RSA Online Fraud Report

January, 2010

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

Online crime is constantly evolving and fraudsters do not discriminate against any organization or person. Online attacks involving phishing, pharming and Trojans represent one of the most organized and sophisticated technological crime waves worldwide. Online criminals work day and night to steal identities, online credentials, credit card information, or any other information that they can efficiently monetize. They target organizations in all sectors, as well as any person who uses the Internet at work or at home.

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.

RSA®
The Security Division of EMC

About the RSA Anti-Fraud Command Center

The RSA® Anti-Fraud Command Center is a 24x7 war room that helps organizations detect, block, monitor, track and shut down phishing, pharming and Trojan attacks across more than 140 countries. Protecting more than 300 organizations against online attacks, the RSA Anti-Fraud Command Center has shut down more than 260,000 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 more than 100 experienced fraud analysts and has established direct, open channels with dozens of Internet Service Providers around the world, as well as numerous CERTs and law enforcement agencies. Multi-lingual translation support is available in nearly 200 languages to further enhance its ability to detect, block and shut down fraudulent websites and significantly reduce the average uptime of online attacks around the globe.

The RSA Anti-Fraud Command Center is staffed by over 100 experienced fraud analysts.

Consumer Concern Extends Beyond Online Banking; More Security Wanted and Expected

In the RSA 2010 Global Online Consumer Security Survey, we asked over 4,500 adults from 22 countries to share their opinions and attitudes on the online security risks they face, their level of awareness concerning the latest threats, and what online service providers should do to protect them.

Respondents were represented from all regions of the world including North America, Europe, Asia, Australia, and Central and South America and considered active online users. Among those surveyed, the vast majority regularly visit and interact with online sites such as online banking, and government and healthcare portals, and social networking sites, with 92 percent conducting an online banking transaction and 80 percent making an online purchase in the last month.

This month's highlight will focus on some of the major findings from the survey and provide in-depth analysis of what those findings mean to the state of online security in 2010.

Consumers more aware of threats, but remain concerned

Consumers have expressed an increased awareness in many types of threats they face online each day. Banks and social networking sites, perhaps the two types of sites most targeted by online criminals, have been very proactive in providing ongoing user education. In addition, online fraud and cyber crime is of great interest to the media and has become a highly popular topic to report on in the news. The increase in consumer awareness can be attributed, at least partly, to the ongoing education offered by service providers and the media.

This is evident in the vast increase in consumer awareness among many popular online threats. For example, in 2007, only 38% of respondents to our survey expressed they were aware of the threat of phishing and what it meant. In 2009, that figure has literally doubled, with 76% of respondents expressing they are familiar with phishing.

While awareness of phishing has increased, concern over the threat also remains high. Among those surveyed, 89 percent stated that they were somewhat to very concerned about the threat of phishing. Some regions, however, demonstrated a higher level of concern for phishing than others. For example, 61 percent of respondents from Asia and 59 percent of respondents from Central and South America stated they were "very concerned" about the threat of phishing. These figures are much higher compared to other geographies, where only 37 percent of respondents in the United States and Canada and 29 percent of respondents in Europe express they were "very concerned" about phishing.

Table 1

Which of the following types of online threats are you familiar with? (Respondents were allowed to choose **multiple** responses.)

Response	Freq.
Phishing emails	76%
Phishing via SMS / text message ("SMiShing")	33%
Phishing over the phone ("Vishing")	26%
Trojans	81%
Keyloggers	26%
Malware	54%
Spyware	74%
Adware	52%
Botnets	14%
Viruses	88%
Worms	65%
Other	1%

Despite increased awareness, there have been a growing number of online users that have fallen victim to a phishing attack. In our 2007 survey, only 5 percent of respondents cited that they had been a victim of a phishing attack, whereas in 2009, 29 percent claimed they had fallen for a phishing scam.

The increase in phishing victims can likely be attributed to the advanced tactics that online criminals use today and the fact that phishing attacks have become more sophisticated and targeted. In addition, the sheer volume of phishing attacks being launched today is also contributing to these trends. The RSA Anti-Fraud Command Center reported a 17% increase in the number of phishing attacks identified in 2009 compared to the number identified in 2008.

An increase in consumer awareness is further evident from the growth in the number of respondents that expressed awareness of Trojans. In 2007, 63 percent of respondents stated that they knew what a Trojan was compared to the 81 percent of respondents that cited a knowledge of Trojans in 2009.

