THE YEAR IN PHISHING

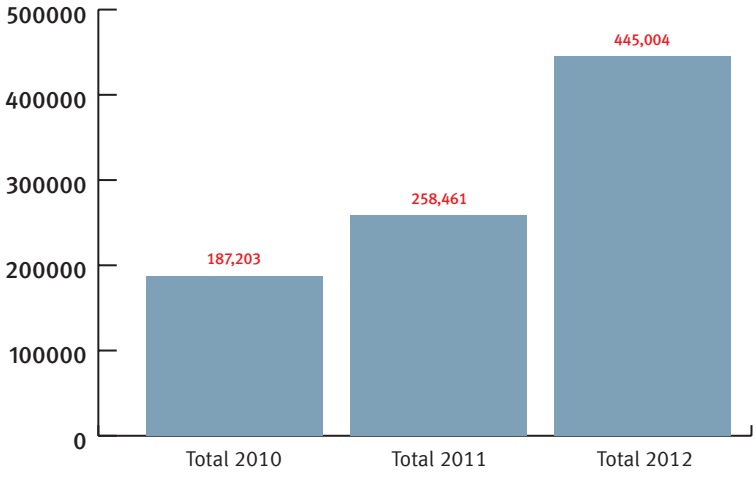
January, 2013

The total number of phishing attacks launched in 2012 was 59% higher than 2011. It appears that phishing has been able to set yet another record year in attack volumes, with global losses from phishing estimated at $1.5 billion in 2012. This represents a 22% increase from 2011.

The estimated amount lost from phishing this year was affected by the industry median – the number of uptime hours per attack. The median dropped in 2012 (from 15.3 to 11.72 hours per attack, according to the Anti-Phishing Working Group), somewhat curbing the impact of losses overall. If attack medians had remained the same, estimated losses from phishing would have exceeded $2 billion.

Phishing Attacks per Year

Total number of phishing attacks detected by the RSA Anti-Fraud Command Center (AFCC) yearly.



There is no doubt phishing still continues to be a persistent threat to all organizations. The RSA Anti-Fraud Command Center is at the forefront of phishing attack shut down. To understand the magnitude of growth however, consider the following fact: at the end of 2011, RSA celebrated its 500,000th attack takedown; that number was achieved over seven years. In 2012 alone, RSA took down almost an additional 50% of that total volume!

The roster of countries most attacked by phishing throughout the year was not surprising; the same countries appeared on the shortlist of the most attacked – the UK, the U.S., Canada, Brazil and South Africa. In Latin America, Colombia and Brazil were the two most attacked countries.

There have been major increases in phishing attack volume in some countries, while slight declines were recorded for others. One of the most significant increases in 2012 phishing numbers occurred in Canada, where attacks increased nearly 400% in the first half of the year. There have been many speculations as to why the sharp increase, but the main reason is simply economics – fraudsters follow the money. With the Canadian and U.S. dollar being exchanged at nearly a 1:1 ratio, Canada has become as lucrative a target for cybercrime.

The list of top countries to have consistently hosted the most phishing attacks throughout 2012 remained nearly identical to 2011. The top hosting countries for 2013 are (in order):

1. U.S.
2. UK
3. Germany
4. Brazil
5. Canada
6. France
7. Russia
8. Poland
9. The Netherlands
10. Japan

PHISHING TARGETS AND TACTICS IN 2012

The past year saw phishing diversify the top aims to include popular online retailers that were targeted via the usual web portals but also through the increasingly popular use of mobile apps for shopping. Other targets on phishers' lists were airline companies, gaming platforms, mobile communication providers and webmail services.

It appears that malware writers are strong players in the world of phishing kit coding, responding to the demand in the underground and servicing phishers looking for off-the-shelf kit templates or custom written specialty kits. The top requests for phishing kit writers were, unsurprisingly, the login pages of U.S.-based banks, credit card issuers and the dedicated login pages for business/corporate users of online banking/investments.

In terms of the tactics used by cybercriminals to launch their attacks, 2012 saw the use of rather simple hosting methods, mainly taking advantage of hijacked websites.

The most prominent trends noted came in the shape of using web shells and automated toolkits to hijack massive numbers of websites and smarter phishing kits containing custom plug-ins such as web-analytics tools. A proliferation of off-the-shelf codes written by black hat programmers, and the use of combined attack schemes to phish users and then redirect them to subsequent malware infection points were noted by RSA forensics analysts.

GLOBAL PHISHING FORECAST FOR 2013

Phishing Via Mobile

The most prominent market trends relevant to the mobile channel have to do with the growth in mobile device usage in both our personal and work life and the pivotal role of mobile apps. RSA expects to see more phishing directed at mobile device users, particularly smartphones, as we move into 2013. Varying social engineering schemes will target users by voice (vishing), SMS (smishing), app-based phishing (rogue apps), as well as classic email spam that users will receive and open on their mobile devices.

