

RSA Online Fraud Report

February/March 2009

A Monthly Intelligence Report from the RSA® Anti-Fraud Command Center

Online crime is constantly evolving, and fraudsters do not discriminate against any entity or person. Online attacks involving phishing, pharming and Trojan attacks represent one of the most sophisticated, organized and innovative technological crime waves worldwide. Fraudsters work day and night to steal identities, credentials or any other information that they can efficiently monetize. They target online businesses in all sectors, as well as any person who uses the Internet at work or at home for e-commerce, social networking, e-mail and more.

These online criminals also have new tools at their disposal and are able to adapt more quickly than ever with advanced crimeware; rapidly deployed using stealth mechanisms. Their supply chains have evolved to match that of the legitimate business world, including the ability to provide what RSA coined "Fraud-as-a-Service".

This monthly intelligence report has been created by the experienced team of fraud analysts from the RSA Anti-Fraud Command Center. It includes a monthly highlight based on keen insight into the world of online fraud as well as statistics and related analysis from RSA's phishing repositories.

About the RSA Anti-Fraud Command Center

The RSA Anti-Fraud Command Center is a 24x7 war room that is designed to detect, monitor, track and shut down phishing, pharming and Trojan attacks spread across more than 140 countries. Protecting more than 300 institutions against online attacks, the RSA Anti-Fraud Command Center has shut down more than 139,000 phishing attacks to date and is a key industry source for intelligence on new and emerging online threats.

The RSA Anti-Fraud Command Center is staffed by an experienced team of fraud analysts who shut down fraudulent websites, deploy countermeasures, and conduct extensive forensic analysis to stop online criminals and prevent future attacks – reducing the average lifetime of an online attack from approximately 115 hours to five hours.

The RSA Anti-Fraud Command Center has established direct, open channels with dozens of Internet Service Providers around the world, as well as several CERTs and law enforcement agencies. It also provides multi-lingual translation support in nearly 200 languages to further enhance its ability to detect, block and shut down fraudulent websites on a global scale.



Uri Rivner, Head of New Technologies,
at the RSA Anti-Fraud Command Center



The Security Division of EMC

Fraudsters Exploit eCommerce Website to Verify if Stolen Credit Cards are Valid

In February 2009, the RSA Anti-Fraud Command Center traced a new tool designed by online fraudsters that can validate compromised payment cards (e.g. credit cards or debit cards) that are illegally obtained through the underground fraud supply chain. Fraudsters typically test the viability of illegally obtained payment cards before they are used to make fraudulent purchases through a variety of “credit card checkers,” also known as “card checkers” or “cc checkers”. Card checkers are services or tools designed by fraudsters that enable other fraudsters to check the accuracy of compromised payment card data.

RSA found the source code of a desktop application on an online merchant’s website that functions as a payment card checker that can be employed on a mass scale – creating what are called “mass card checkers”. This desktop application can check payment cards by manipulating and attacking a legitimate online merchant’s Address Verification System (AVS) check. An AVS check is a standard system that verifies whether or not a billing address entered online matches the billing address registered to a payment card. In addition, the AVS check returns a result without the need to complete a financial transaction.

Mass card checkers are shared within the fraudster underground for free and can grab the username and password within a legitimate member’s account on an online merchant’s web site. Card checkers are not a novel approach to validate stolen payment cards, but the mass card checker discovered by RSA is new in that it consists of a desktop application solely dedicated to the abuse of an online merchant’s AVS check.

How Card Checkers Work

Fraudsters most commonly check the validity of compromised payment cards in one of two ways: either through fraudster-designed automated online services that utilize card checkers, or through legitimate online merchants.

To use a card checker, fraudsters visit certain legitimate websites and validate compromised payment card data either by paying a small fee per card (approximately USD \$0.30) or by purchasing “in-store credit”. After acquiring enough in-store credit and storing it in the account, fraudsters can validate stolen data on as many payment cards as they choose. The significance is that card checkers can perform validation checks by compromising a legitimate online merchant by connecting and issuing authorization requests to the merchant’s payment gateway. RSA was also able to trace phone numbers of legitimate online merchant customer services departments that fraudsters were using to verify the validity of a payment card.

