

RSA Online Fraud Report

December, 2010

Single Phishing Attacks Target Multiple Entities

Phishing attacks are one of the oldest tools in the cybercriminal's arsenal. The fact that they are low-cost and easy to launch has contributed to their longevity – and also their continued evolution. One of the latest types of phishing attacks to emerge is one that simultaneously targets the brands of multiple organizations through a single attack.

This type of phishing attack is fast becoming popular among cybercriminals and uses many different social engineering schemes. It has most often been distributed under the guise of important notices from tax collection agencies of various countries including the U.S., UK, Australia, South Africa, and India. The attack presents victims with a list of bank logos, prompting them to click on their bank's logo in order to log into their account and claim a tax refund. But instead of logging in to their account, users actually log in to a phishing site where their online banking credentials are captured.

A similar phishing scam that RSA has increasingly witnessed exploits popular consumer brands. Potential victims are sent a phishing email that is disguised as a customer satisfaction survey where they are asked to rate their recent experiences with the brand (typically a restaurant or retail store). The phishing attack promises responders a monetary reward for their participation in the survey. After taking the survey, users are prompted to enter their online banking credentials in order to have their reward credited to their account. The two screenshots on the following page show this attack being perpetrated against Coca-Cola and a popular retailer.

The threat of phishing seems almost insignificant these days with all the talk of malware and Trojans. However, just because it is an old scam that consumers are able to spot more easily (thus, making it less effective in some cases), it does not mean that it is still not a top tool of choice among cybercriminals. They continue to develop the functionality within phishing kits and use various social engineering methods to get online users to fall victim to their scams. And with the number of phishing attacks RSA witnesses each month, it is still working.



France
France
USA

Coca-Cola's Customer Satisfaction Survey - Windows Internet Explorer
File Edit View Favorites Tools Help
File Edit View Favorites Tools Help
Coca-Cola's Customer Satisfaction Survey

Coca-Cola
Coca-Cola's Customer Satisfaction Survey

thank you for taking the time to complete this survey. In return, we will credit £150.00 to your account - just for helping us improve our services.

• Credit Card
• Bank Account
• American Express
• Direct Deposit
• Cash
• Other
• None

Please select your personal bank account in order to continue

© 2008 The Coca-Cola Company. All rights reserved. Coca-Cola®, "Open Happiness" and the Contour Bottles are registered trademarks of The Coca-Cola Company.

Done Internet 100%

Customer Satisfaction Survey - Windows Internet Explorer
File Edit View Favorites Tools Help
File Edit View Favorites Tools Help
Customer Satisfaction Survey

Home About Us Facts & News Health & Wellness Careers Community & Giving Diversity Sustainability Investors Suppliers

Home > Customer Satisfaction Survey

Customer Satisfaction Survey

Thank you for taking the time to respond to this survey.
In return, we will credit \$150 to your account - just for your time.

—Please enter your account to credit your \$150 reward—

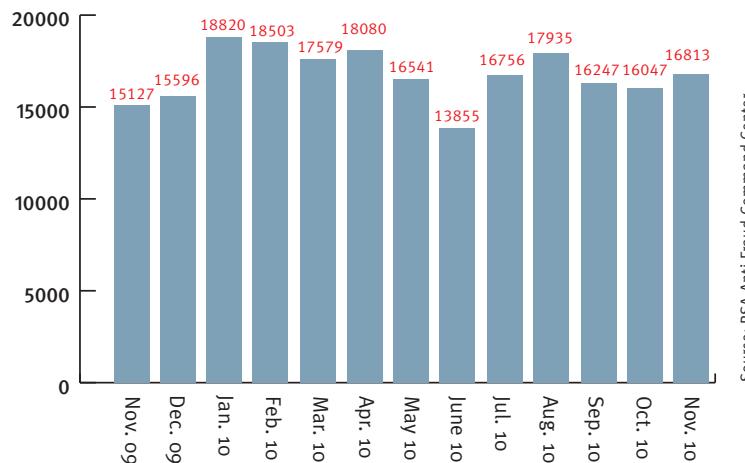
*FirstName:
*LastName:
*Street Address:
*City:
*State:
*Zip Code:
*Card Number:
*Card Expiration Date: Month Year
*Card Security Code: The last 3 digits on the back of your card

©2008 The Coca-Cola Company. All rights reserved. Coca-Cola® and "Open Happiness" are registered trademarks of The Coca-Cola Company.