Phishing Via Apps

Applications are the central resource for smartphone users, and that overall popularity of apps will become just as trendy with cybercriminals.

Nowadays, users download apps designed for just about any day-to-day activity, with the most prominent of those being gaming, social networking and shopping apps. To date, both Apple and Google have surpassed 25 billion app downloads each from their respective stores. In fact, according to research firm Gartner, this number will grow to over 185 billion by 2015.

In 2013 organizations will continue to aggressively tap into this growing market and respond by further moving products and services to this channel, delivering specialized small-screen adaptations for Web browsing, and developing native apps that supply mobile functionality and brand-based services to enable customers anywhere-anytime access.

Following user behavior trends (and money) in 2013, criminals will drive underground demand for threats and attack schemes designed for the mobile. Cybercriminals will focus on apps in order to deliver phishing, conceal malware, infect devices, and steal data and money from users of different mobile platforms.

Phishing Via Social Media

In 2008, slightly more than 20% of online users in the U.S. were members of a social network. That number has since more than doubled and stands at around 50% today.

Data collected last year from *Fortune's* Global 100 revealed that more than 50 percent of companies said they have Twitter, Facebook, and YouTube accounts. Facebook membership, for example, has increased nearly 10 times since 2008, with over 7 billion unique visitors per month worldwide. Twitter shows that the number of members increased by a factor of five over the same period, boasting over 555 million regular users.

With the world turning into a smaller and more 'social' village than ever, cybercriminals are by no means staying behind.[1] They follow the money, and so as user behavior changes, RSA expects cybercriminals to continue following their target audience (future victims) to the virtual hot-spots. According to a Microsoft research study, phishing via social networks in early 2010 was only used in 8.3% of attacks—by the end of 2011 that number stood at 84.5% of the total. Phishing via social media steadily increased through 2012, jumping as much as 13.5% in one month considering Facebook alone .

1 Facebook was the number one target of phishers in November 2012 as attacks aimed at its users increasing 13.2 percentage points. (Source: Kaspersky Labs)

Another factor affecting the success of phishing via social media is the vast popularity of social gaming; an activity that brought payments into the social platform. Users who pay for gaming will not find it suspicious when they are asked for credit card details and personal information on the social network of their choice.

Social media is definitely one way by which criminals get to their target audience, phishing them for access credentials (which are used for webmail at the very least and for more than one site in most cases), as well as stealing payment details they use online.

CONCLUSION

Phishing attack numbers have been increasing annually, and although phishing is one of the oldest online scams, it seems that web users still fall for it which is why it still remains so popular with fraudsters.

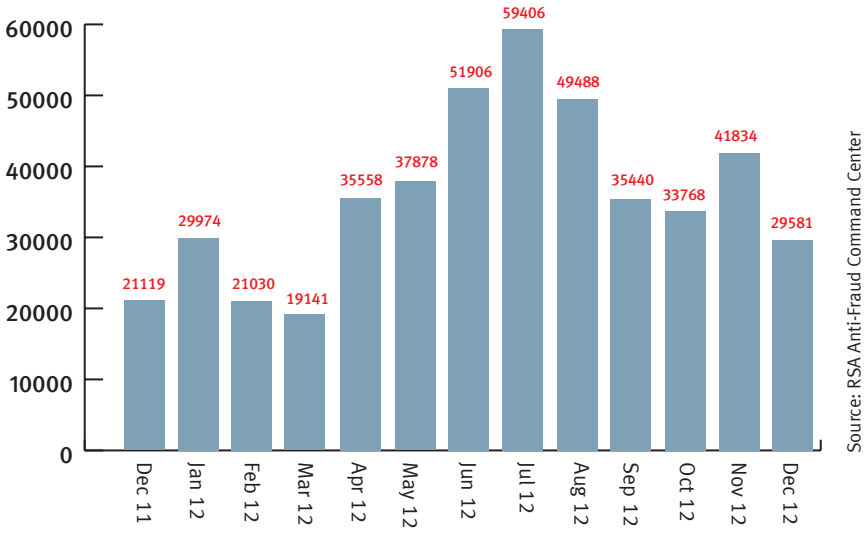
With the heightened availability of kits, cybercriminals' awareness of the latent potential in stolen credentials, and the enhanced quality of today's attacks, the forecasted outlook for 2013 calls for yet another record year riddled with hundreds of thousands of phishing attacks worldwide.

As of January 1, 2013, the RSA Anti-Fraud Command Center has shut down more than 770,000 phishing attacks in more than 180 countries.

