THE YEAR IN PHISHING

January 2012

Unlike its more humble beginnings, phishing in 2011 did keep a strong focus on financial fraud, although the various attacks witnessed were more diverse than ever. Throughout the year, financial institutions consistently comprised at least half of the entities targeted by phishing. Consequently, financial institutions also topped the chart of entities whose web pages were spoofed to serve as the face of a majority of phishing attacks. Payment services was the second most highly targeted industry followed by retail at third.

PHISHING IS A NUMBERS GAME

In 2011, approximately one in every 300 emails circulating the web was deemed to contain elements pointing to phishing. Most phishing content targeted the public sector, which was followed by the SME business sector.

Compared with the total numbers of phishing attacks recorded in 2010, phishing numbers have increased considerably through the past year. The cumulative number of phishing attacks recorded through 2011 was 279,580—a 37% increase from 2010.

In 2011, phishing attacks also received better coverage around the globe, with brands targeted from 31 different geographies and phishing emails communicated in 16 different languages – reaching an even more diverse crowd of Internet users. The top countries in which the most brands were attacked include: the U.S., the UK, Australia, Canada, India, and Brazil.

THE PHISHER'S PORTFOLIO

The past year saw phishing diversify the top aims to include popular retailers, airlines, online auction sites and mobile communication providers. It appears that malware writers have also become strong players in the world of phishing kits, helping diversity

grow. Coders are responding to the needs of their would-be customers with offers to prepare replicas of the pages fraudsters wish to target, selling them customized “have it your way” kits.

The top requests to phishing kit writers were, unsurprisingly, the login pages of U.S.-based banks and the dedicated login pages for business clientele (banks and business services).

THE PHISH TO GO

With the increased popularity of people browsing the Internet and receiving emails to their smartphones, phishers simply followed the money. Smartphone users get their emails delivered to their mobile devices and check them in near real-time. Smartphone users have turned out to be the first to follow phishing emails, the first visitors to end up on phishing websites, and once they are already there, are also three times more likely to provide their login information than those accessing the Internet from a PC.

Yet, links to phishing pages do not have to be sent via email; mobile users can receive them in SMS messages and once they land on the phishing page, would find it hard to discern if the URL is genuine (most phones show abbreviated forms of the URL or show the mobile version of the site, thus using another URL).

THE AUTO PHISH

The favorite hosting method for phishing in 2011 was hijacked websites, by a large margin. On average, 86 percent of attacks were hosted on hijacked sites every month throughout last year. Correlating this number with the average number of monthly attacks in 2011 would mean that phishers compromised well over 23,000 websites each month in 2011.

One of the reasons for the increase in phishing attacks across the board is definitely the enhanced use of automated toolkits for the creation and hosting of phishing pages. Not only have ready-made kits become more available than ever, automated vulnerability exploits designed to compromise websites and host the phishing web pages have also played a large role in the increase of attacks.

CONCLUSION

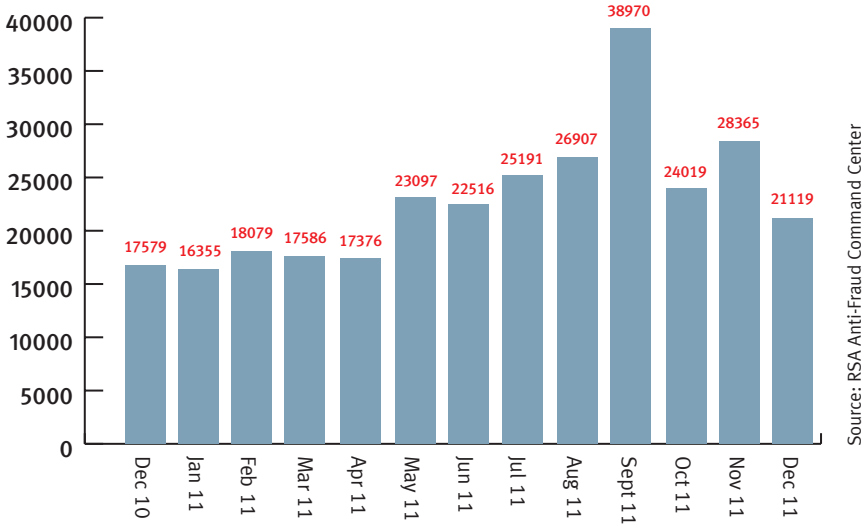
Looking at the year in phishing, it is clear that phishing has become easier than ever before with more automated toolkits available. In fact, some cybercriminals are known to invest all their efforts into phishing attacks only. On average, every phishing attack yields a $4,500 profit in stolen funds for the fraudster, a number which keeps this work-from-home endeavor rather lucrative.

Attack numbers have been increasing annually, and although phishing is one of the oldest online scams, and user awareness is higher than ever, it seems that web users still fall for phishing, unknowingly parting with their credentials over convincing enough replicas of websites they have come to trust.