While awareness of phishing and Trojans has increased, there are still very low levels of awareness among consumers regarding newer threats such as vishing (voice phishing) and smishing (phishing via SMS messaging). This is particularly concerning to RSA as we have witnessed the incidence of vishing and smishing rising rapidly. For example, the number of vishing attacks addressed by our Anti-Fraud Command Center grew fourfold in the last twelve months. This increase, coupled with a lack of awareness among consumers concerning these types of threats, makes it likely that vishing and smishing will be an increasing cause for concern over the next year.

Consumer concern extends beyond online banking

Increased awareness also brings increased concern. Consumers have more threats to be concerned with, but have also brought more parts of their daily life to the Internet. Beyond online commerce and banking, there has been a dramatic increase in the way we communicate and network with others via social networking. Healthcare companies and local, state and federal government agencies are also bringing the power and convenience of online services to the market, allowing consumers the opportunity to view their health records, schedule appointments, renew their driver's license and pay tax bills over the Internet.

To address the changes in online behavior that have occurred within the last two years, RSA surveyed consumers about their level of concern regarding their personal information being accessed or stolen at the various online sites they visit and how those concerns impact their willingness to interact with these sites.

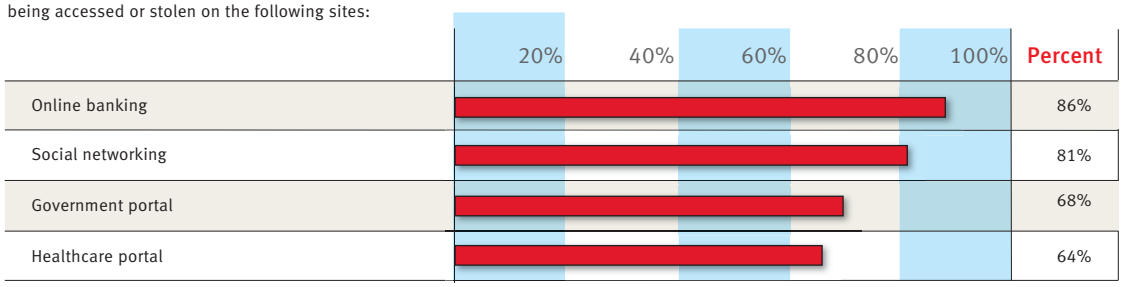
Overwhelmingly, consumers expressed they were somewhat to very concerned (86 percent) with their personal information being accessed or stolen at their online banking site compared to a healthcare (64 percent), government (68 percent) or social networking site (81 percent).

This finding is interesting for a number of reasons. First, many financial institutions that offer online banking are diligent about online security for their customers and have already implemented some form of strong two-factor authentication to protect customer accounts from unauthorized access. This is contrary to healthcare, government and social networking sites that, for the most part, still only require a simple username and password to gain access.

This finding also indicates that consumers are most protective and place the most value in their financial information. However, they are likely unaware of what an

Table 2

Are you concerned with your personal information being accessed or stolen on the following sites:



online criminal can do with a full personal information profile and what the value is to them compared to a single bank account or credit card number. For example, the requests for full personal information profiles in the fraud underground have become such a commodity that lookup services have evolved to meet the demand. Personal information has also been proven to boost the price a criminal will pay for stolen payment cards and bank account details.

Not surprisingly, consumer concerns about submitting their personal information to the online sites they interact with was similar to their concerns about their information being accessed or stolen at these same sites. Online banking (67 percent) and social networking sites (65 percent) drew the most concern from consumers with healthcare and government sites right behind them at 59 percent and 60 percent respectively.

Banking customers most concerned about online and mobile threats

Financial institutions interact with their customers across multiple touch points – online, over the telephone, on mobile devices, and at ATMs and branches. For the purposes of this survey, we asked consumers their attitudes towards security for all these different points of contact (excluding banking in the branch).

Online banking still garners the most concern among consumers. As demonstrated in the previous section, 86 percent of consumers stated they were somewhat to very concerned with their personal information being accessed or stolen at their online banking site. As a result, 80 percent of consumers also responded that they felt banks should implement a stronger form of security beyond a username and password when they log into online banking.

Consumers also responded that they expected their banks to conduct some level of transaction monitoring on their online banking accounts to detect unusual activity. Among those surveyed, 90 percent stated they expect their banks to monitor their Internet banking transactions. This figure was up slightly compared to 2007 where 82 percent of consumers declared they expected their banks to monitor their transactions.