Phishing Attacks per Month

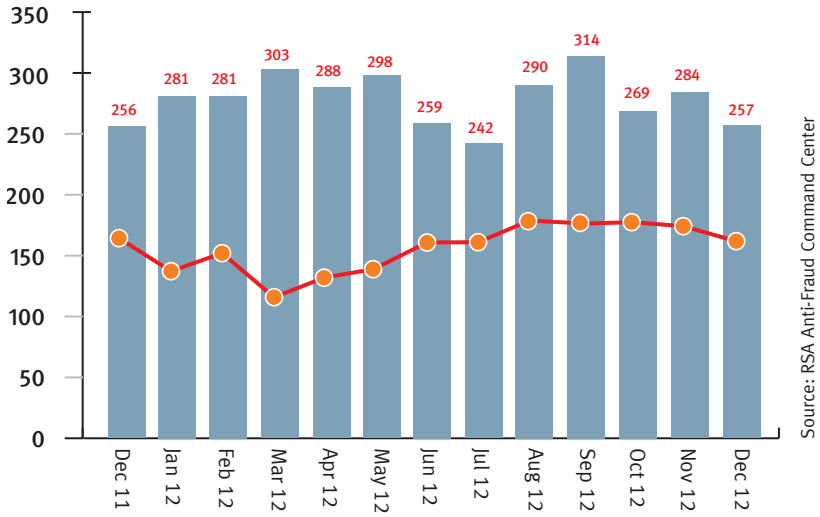
In December, RSA identified 29,581 attacks launched worldwide, marking a 29% decrease in attack volume from November, but a 40% increase year-over-year in comparison to December 2011.

The overall trend in attack numbers showed a steady rise in volume throughout the year, reaching an all-time high in July, with 59,406 attacks detected in a single month – 52% more than 2011's peak of 38,970 attacks.



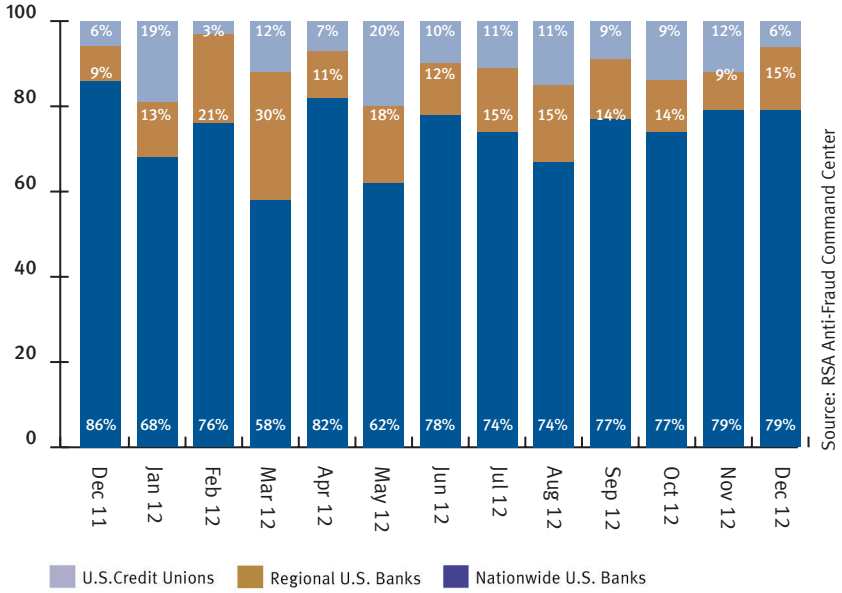
Number of Brands Attacked

In December, 257 brands were targeted in phishing attacks, marking a 10% decrease from November. Of the 257 targeted brands, 49% endured five attacks or less.