When exploiting legitimate online merchant websites, fraudsters can manually check compromised payment card data by making low-sum purchases at amounts varying between USD\$.03 – \$1.00. Alternatively, they can donate similar amounts of money on legitimate charitable websites. When these small purchases and donations are successfully processed, the stolen payment card is considered valid.

The significance of the RSA discovery is that the free mass card checker desktop application requires no purchase or donation whatsoever, and no payment is required in return for the card verification service. Instead, the mass card checker directly exploits an online merchant’s AVS check and enables many compromised payment cards to be checked simultaneously. Fraudsters who have bought compromised payment card data by the batch or possess their own stolen data (e.g., obtained via a phishing attack) could potentially find mass card-checking capabilities to be a more effective means to conduct identity theft and obtain stolen goods.



ID	Status	Name, Number, CVV, Month, Year	Line
1	Die	Die / [REDACTED]	CC Live

The Mass Card Checker Interface

How the Mass Card Checker Application Works

The mass card checker performs the following steps in order to verify the validity of compromised cards:

1. It accesses a specific URL on the online merchant's website, with the username and password of a member account specified within the application's source code.
2. As the online merchant's website functionality enables legitimate users to change their billing information, fraudsters can check the information of an unlimited number of cards by simultaneously submitting their details to the mass card checker application. Payment card information that can be validated includes the cardholder's name, card number, card security code (e.g. CVV2), and expiration date. The valid billing address associated with the illegally obtained payment cards remains unchanged throughout the checking procedure. This is key to the mass card checker operation which relies on an AVS mismatch.
3. The online merchant tests the payment cards for validity and performs an AVS check. As the billing information is declined in the case of an AVS mismatch (which does not cost anything) the card checker responds with one of the two following error messages:

"The billing information you entered does not match that which is on record with your bank."

This indicates that the card is valid and can be used for illegal transactions, regardless of the fact that the billing address of the card did not match its other details.

"Sorry, we were unable to receive an authorization from your bank. Please direct any questions to your financial institution or try using a different payment method."

This error message indicates that the payment card information is not valid.

RSA notified the online merchant website where the mass card checker application was discovered. The merchant was fully briefed on the situation and was made aware of the member account used by the mass card checker application. The merchant blacklisted the member account.

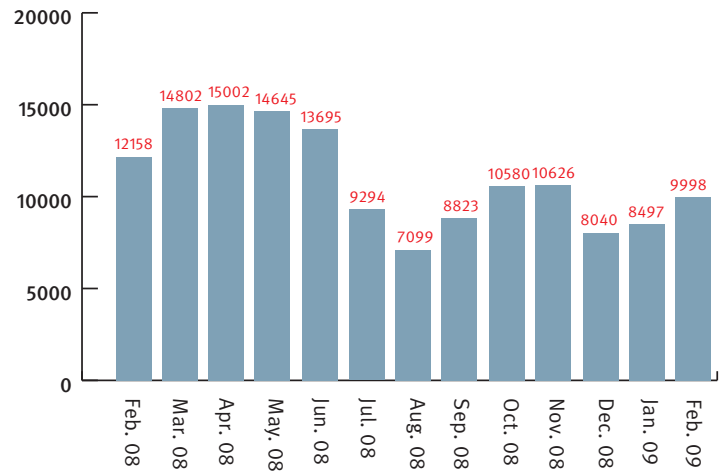
In light of this newly-traced exploitation, merchants may want to consider better securing their website's billing functionality (using CAPTCHA, for example) to prevent it from being abused by an automated mass card checking application.

