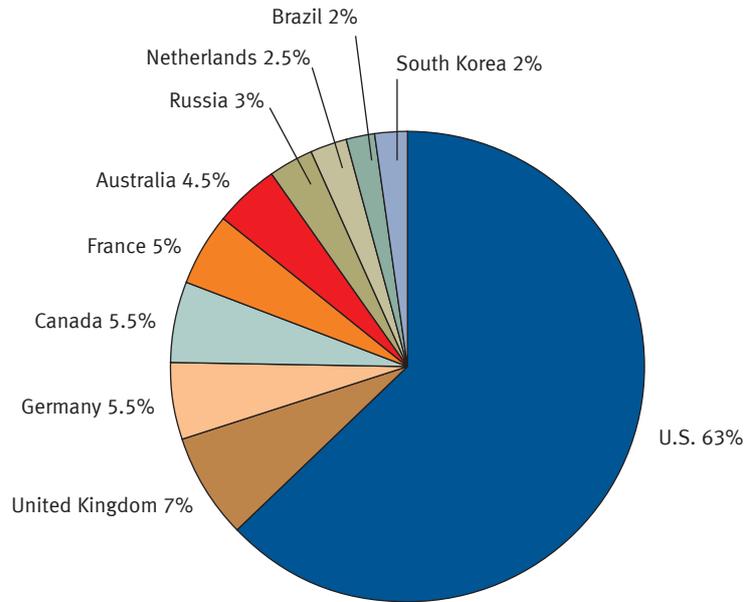


Source: RSA Anti-Fraud Command Center

**Top Ten Hosting Countries**

The U.S., UK, Germany and Canada hosted over 80 percent of all phishing attacks in April. Since March 2010, the countries that have consistently hosted the highest portions of phishing attacks have been the US, UK, Canada, Germany, France, Russia, and South Korea.

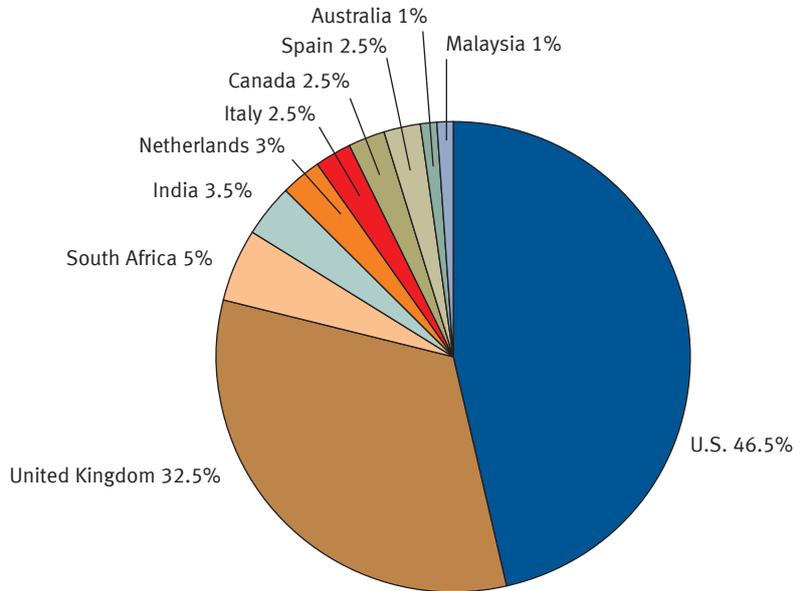
Source: RSA Anti-Fraud Command Center



**Top Ten Countries by Attack Volume**

The U.S., UK, and South Africa continue to be the countries that have endured the highest volume of phishing attacks – for 15 consecutive months. Over the past year, the U.S. and UK have absorbed a combined average portion of 65 percent of the attacks. (May 2010 - April 2011).

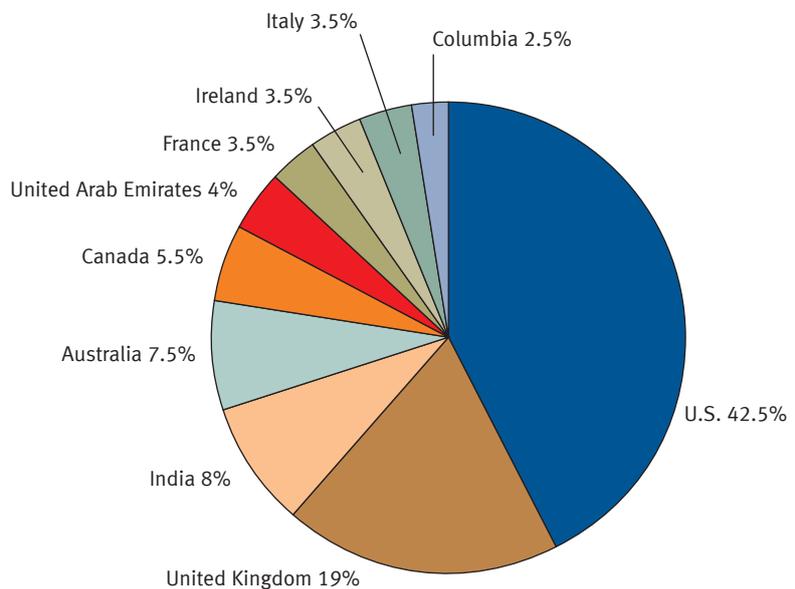
Source: RSA Anti-Fraud Command Center



**Top Ten Countries by Attacked Brands**

The U.S., UK, and India accounted for seventy percent of the brands targeted by phishing in April. Brazil and China fell off and were replaced by Ireland and Colombia in terms of the countries with the most targeted brands.

Source: RSA Anti-Fraud Command Center



## CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at [www.RSA.com](http://www.RSA.com)

[www.rsa.com](http://www.rsa.com)

©2011 EMC Corporation. EMC, RSA, the RSA logo, and FraudAction are trademarks or registered trademarks of EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned are the property of their respective holders. MAY RPT 0511