Done Internet 100%

Phishing Attacks per Month

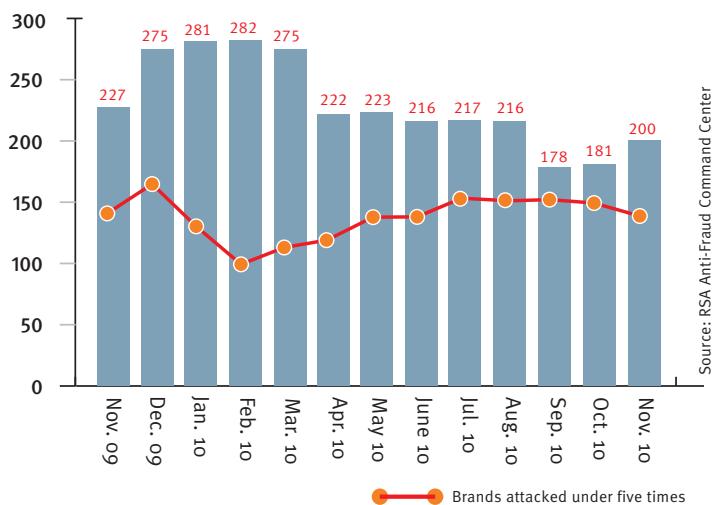
In November, RSA identified 16,813 worldwide phishing attacks – a five percent increase from the total reported in October.



Source: RSA Anti-Fraud Command Center

Number of Brands Attacked

The total number of brands attacked in November increased by ten percent. The number of entities that endured their first attack was five, continuing a downward trend observed over the past several months, as compared to the average figure of 20-25 newly targeted brands.



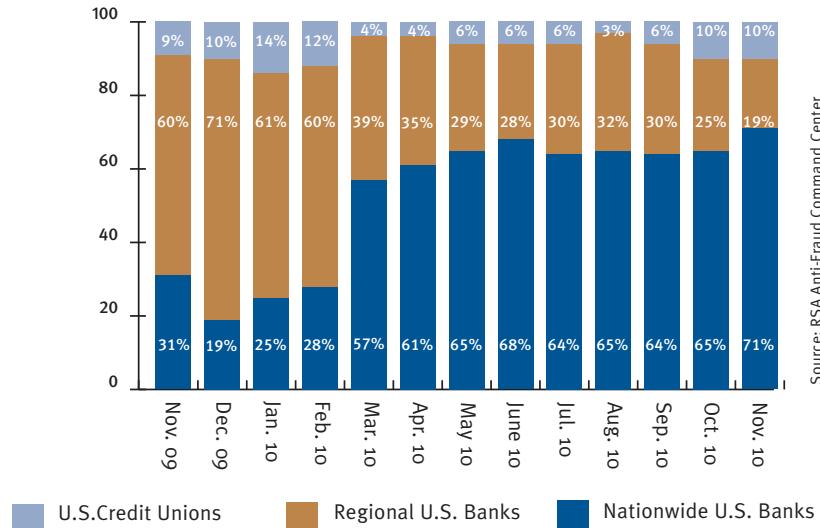
Source: RSA Anti-Fraud Command Center



Segmentation of Financial Institutions Attacked Within the U.S.

The portion of attacks recorded for U.S. credit unions held steady in November at 10 percent. Meanwhile, the portion of targeted U.S. brands by nationwide banks climbed six percent while that of regional banks decreased by the same proportion.

The data for attacks recorded within the U.S. financial services sector by RSA in just the past year has done a complete shift. In December 2009, regional banks were the target of about seven out of every ten attacks while today, that same percentage of attacks is targeted at nationwide banks.

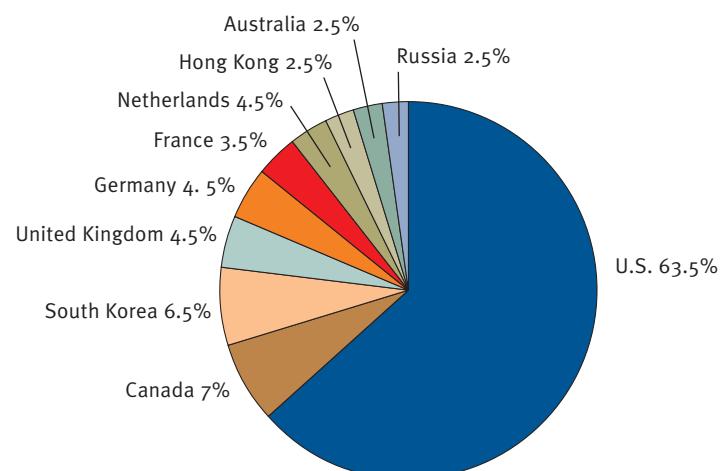


Source: RSA Anti-Fraud Command Center

Top Ten Hosting Countries

The U.S. continues to be the top hosting country for phishing attacks, recording a six percent increase over the number hosted in the U.S. in October. There was a five percent decrease in the portion of attacks hosted in Canada. All other hosting countries remained virtually the same in November with the exception of Hong Kong which replaced Hungary as a top hosting country.