This figure is important, especially in regions like Europe where two-factor authentication such as one-time password tokens, EMV-CAP, iTan and mTan are widely used in the consumer market, and as a result, are increasingly targeted by man-in-the-middle and man-in-the-browser attacks. Concerns over privacy are an ongoing issue in Europe, but when it comes to security, consumers are very willing to accept ongoing monitoring of the transactions they perform to ensure the protection of their financial accounts. Overall, the expectation of consumers to have their online banking transaction monitored did not vary significantly by region, despite the different perceptions of privacy and security typically seen in each of these regions.

Mobile banking presents its own set of concerns for consumers as well. Among those surveyed that use mobile banking, only 49 percent indicated they felt secure when using it, with only 11 percent responding very secure. Concerns over mobile banking can likely be attributed to the fact that it is still a new and growing user population and customers are not as aware of the threats posed by it.

Among mobile users, 84 percent stated that banks should implement a stronger form of security for mobile banking. The desire for stronger authentication for mobile banking did not vary much by region.

Consumers showed the greatest concern over the security of online and mobile banking compared to more traditional methods of interaction such as using telephone banking or ATM machines. Among those surveyed, 68 percent felt somewhat to very secure transacting with their bank using the telephone banking system. Likewise, 67 percent stated they felt somewhat to very secure using an ATM machine.

Online security inspires confidence

Online commerce is perhaps the oldest form of online "service." Yet, retailers still face the same barriers in trying to convert traditional brick-and-mortar shoppers to make purchases online. In one survey after another regarding the topic, security is most often cited as the primary reason some consumers are hesitant to shop online; they are afraid of submitting personal and financial information over the Internet.

Consumer confidence can be directly attributed to increased transactions. In order to gain that confidence, providers of an online website and portal – whether offered through a retailer, bank, or healthcare organization - must consider security a key driver to adoption. To demonstrate, one major UK bank that deployed strong authentication to their online users reported a 20 percent increase in the number of transactions performed online only one month after the system was launched.

RSA found that consumer confidence and the willingness to transact online was clearly correlated. When consumers were asked, in general, how stronger security would impact

Table 3

How secure do you feel when banking with your mobile phone?
(Respondents could only choose a **single** response.)

Response	20%	40%	60%	80%	100%	Freq.
Very secure						11%
Somewhat secure						38%
Neither secure nor insecure						22%
Somewhat insecure						20%
Very insecure						9%

their confidence in transacting online, 92 percent of consumers stated they would be more confident, with 53 percent stating they would be significantly more confident and 39 percent somewhat more confident.

Among each region surveyed, the impact of stronger security on confidence seemed to resonate most among respondents from Central and South America where 74 percent stated they would be "significantly" more confident. This is much higher compared to other regions; among respondents, 42 percent in the U.S., 50 percent in Australia, and 46 percent in Asia stated they would be "significantly" more confident.

When asked how stronger security features, offered in addition to a username and password, would impact their willingness to interact, purchase items, and submit personal information to the sites they regularly visit, 72 percent of consumers said they would be more likely to interact and submit personal information online.

Among each region surveyed, the impact of stronger security on the consumer's willingness to interact and submit personal information online seemed to have the most significant effect in Central and South America, once again. In this region, 57 percent of respondents stated they would be "significantly" more likely to interact with or submit personal information online if their provider offered stronger security. This is also much higher compared to other regions; among respondents, 21 percent in the U.S., 26 percent in Europe and 32 percent in Asia stated they would be "significantly" more likely to interact or submit personal information online.

For more information

These are just some highlights that were included in the survey we conducted among online consumers. For more information and a complete overview of the results, please visit www.rsa.com/consumersurvey.

Table 4

How would any new security features, offered in addition to a username and password, impact your willingness to interact, purchase items, or submit personal information to those sites?
(Respondents could only choose a **single** response.)

Response	20%	40%	60%	80%	100%	Freq.
I would be significantly more likely to interact or submit my personal information						34%
I would be somewhat more likely to interact or submit my personal information						38%
No change						24%
I would be somewhat less likely to interact or submit my personal information						3%
I would be significantly less likely to interact or submit my personal information						1%