Source: RSA Anti-Fraud Command Center

Total Number of Phishing Attacks

Trend Analysis for February, 2009

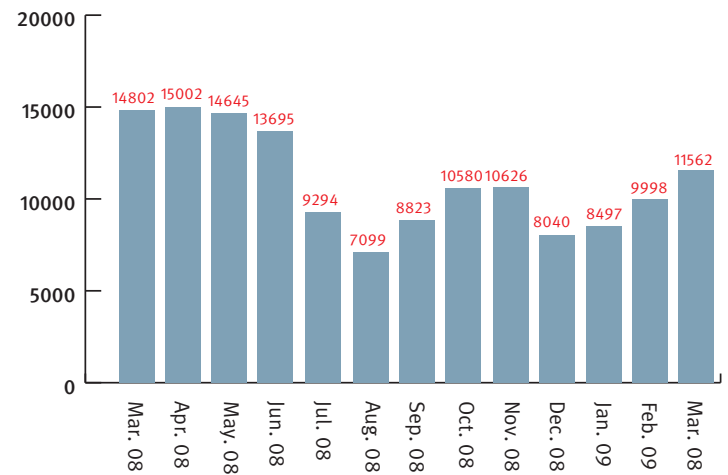
The total number of phishing attacks detected by the RSA Anti-Fraud Command Center in February 2009 rose by 18 percent when compared to January 2009 – representing an increase of 1,500 attacks. The sole cause of this increase in phishing attacks was a sharp surge of attacks initiated by the Rock Phish Gang and others generated by fast flux networks. In fact, while standard attacks actually diminished throughout February, fast flux-based attacks climbed by nearly 80%. When compared to the spring of 2008, the total number of attacks remains significantly lower but fewer attacks upon organizations are not necessarily indicative of a reduction of an overall impact.



Source: RSA Anti-Fraud Command Center

Trend Analysis for March, 2009

Continuing the upward trend from February 2009, the number of phishing attacks detected in March 2009 rose by just over 15 percent, or slightly more than 1,500 attacks. This represents the highest number of phishing attacks since June 2008. The rise in attacks in February 2009 was mainly due to an increase of nearly 20 percent in the number of “standard” phishing attacks. The number of Rock Phish and other fast-flux phishing attacks rose only slightly in March 2009. However, these attacks comprised almost 45 percent of the total attacks.



Source: RSA Anti-Fraud Command Center

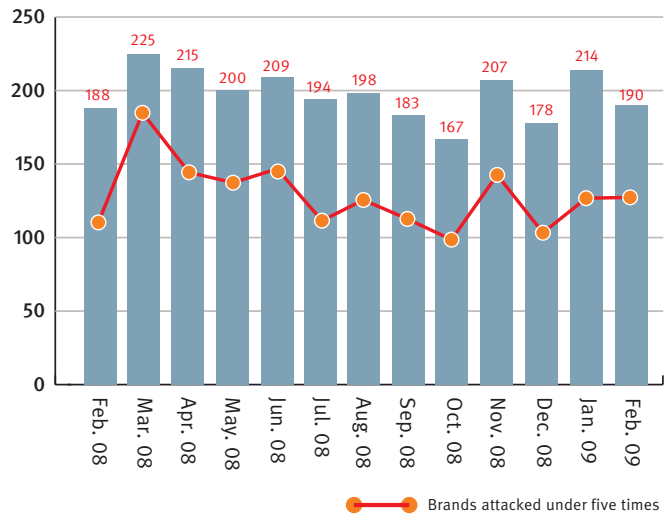


Total Number of Brands Attacked

Trend Analysis for February, 2009

The number of brands suffering phishing attacks during February 2009 decreased by ten percent when compared to January 2009. Out of the 190 brands attacked during February 2009, 14 brands suffered their first attack.