Source: RSA Anti-Fraud Command Center

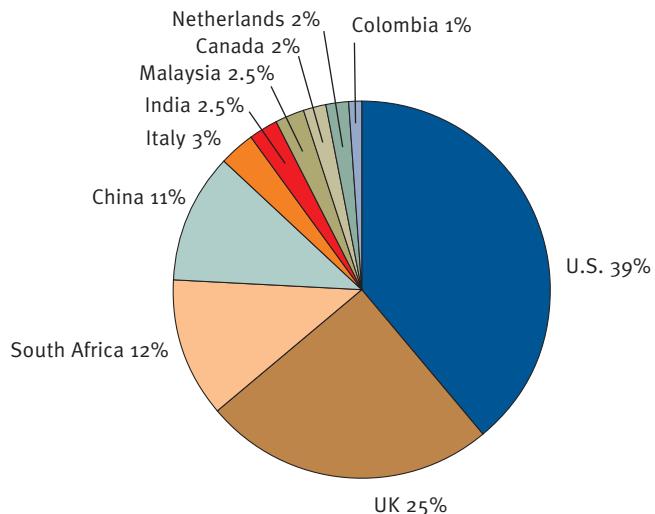


Online Attack Volume

Top Ten Countries by Attack Volume

The five countries whose brands suffered the highest volumes of phishing attacks – the U.S., UK, South Africa, China and Italy – have all retained their positions on the chart in November, with fluctuation of no more than four percent each. As compared with October, the share of attack volume in the U.S. and China increased two and four percent respectively while the UK decreased by two percent.

Source: RSA Anti-Fraud Command Center

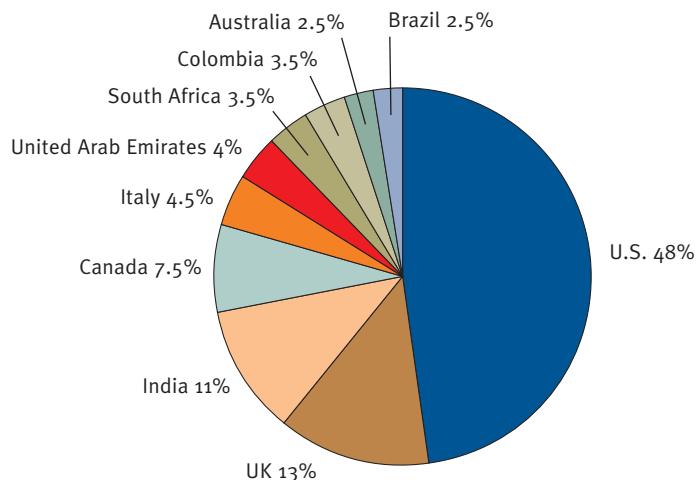


Top Ten Countries by Attacked Brands

The most prominent change in November was the reappearance of Colombia and Brazil on the list of countries with the most attacked brands after a respective seven and five month absence. The four countries that had the highest number of attacked brands in November – the U.S., UK, India, and Canada – retained their relative positions from October, with the UK's portion showing the most significant change with a six percent decrease.

Within the past six months, the countries that have consistently ranked as having the highest number of targeted brands have been the U.S., UK, Italy, Canada, India, Australia and South Africa.

Source: RSA Anti-Fraud Command Center





The Security Division of EMC

www.rsa.com

The information set forth in this RSA Online Fraud Report is based on sources and analysis that RSA Security Inc. ("RSA") believes are reliable. Statements concerning financial, regulatory or legal matters should be understood to be general observations of the RSA professionals and may not be relied upon as financial, regulatory or legal advice, which RSA is not authorized to provide. All such matters should be reviewed with appropriate qualified advisors in these areas. RSA reserves the right to notify law enforcement authorities and/or other relevant agencies regarding the information RSA uncovers in the course of doing business.

Usage Guidelines

Individuals and organizations may reference content from any RSA Online Fraud Report by following these guidelines:

- (1) Reprinting and/or distributing an entire RSA Online Fraud Report requires prior approval from RSA in all cases. This includes an entire Monthly Highlight and/or the full set of Statistics and Analysis from RSA's phishing repositories. Any requests to reprint and/or distribute an RSA Online Fraud Report must be directed to Heidi Bleau at heidi.bleau@rsa.com.
- (2) It is permissible to reference up to three sentences from the Monthly Highlight. They must be cited in their entirety and within quotation marks. Any requests to cite more than three sentences must be directed to RSA.
- (3) It is permissible to reference up to three sets of Statistics and Analysis from RSA's phishing repositories. Any requests to cite more than three sets may be directed to RSA. Charts may not be redrawn. All citations from related data analysis must appear in full sentences and within quotation marks.
- (4) It is required that all references to the RSA Online Fraud Report are credited in the following manner: "Source: RSA Anti-Fraud Command Center, RSA Online Fraud Report, [month], [year]".

EMC, RSA, RSA Security, FraudAction™ and the RSA logo are registered trademarks or trademarks of EMC Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the properties of their respective owners.