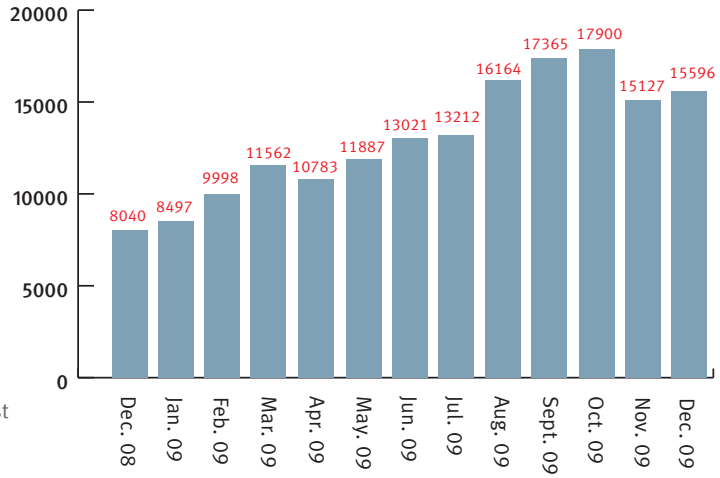
Phishing Attacks per Month

Trend Analysis

The total number of phishing attacks identified by RSA in December was 15,596 attacks, only a three percent increase from November. Fast-flux attacks in December accounted for only 20 percent, down from 38 percent in November and signifying yet another sharp drop in malicious content delivered over this type of infrastructure.

This drop is likely the result of major changes observed in the Rock Phish gang's activity and operations over the MS-Redirect Fast-Flux network. The Rock Phish gang is the primary cybercrime client of the network and known to be accountable for the vast majority of phishing and malware attacks, exclusively hosted on a dedicated server owned by MS-Redirect.

Will Fast flux attacks regain momentum? RSA believes that the number of phishing attacks launched by the Rock Phish will increase in volume once they have settled into their new infrastructure. However, it may take several months for these attacks to have a noticeable effect and reach the peak numbers reported in August, September and October 2009.



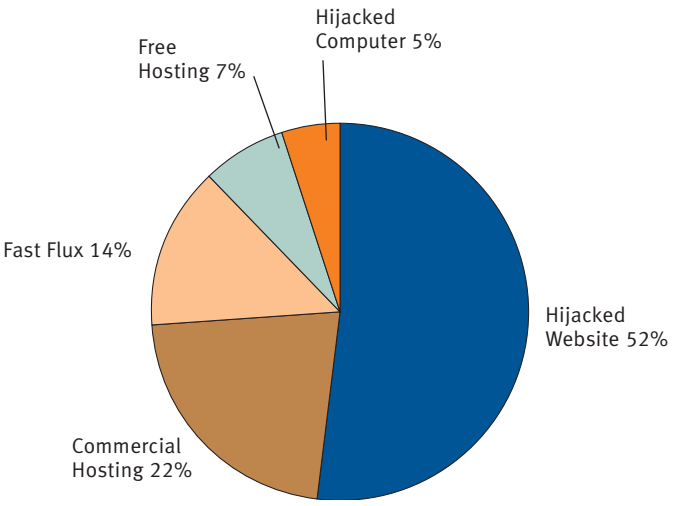
Source: RSA Anti-Fraud Command Center

Distribution of Attacks by Hosting Method

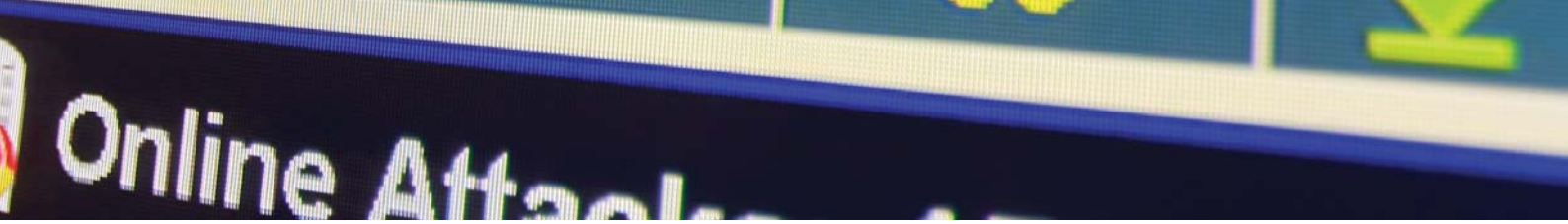
Trend Analysis

December marked another month where the number of attacks hosted on fast-flux networks diminished. This shift initially reflected the Rock Phish gang's diminished activity throughout November and has carried on through December with another drop to just 14 percent of attacks.

Hijacked sites have been the main target for launching phishing attacks, with 52 percent of attacks in December being hosted on these sites. Attacks using commercial hosting increased from 13 percent to 22 percent while free hosting more than doubled in volume (from three percent to seven percent).