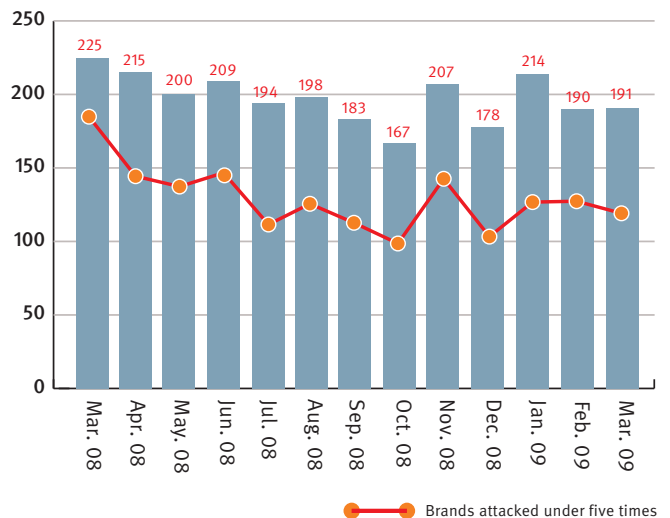
125 brands, accounting for just over 65 percent of the total amount attacked, suffered less than five attacks over the course of February. This is a consistent trend, typically comprising 60-65 percent of the total number of brands attacked in any given month. Fraudsters prefer targeting a very small number of financial institutions, which can be more lucrative or vulnerable targets, rather than spreading their attacks more broadly.



Source: RSA Anti-Fraud Command Center

Trend Analysis for March, 2009

The number of brands that suffered phishing attacks during March 2009 was almost identical to those targeted in February 2009. Out of the 191 brands attacked in March, eleven brands suffered their first attack. In addition, 112 brands, or almost 60 percent, suffered less than five attacks over the course of March 2009, consistent with the trend outlined in the February 2009 analysis.



Source: RSA Anti-Fraud Command Center

Top Ten Countries Hosting Phishing Attacks

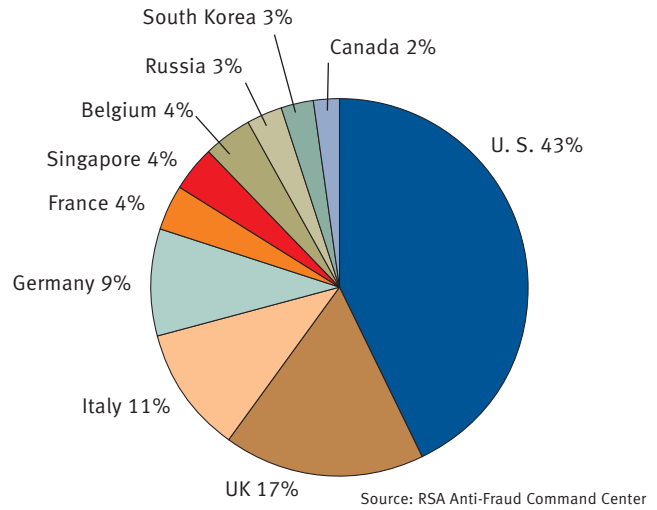
Trend Analysis for February, 2009

It was a dramatic month in certain parts of the world where some countries significantly shifted their volumes of hosted phishing attacks (as enumerated by the location of the ISP or the hosting company).

During February, the United States hosted 43 percent of the world's phishing attacks and this represents that country's second lowest amount since September 2007 when it hosted 39 percent of the total. By comparison, the United States hosted 60 percent of the world's attacks in August 2008.

Also very notable this month, the United Kingdom rocketed to second place by hosting 17 percent of the world's attacks during February 2009. This represents a significant 13 percent increase over January 2009, when that country placed seventh place on the list.

Italy shot up the list this month, climbing quickly from tenth place in January 2009 with three percent of the total, to third place in February 2009 with 11 percent of the total. Canada fell significantly from second place to tenth place in February 2009 by hosting only two percent of the attacks, down by nine percent over January 2009.



Singapore appeared on the list this month at sixth place (four percent) due to the fact of the large number of domains registered in that country for fast-flux attacks. Australia fell off the list completely after placing eighth in January with three percent. France, South Korea, Russia, and Belgium changed by no more or less than three percent when compared to January 2009 – the only exception was Germany which increased by four percent, but still maintained its fourth place on the list.