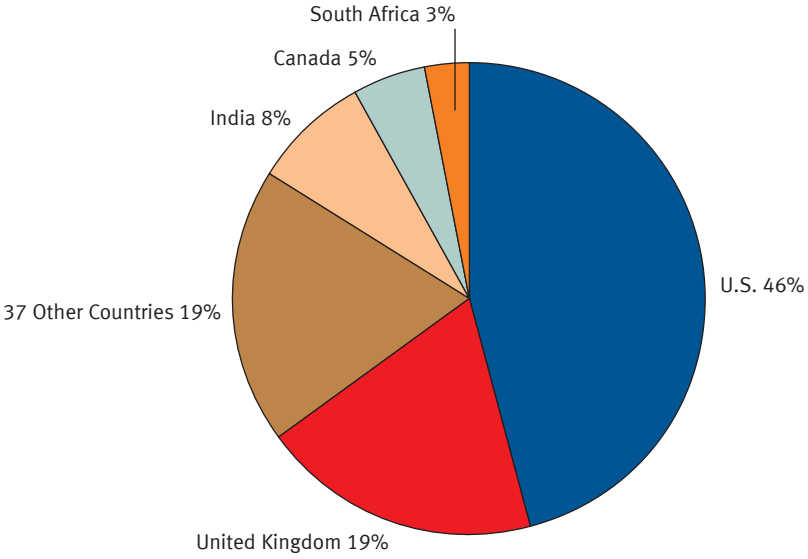
US Bank Types Attacked

U.S. nationwide banks continued to be the most targeted, absorbing 79% of total attack volume in December. It is not surprising that fraudsters prefer large financial institutions over smaller ones as the potential "victim rate" rises in conjunction with the size of the bank's customer base. Moreover, information regarding security procedures at larger institutions can be more easily located in open-source searches.



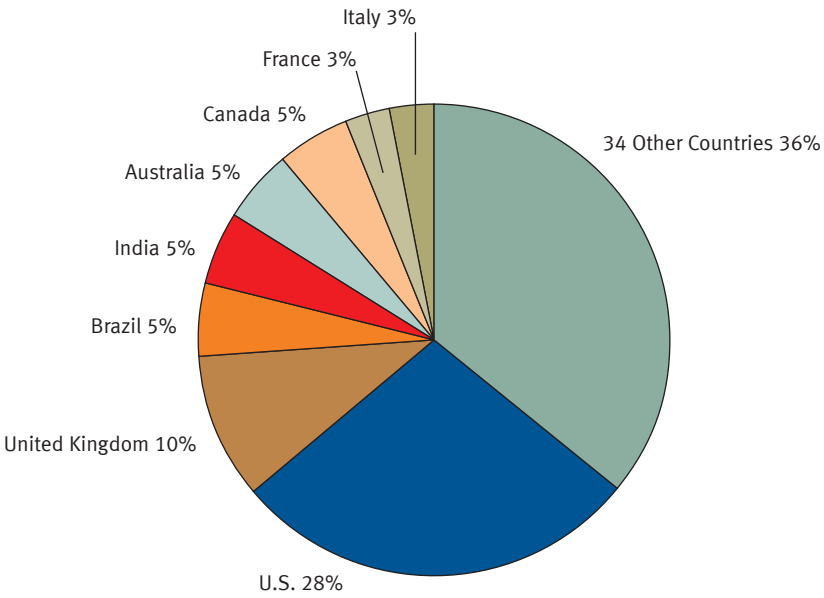
Top Countries by Attack Volume

The U.S. was targeted by the majority of – or 46% - of total phishing volume in December. The UK accounted for 19% of attack volume, while India and Canada remained third and fourth with 8% and 5% of attack volume.



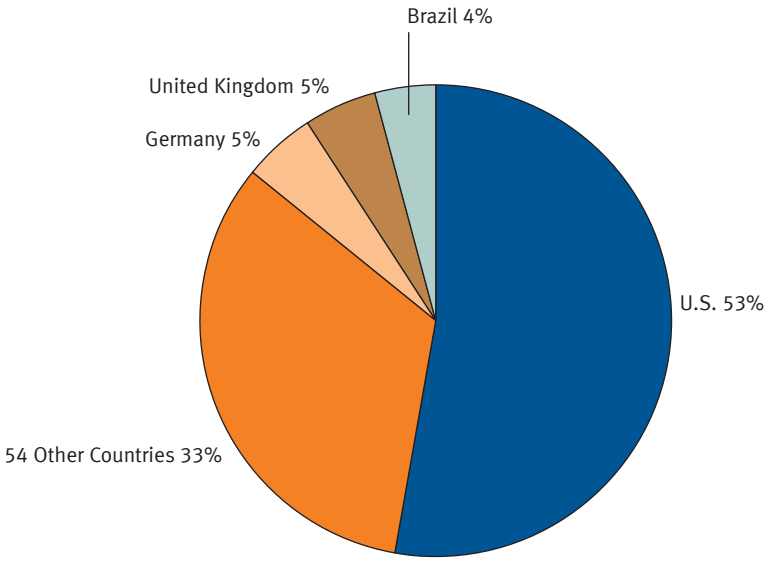
Top Countries by Attacked Brands

U.S. brands were the most targeted again in December, with 28% of total phishing attack volume, followed by UK brands which were targeted by 10% of attacks. Brands in Canada, Australia, India and Brazil were each targeted by 5% of phishing volume.



Top Hosting Countries

In December, the U.S. remained the top hosting country for phishers, hosting 53% of global phishing attacks. Germany and the UK were the second top hosting countries accounting for 5% of hosted attacks.



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.emc.com/rsa

www.emc.com/rsa

RSA®

EMC²®