With the ease of production and the enhanced quality of today’s attacks, the forecasted outlook for 2012 calls for yet another year riddled with hundreds of thousands of phishing attacks worldwide. As the phenomenon continues to spread, it stands to reason that phishing will move on to even more geographies, target more brands and be spread in more languages in 2012.

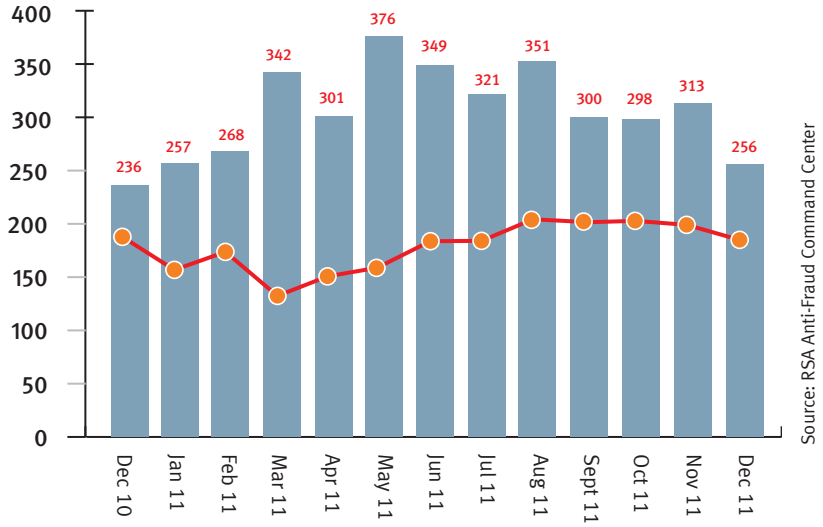
Phishing Attacks per Month

In December, phishing volumes decreased 26 percent with 21,119 unique phishing attacks identified by RSA worldwide. The UK continued to be country most targeted by phishing attacks in December, suffering 50 percent of global volume while the U.S. continued to be the top hosting country – hosting 52 percent of the world's phishing attacks in December.



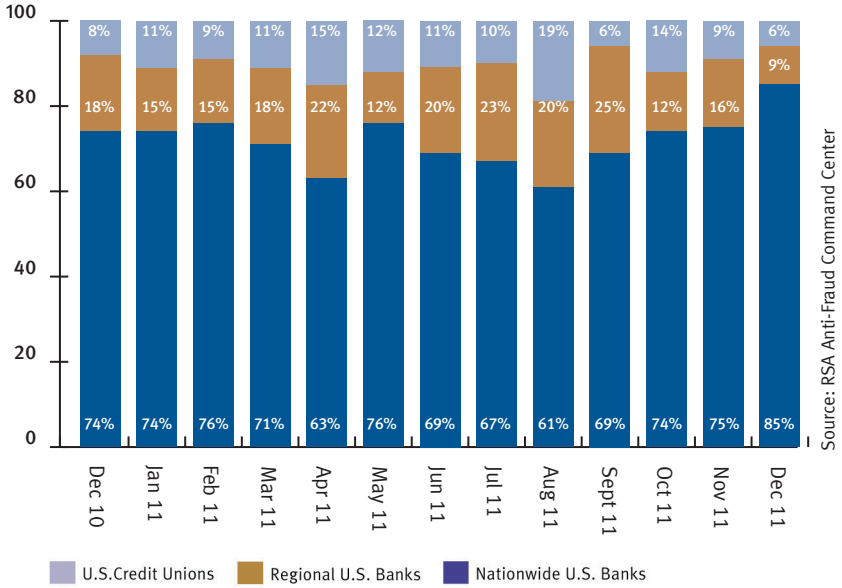
Number of Brands Attacked

In December, 256 brands were targeted through phishing attacks, marking an 18 percent decrease from November. The number of new brands attacked for the first time decreased from 13 brands in November to six brands in December.