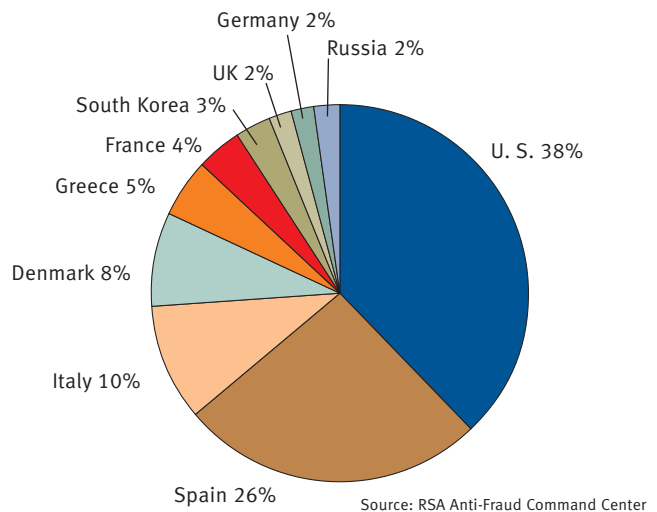
Trend Analysis for March, 2009

In March 2009, the United States hosted 38 percent of the total phishing attacks – an all time low (as enumerated by the location of the ISP or the hosting company).

Spain did not appear on the top ten list at all in February 2009, but appeared massively strong in second place in March 2009 by hosting 26 percent of the phishing attacks. This represents the highest figure of any country in second place to date.

Denmark, Greece and Spain were significant newcomers to the top half of the list as a result of numerous phishing domains registered in each of those countries by the Rock Phish gang.

The countries that have consistently hosted the most phishing attacks over the past year are the United States, United Kingdom, Germany, France, Russia, and South Korea.



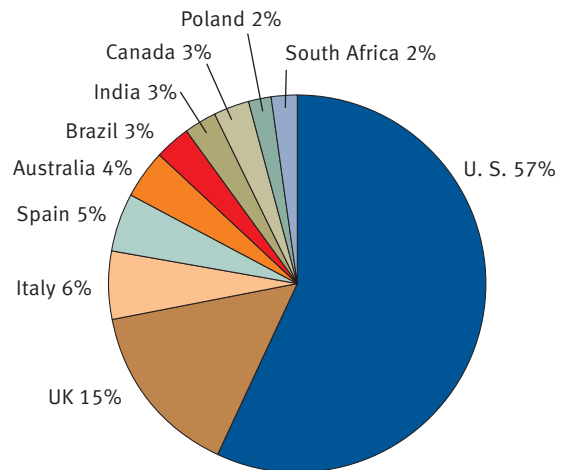


Top Ten Countries by Attacked Brands

Trend Analysis for February, 2009

In February 2009, the United States, United Kingdom, Italy and Spain all maintained the same positions on this list as they did in January 2009 by accounting for the highest number of attacked brands, and their percentages of the total did not change by more or less than four percent. Brazilian brands entered the top ten this month at sixth place with three percent of the total, resurfacing after their last appearance in July 2008. German brands fell off the list this month after placing tenth in January.

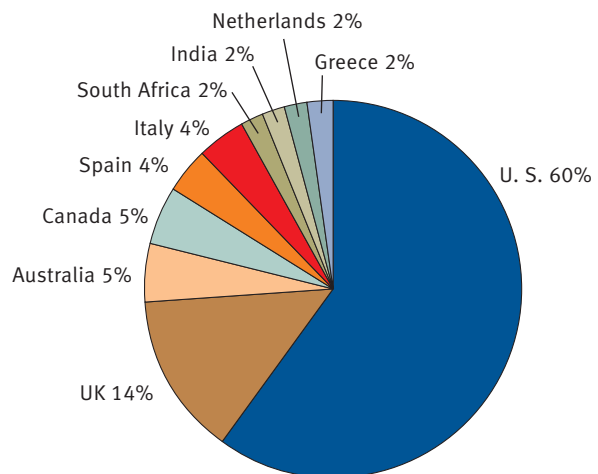
While certain Australian, Brazilian, Indian and Polish brands were heavily attacked during February, the overall number of attacks in these countries remains rather low.