Source: RSA Anti-Fraud Command Center



Hosting Methods

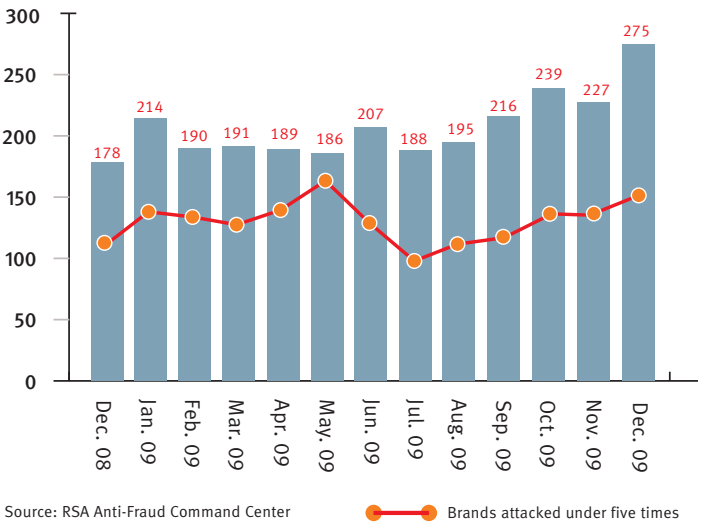
- Fast-flux networks produce an advanced Denial of Service (DNS) technique that utilizes a network of compromised computers, known as a botnet, to host and deliver phishing and malware websites. The compromised computers act as a proxy, or middleman, between the victim and the website. It is difficult to expose and shut down fast-flux networks as content servers that deliver phishing and malware websites are hidden behind a cloud of compromised machines whose addresses change very quickly in order to avoid detection.
- 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.
- Commercial hosting involves fraudsters who host their malicious websites for other fraudsters in exchange for a fee.
- Hijacked computers consist of compromised computers whose IP addresses were assigned to a specific phishing domain.
- Free Hosting refers to attacks that leverage free hosting services.

Total Number of Brands Attacked

Trend Analysis

In December, the total number of attacked brands climbed 21 percent from November. The number of brands attacked under five times showed a slight increase with 163 entities (versus 137 in November) representing a 60 percent portion. In addition, ten new entities endured their first phishing attack in December.

These figures are in line with the ongoing trend observed in previous months, showing a 55 to 60 percent portion of entities enduring five attacks or less. These relatively steady figures reflect the tendency of online criminals to repeatedly target the same few brands.

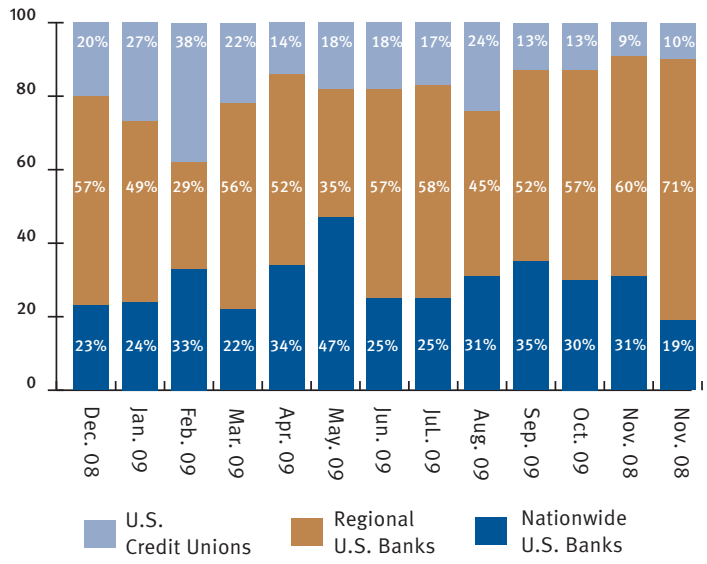


Source: RSA Anti-Fraud Command Center

Segmentation of Financial Institutions Attacked Within the U.S.

Trend Analysis

Regional U.S. banks remained the most targeted segment among online criminals, representing 71 percent of the total attack volume in December. The portion of nationwide U.S. banks, in terms of the number of banks that were attacked in each sector, fell 37 percent compared to November. The portion of targeted U.S. credit unions increased by just one percent.