US Bank Types Attacked

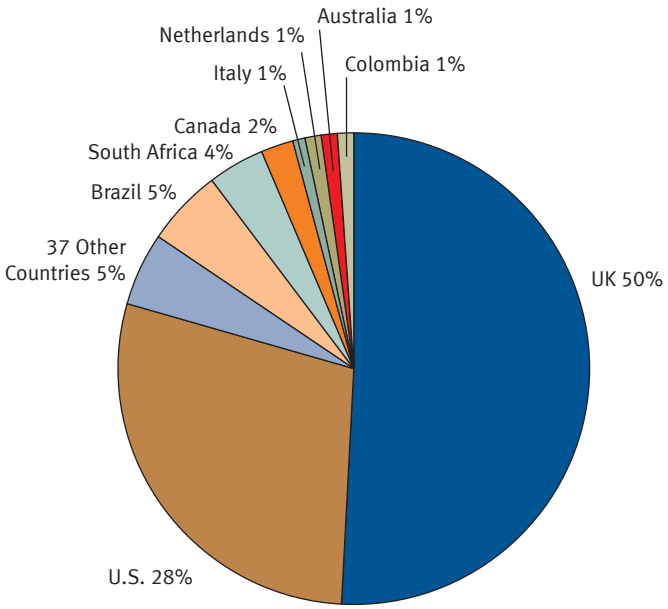
Last month, the portion of brands targeted in the U.S. credit union sector decreased three percent as did the portion of brands targeted by phishing in the U.S. regional banks sector (decreasing seven percent). The portion of attacked brands representing U.S. nationwide banks increased ten percent from 76 percent to 86 percent. This represents the highest portion of brands in the U.S. nationwide banking sector targeted by phishing in the last year.

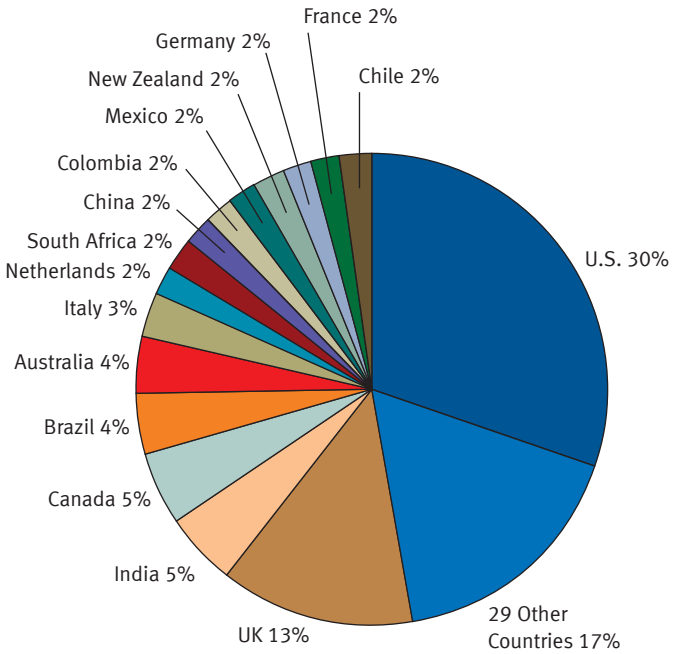


Top Countries by Attack Volume

The UK was the country most targeted by phishing once again in December – targeted by 50 percent of all attacks – for the fourth consecutive month. The U.S. was the second most targeted country with 28 percent of all phishing attacks.

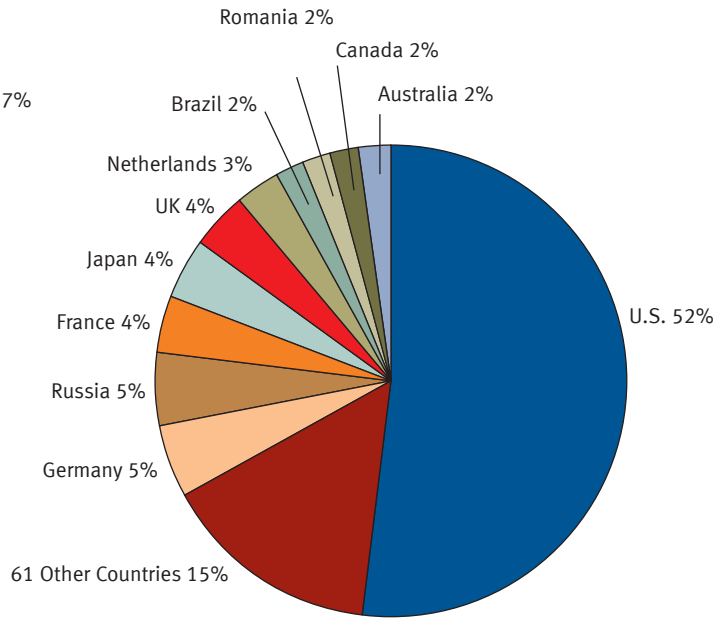
Since this time last year, the top five countries that have endured the highest volume of phishing include the UK, the U.S., South Africa, Canada and Brazil. In terms of the languages used in phishing attacks, English is still the most dominant, followed by Portuguese, Spanish and Dutch.





Top Countries by Attacked Brands

Together, the U.S. and UK accounted for 43 percent of the world's targeted brands, while the brands of 14 additional countries accounted for a total of 39 percent of phishing attacks in December.



Top Hosting Countries

In December, the US hosted 52 percent of the world's phishing attacks, a nine percent decrease from November. Germany and Russia were the second top hosts with five percent of attacks. A surprising entrance came from Japan as a top host in December, accounting for four percent of attacks.

www.rsa.com

RSA®

EMC²®