Source: RSA Anti-Fraud Command Center

Trend Analysis for March, 2009

In March 2009, brands in the United States and United Kingdom suffered the greatest number of attacks, with the combined total comprising almost three-quarters of the month's total. Brazil and Poland fell off the list in March while the Netherlands and Greece entered the list in ninth and tenth place, respectively.

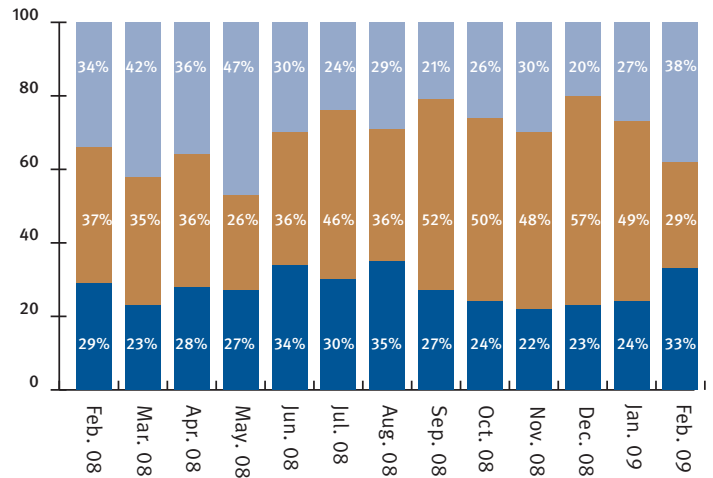


Source: RSA Anti-Fraud Command Center

Segmentation of Financial Institutions Attacked Within the U.S.

Trend Analysis for February, 2009

In February 2009, credit unions accounted for 38 percent of the targeted brands, up from 27 percent from January 2009. This is the first time that credit unions were the most targeted since May 2008 when nationwide banks were the most attacked brand. Regional banks fell to second place and accounted for only 29 percent of the total of targeted brands. This was a major drop from January 2009 where they accounted for 49 percent of the total. Nationwide banks accounted for 33 percent of the targeted brands in February 2009, down from 24 percent in January 2009.



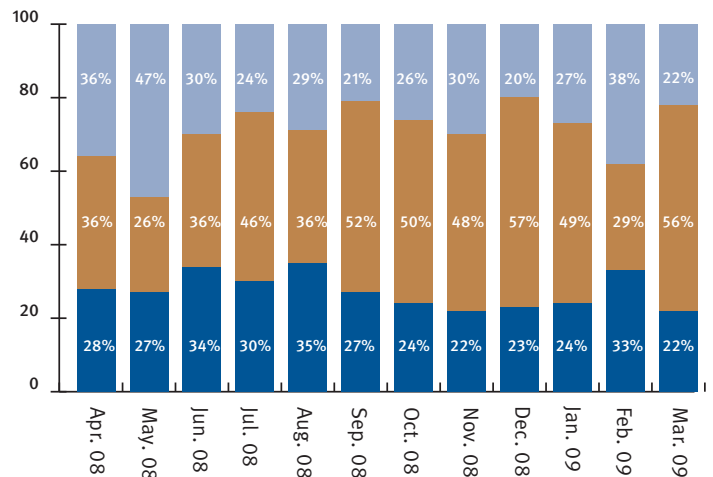
Source: RSA Anti-Fraud Command Center

■ Nationwide U.S. Banks
 ■ Regional U.S. Banks
 ■ U.S. Credit Unions

Trend Analysis for March, 2009

In March 2009 the rate of attacks against credit unions (when compared to nationwide and regional banks) was 22 percent of the total. This is a significant decrease from February 2009 where the figure was 38 percent and this segment landed in a rare first place as the most attacked brand.