Source: RSA Anti-Fraud Command Center

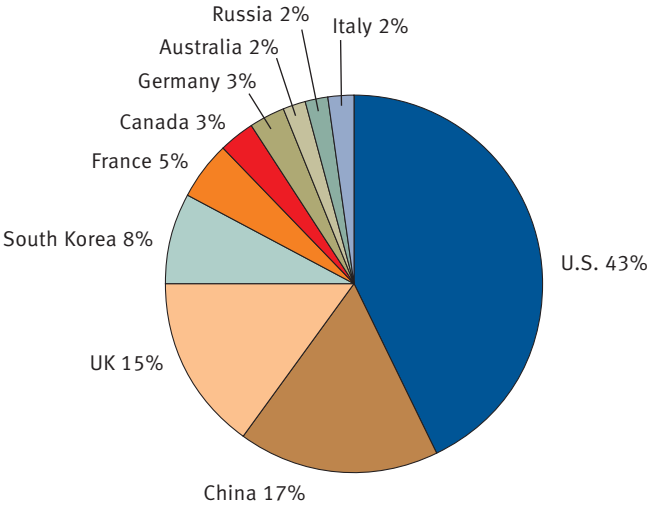
Top Ten Countries Hosting Phishing Attacks

Trend Analysis

In October 2009, we witnessed Canada become the top hosting country and the second top hosting country in November. In December, this figure has dropped sharply, with Canada only hosting three percent of attacks.

The United States hosted the most phishing attacks in December followed by China which has doubled last month's registrations (from eight percent to 17 percent). South Korea, France, Germany, Italy and Australia all remain as top hosts – although together hosting less than twenty percent of total attacks in December.

The year was predictable as fraudsters continue to target the same countries when registering malicious content websites and domains. Although some countries loop in and out of the list each month, the majority of hosting activity is repeatedly found in the U.S., the UK, China and South Korea.

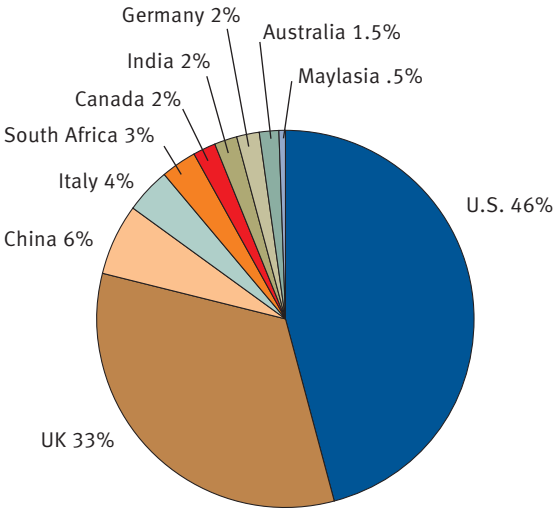


Source: RSA Anti-Fraud Command Center

Top Ten Countries by Attack Volume

Trend Analysis

The United States remains at the top of the list as the country suffering the largest volume of attacks in December, followed closely by the UK which experienced 33 percent of the attack volume. China was third, suffering six percent of attacks, followed by Italy at four percent.

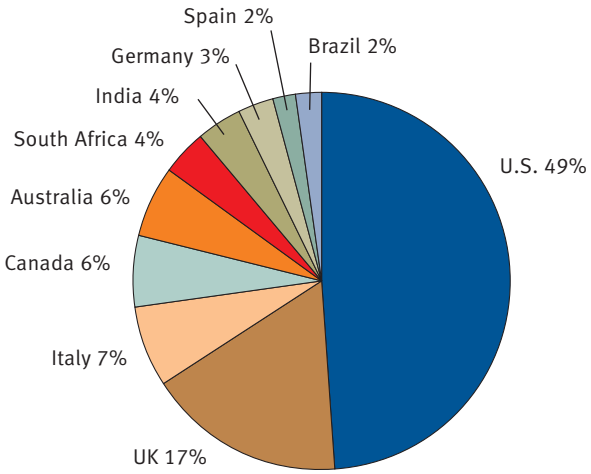


Source: RSA Anti-Fraud Command Center

Top Ten Countries by Attacked Brands

Trend Analysis

December offered yet another month of figures to support the general tendency of online criminals to attack brands in the same countries, namely the U.S., the UK, Italy, Canada, Australia, South Africa and India. The portion of brands attacked in these countries only saw minor fluctuations (ranging one half to one percent) when compared with data from November.



Source: RSA Anti-Fraud Command Center

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com
The Security Division of EMC