Regional banks took back their lead as the most attacked brand with 56 percent of the total, a significant increase from 29 percent of the total in February. This segment had been the most attacked brand for eight months in a row before a one month respite in February where credit unions become the most targeted. The rate of attacks against nationwide banks was 22 percent, down from 33 percent in February.



Source: RSA Anti-Fraud Command Center

■ Nationwide U.S. Banks
 ■ Regional U.S. Banks
 ■ U.S. Credit Unions



New

Distribution of Attacks by Hosting Method

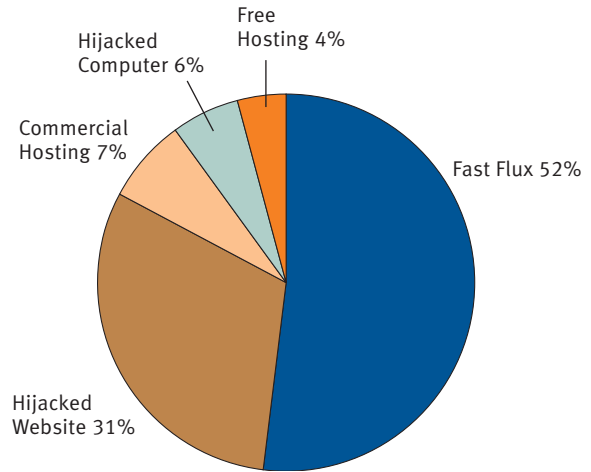
Trend Analysis for March, 2009

During March 2009, the most widely used hosting method used to launch phishing attacks were those based upon fast-flux networks, with 52 percent of the total. Within fast-flux networks, instead of just one IP address, multiple and periodically changing IP addresses are assigned to each domain of each fraudulent website.

In second place at 31 percent were phishing attacks based upon hijacked websites. Hijacked websites are those where fraudsters host their illegal content on legitimate websites' sub-domains, avoiding the registration of their own domains used for phishing attacks.

Dwindling down to the single digits, commercial hosting placed third at seven percent. Commercial hosting involves fraudsters who host their malicious websites for others in exchange for a fee.

Hijacked computers were close behind at six percent. Hijacked computers consist of compromised computers whose IP addresses were assigned to a specific phishing



Source: RSA Anti-Fraud Command Center

domain.

Attacks launched from websites that provide free hosting services accounted for the smallest portion of attacks at four percent.

New

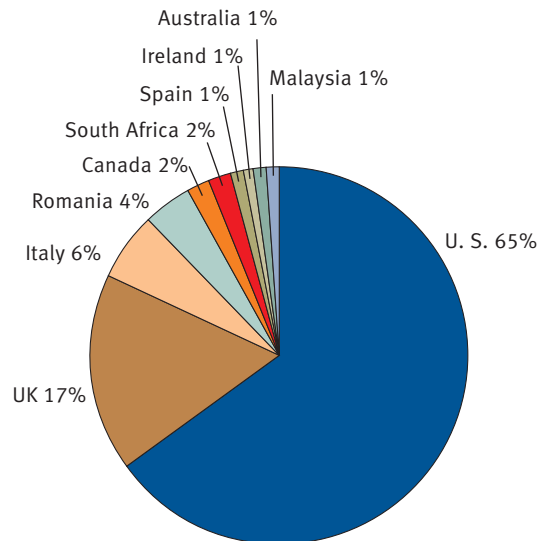
Top Ten Countries by Attack Volume

Trend Analysis for March, 2009

In March 2009, out of the top ten countries by attack volume, the United States placed first, United Kingdom placed second, and Italy placed third. These are the same order of rankings since December 2008. In addition, these three countries have been in the top three on this list for over 12 months.

In March 2009 the United States was the most attacked country at 65 percent. Although the United Kingdom placed a distant second at 17 percent it is the only other country on the list with attack rates in the double digits.

Over the past year, the six countries that have regularly suffered the most attacks have been the United States, United Kingdom, Italy, Canada, Spain and South Africa.



Source: RSA Anti-Fraud Command Center